

 Universidad del Valle	Manual de Procedimientos	Código: MP-XX-XX-XX	Versión: X.0
		Página: 1 de 38	
Fecha de Emisión: Mes Año	Título: MANUAL POLITICAS SEGURIDAD DE LA INFORMACIÓN		
Elaborado por:	Revisado por:	Aprobado por:	

CONTENIDO

1 INTRODUCCION	3
2 OBJETIVO	3
3 ALCANCE.....	4
4 DEFINICIONES.....	4
5 COMPROMISO DE LA DIRECCIÓN	7
6 SANCIONES PARA LAS VIOLACIONES A LAS POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN	8
7 POLITICAS	8
7.1 Dispositivos Móviles	9
7.2 Teletrabajo.....	10
7.3 Lineamientos Talento Humano.....	11
7.3.1 Vinculación de Funcionarios.....	11
7.3.2 Durante la Vinculación de Funcionarios y Terceras Partes	12
7.3.3 Desvinculación o Cambio de roles de los Funcionarios, estudiantes y Terceras Partes	14
7.4 Uso Aceptable de los Activos	14
7.4.1 Asignación de activos de información tipo hardware	18
7.4.2 Salida y devolución de activos de información tipo hardware.....	19
7.4.3 Entrega y Disposición segura de los activos de información	19
7.5 Control de Acceso	19
7.5.1 Administración de Acceso de Usuarios	19
7.5.2 Acceso a Redes y Recursos de Red	22
7.5.3 Uso de Altos Privilegios y Utilitarios de Administración	23
7.5.4 Accesos a sistemas y aplicativos.....	25

 <u>Universidad del Valle</u>	Manual de Procedimientos	Código:	Versión: 1.0
		Página: 2 de 38	
Fecha de Emisión: 01/2019	Título: MANUAL POLITICAS SEGURIDAD DE LA INFORMACIÓN		
Elaborado por: OITEL	Revisado por: César Narváez	Aprobado por: Pablo Emilio Astroz	

7.6	Seguridad de la información en la gestión de proyectos	26
7.7	Uso de controles criptográficos y llaves.....	26
7.8	Escritorio Limpio y Pantalla Limpia	28
7.9	Respaldo de la Información	28
7.10	Transferencia de Información	30
7.11	Política de Desarrollo Seguro	31
7.12	Relación con Proveedores.....	35
7.13	Cumplimiento de Requisitos Legales y Contractuales.....	37
	7.13.1 Privacidad y protección de información de datos personales	37
	7.13.2 Reglamentación de controles criptográficos	38
7.14	Notificación de Incidentes de Seguridad de la Información	38

 <u>Universidad del Valle</u>	Manual de Procedimientos	Código:	Versión: 1.0
		Página: 3 de 38	
Fecha de Emisión: 01/2019	Título: MANUAL POLITICAS SEGURIDAD DE LA INFORMACIÓN		
Elaborado por: OITEL	Revisado por: César Narváez	Aprobado por: Pablo Emilio Astroz	

1 INTRODUCCION

La Universidad del Valle reconoce la información como activo vital para la institución. La protección y seguridad de esta información tiene una importancia primordial en muchos aspectos de su entorno. Así, para disminuir los riesgos y proteger la información, es necesario que estén implementadas un conjunto de controles y procedimientos para mantener y mejorar los niveles de seguridad de la información, independientemente de la forma en la que ésta es manejada, procesada, transportada o almacenada.

Este documento describe las políticas y normas de seguridad de la información definidas por La Universidad del Valle. Para la elaboración del mismo, se toman como base las leyes y demás regulaciones aplicables vigentes, la norma ISO/IEC 27001:2013 y las recomendaciones del estándar ISO/IEC 27002:2013.

Las políticas incluidas en este documento se constituyen como parte fundamental del Sistema de Gestión de Seguridad de la Información (SGSI) de la Universidad del Valle y se convierten en la base para la implantación y mejoramiento de los controles, procedimientos necesarios y estándares definidos, que apoyará la identificación y reducción de los riesgos vitales de seguridad, centrar los esfuerzos en la seguridad de la información y lograr su protección.

La seguridad de la información es una prioridad para la Universidad del Valle y por tanto es responsabilidad de todos velar por que no se realicen actividades que contradigan la esencia y el espíritu de cada una de estas políticas.

2 OBJETIVO

El objetivo de este documento es establecer las políticas en seguridad de la información de la Universidad del Valle, con el fin de regular la gestión de la seguridad de la información al interior de la institución, y que deben ser conocidas a través de la divulgación a toda la comunidad universitaria (funcionarios, estudiantes, contratistas y terceros) de manera individual o colectiva.

 <u>Universidad del Valle</u>	Manual de Procedimientos	Código:	Versión: 1.0
		Página: 4 de 38	
Fecha de Emisión: 01/2019	Título: MANUAL POLITICAS SEGURIDAD DE LA INFORMACIÓN		
Elaborado por: OITEL	Revisado por: César Narváez	Aprobado por: Pablo Emilio Astroz	

3 ALCANCE

Las políticas de seguridad de la información cubren todos los aspectos administrativos y de control que deben ser cumplidos por los responsables de administrar los activos, recursos y servicios tecnológicos, así como por todos los funcionarios, estudiantes, contratistas y terceros con acceso a la información y servicios de la Universidad del Valle y que estén bajo el control de la OITEL; con el fin de lograr un adecuado nivel de confidencialidad, integridad, disponibilidad en la infraestructura de información.

4 DEFINICIONES

Acuerdo de Confidencialidad: es un documento en los que los funcionarios de la Universidad del valle o los provistos por terceras partes manifiestan su voluntad de mantener la confidencialidad de la información del instituto, comprometiéndose a no divulgar, usar o explotar la información confidencial a la que tengan acceso en virtud de la labor que desarrollan dentro de la misma.

Auditoría: Proceso sistemático, independiente y documentado, para obtener evidencias de auditoría y obviamente para determinar el grado en el que se cumplen los criterios de auditoría. (ISO/IEC 27000)

Autenticación: es el procedimiento de comprobación de la identidad de un usuario o recurso tecnológico al tratar de acceder a un recurso de procesamiento o sistema de información.

Cifrado: es la transformación de los datos mediante el uso de la criptografía para producir datos ininteligibles (cifrados) y asegurar su confidencialidad. El cifrado es una técnica muy útil para prevenir la fuga de información, el monitoreo no autorizado e incluso el acceso no autorizado a los repositorios de información.

Confidencialidad: es la garantía de que la información no está disponible o divulgada a personas, entidades o procesos no autorizados.

 <u>Universidad del Valle</u>	Manual de Procedimientos	Código:	Versión: 1.0
		Página: 5 de 38	
Fecha de Emisión: 01/2019	Título: MANUAL POLITICAS SEGURIDAD DE LA INFORMACIÓN		
Elaborado por: OITEL	Revisado por: César Narváez	Aprobado por: Pablo Emilio Astroz	

Control: es toda actividad o proceso encaminado a mitigar o evitar un riesgo. Incluye políticas, procedimientos, guías, estructuras organizacionales y buenas prácticas, que pueden ser de carácter administrativo, tecnológico, físico o legal.

Disponibilidad: Es la garantía de que los usuarios autorizados tienen acceso a la información y a los activos asociados cuando lo requieren.

Escritorio lógico: Se hace referencia al escritorio del sistema operativo.

Gestión de incidentes de seguridad de la información: Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información. (ISO/IEC 27000).

Clasificación de la información: directrices para catalogar la información de la entidad y hacer una distinción entre la información que es crítica y aquella que lo es menos o no lo es y, de acuerdo con esto, establecer diferencias entre las medidas de seguridad a aplicar para preservar los criterios de confidencialidad, integridad y disponibilidad de la información

Incidente de Seguridad: es un evento adverso, confirmado o bajo sospecha, que haya vulnerado la seguridad de la información o que intente vulnerarla, sin importar la información afectada, la nube institucional académica de la Universidad del Valle, bajo el control técnico de la OITEL, la frecuencia, las consecuencias, el número de veces ocurrido o el origen (interno o externo).

Integridad: es la protección de la exactitud y estado completo de los activos.

Licencia de software: es un contrato en donde se especifican todas las normas y cláusulas que rigen el uso de un determinado producto de software, teniendo en cuenta aspectos como: alcances de uso, instalación, reproducción y copia de estos productos.

Medio removible: es cualquier componente extraíble de hardware que sea usado para el almacenamiento de información; los medios removibles incluyen cintas, discos duros removibles, CDs, DVDs, Blu Ray y unidades de almacenamiento USB, entre otras.

 Universidad del Valle	Manual de Procedimientos	Código:	Versión: 1.0
		Página: 6 de 38	
Fecha de Emisión: 01/2019	Título: MANUAL POLITICAS SEGURIDAD DE LA INFORMACIÓN		
Elaborado por: OITEL	Revisado por: César Narváez	Aprobado por: Pablo Emilio Astroz	

Perfiles de usuario: son grupos que concentran varios usuarios con similares necesidades de información y autorizaciones idénticas sobre los recursos tecnológicos o los sistemas de información a los cuales se les concede acceso de acuerdo con las funciones realizadas.

Propiedad intelectual: es el reconocimiento de un derecho particular en favor de un autor u otros titulares de derechos, sobre las obras del intelecto humano. Este reconocimiento es aplicable a cualquier propiedad que se considere de naturaleza intelectual y merecedora de protección, incluyendo las invenciones científicas y tecnológicas, las producciones literarias o artísticas, las marcas y los identificadores, los dibujos y modelos industriales y las indicaciones geográficas.

Propietario de la información: es la unidad organizacional o proceso donde se crean los activos de información.

Nube institucional académica: Todos los activos de información almacenados, localizados y gestionados en el centro de datos de la oficina de informática y telecomunicaciones (OITEL).

Recursos tecnológicos: son aquellos componentes de hardware y software tales como: servidores (de aplicaciones y de servicios de red), estaciones de trabajo, equipos portátiles, dispositivos de comunicaciones y de seguridad, servicios de red de datos y bases de datos, entre otros, los cuales tienen como finalidad apoyar las tareas administrativas necesarias para el buen funcionamiento y la optimización del trabajo al interior de la Universidad del Valle.

Responsable por el activo de información: es la persona o grupo de personas, designadas por los propietarios, encargados de velar por la confidencialidad, la integridad y disponibilidad de los activos de información y decidir la forma de usar, identificar, clasificar y proteger dichos activos a su cargo.

 <u>Universidad del Valle</u>	Manual de Procedimientos	Código:	Versión: 1.0
		Página: 7 de 38	
Fecha de Emisión: 01/2019	Título: MANUAL POLITICAS SEGURIDAD DE LA INFORMACIÓN		
Elaborado por: OITEL	Revisado por: César Narváez	Aprobado por: Pablo Emilio Astroz	

Riesgo: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).

Seguridad de la información: Preservación de la confidencialidad, integridad, y disponibilidad de la información. (ISO/IEC 27000).

Sistema de Gestión de Seguridad de la Información (SGSI): Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión y de mejora continua. (ISO/IEC 27000).

Sistema de información: es un conjunto organizado de datos, operaciones y transacciones que interactúan para el almacenamiento y procesamiento de la información que, a su vez, requiere la interacción de uno o más activos de información para efectuar sus tareas. Un sistema de información es todo componente de software ya sea de origen interno, es decir desarrollado por la Oficina de Informática y telecomunicaciones o de origen externo ya sea adquirido por la entidad como un producto estándar de mercado o desarrollado para las necesidades de ésta.

Software malicioso: es una variedad de software o programas de códigos hostiles e intrusivos que tienen como objeto infiltrarse o dañar los recursos tecnológicos, sistemas operativos, redes de datos o sistemas de información.

5 COMPROMISO DE LA DIRECCIÓN

El Consejo Superior de la Universidad del Valle aprueba esta Política de Seguridad de la Información como muestra de su compromiso y apoyo en el diseño e implementación de políticas eficientes que garanticen la seguridad de la información de la Universidad.

El Consejo Superior de la Universidad del Valle demuestran su compromiso a través de:

 <u>Universidad del Valle</u>	Manual de Procedimientos	Código:	Versión: 1.0
		Página: 8 de 38	
Fecha de Emisión: 01/2019	Título: MANUAL POLITICAS SEGURIDAD DE LA INFORMACIÓN		
Elaborado por: OITEL	Revisado por: César Narváez	Aprobado por: Pablo Emilio Astroz	

- La revisión y aprobación de las Políticas de Seguridad de la Información contenidas en este documento.
- La promoción activa de una cultura de seguridad.
- Facilitar la divulgación de este manual a todos los funcionarios de la entidad.
- El aseguramiento de los recursos adecuados para implementar y mantener las políticas de seguridad de la información.
- La verificación del cumplimiento de las políticas aquí mencionadas.

6 SANCIONES PARA LAS VIOLACIONES A LAS POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

Las Políticas de Seguridad de la Información pretenden instituir y afianzar la cultura de seguridad de la información entre los funcionarios, profesores, empleados, estudiantes, contratistas, personal externo y proveedores de la Universidad. Por tal razón, es necesaria que las violaciones a las Políticas Seguridad de la Información sean clasificadas, con el objetivo de aplicar medidas correctivas conforme con los niveles de clasificación definidos y mitigar posibles afectaciones contra la seguridad de la información. Las medidas correctivas pueden considerar desde acciones administrativas, hasta acciones de orden disciplinario o penal, de acuerdo con las circunstancias, si así lo ameritan.

7 POLITICAS

Las siguientes políticas se encuentran soportadas por normas y procedimientos específicos los cuales guiaran el manejo adecuado de la información en la universidad del valle.

 <u>Universidad del Valle</u>	Manual de Procedimientos	Código:	Versión: 1.0
		Página: 9 de 38	
Fecha de Emisión: 01/2019	Título: MANUAL POLITICAS SEGURIDAD DE LA INFORMACIÓN		
Elaborado por: OITEL	Revisado por: César Narváez	Aprobado por: Pablo Emilio Astroz	

7.1 Dispositivos Móviles

La Oficina de Informática y Telecomunicaciones (OITEL), proveerá las condiciones para el manejo de los dispositivos móviles (teléfonos inteligentes y tabletas, entre otros) siempre y cuando estén bajo el control de la misma, que hagan uso de servicios de la Universidad del Valle y que hagan parte del inventario de la Universidad. Así mismo, velará porque los funcionarios hagan un uso responsable de los servicios y equipos proporcionados por la misma.

- La Oficina de Informática y Telecomunicaciones (OITEL) establece los lineamientos aceptables para los dispositivos móviles institucionales que hagan uso de los servicios entregados por la Universidad del Valle que son:
 - Los funcionarios deben de aplicar el método de bloqueo recomendado por la OITEL, para la protección de los dispositivos móviles institucionales que serán entregados a los funcionarios. Se debe configurar estos dispositivos para que pasado un tiempo de inactividad pasen automáticamente a modo de suspensión y, en consecuencia, se active el bloqueo de la pantalla el cual requerirá el método de desbloqueo por usuario y contraseña.
 - Los funcionarios deben activar la opción de cifrado en los dispositivos móviles institucionales haciendo imposible la copia o extracción de datos si no se conoce el método de desbloqueo.
 - Los funcionarios deben evitar usar los dispositivos móviles institucionales en lugares que no les ofrezcan las garantías de seguridad física necesarias para evitar pérdida o robo de estos.
 - Los funcionarios no deben modificar las configuraciones de seguridad de los dispositivos móviles institucionales bajo su responsabilidad, ni desinstalar el software provisto con ellos al momento de su entrega.
 - Los funcionarios deben evitar la instalación de programas desde fuentes desconocidas; se deben instalar aplicaciones únicamente desde los

 <u>Universidad del Valle</u>	Manual de Procedimientos	Código:	Versión: 1.0
		Página: 10 de 38	
Fecha de Emisión: 01/2019	Título: MANUAL POLITICAS SEGURIDAD DE LA INFORMACIÓN		
Elaborado por: OITEL	Revisado por: César Narváez	Aprobado por: Pablo Emilio Astroz	

repositorios oficiales de los dispositivos móviles institucionales.

- Los funcionarios deben evitar hacer uso de redes inalámbricas de uso público.
- Los usuarios deben evitar conectar los dispositivos móviles institucionales asignados por puerto USB a cualquier computador público, de hoteles o cafés internet, entre otros.
- Los funcionarios no deben almacenar videos, fotografías o información personal en los dispositivos móviles institucionales asignados.

7.2 Teletrabajo

En caso de formalizarse y definirse el Teletrabajo para personal, con responsabilidades dentro de la Universidad del Valle, y cumpliendo con la Ley 1221 de 2008 se deberán tener en cuenta:

- La seguridad física existente en el sitio, teniendo en cuenta la seguridad física de la edificación y del entorno local;
- El entorno físico de teletrabajo propuesto;
- Los requisitos de seguridad de las comunicaciones, teniendo en cuenta la necesidad de acceso remoto a los sistemas internos de la Universidad, la sensibilidad de la información a la que se tendrá acceso y que pasará a través del enlace de comunicación y la sensibilidad del sistema interno;
- La amenaza de acceso no autorizado a información o a recursos, por parte de otras personas que usan el mismo alojamiento, por ejemplo, familia y amigos;
- El uso de redes domésticas y requisitos o restricciones sobre la configuración de servicios de red inalámbrica;
- Acuerdos para evitar disputas acerca de derechos de propiedad intelectual desarrollados en equipos de propiedad privada;

 Universidad del Valle	Manual de Procedimientos	Código:	Versión: 1.0
		Página: 11 de 38	
Fecha de Emisión: 01/2019	Título: MANUAL POLITICAS SEGURIDAD DE LA INFORMACIÓN		
Elaborado por: OITEL	Revisado por: César Narváez	Aprobado por: Pablo Emilio Astroz	

- Requisitos de firewall y de protección contra software malicioso.

Las directrices y acuerdos que se consideren deberían incluir:

- El suministro de equipo adecuado y de muebles de almacenamiento para las actividades de teletrabajo, cuando no se permite el uso del equipo de propiedad privada que no está bajo el control de la institución;
- Una definición del trabajo permitido, las horas de trabajo, la clasificación de la información que se puede mantener, y los sistemas y servicios internos a los que el teletrabajador está autorizado a acceder;
- El suministro de equipos de comunicación adecuados, incluidos los métodos para asegurar el acceso remoto;
- La seguridad física;
- Las reglas y la orientación sobre el acceso de la familia y los visitantes a los equipos y a la información;
- El suministro de soporte y mantenimiento del hardware y el software;
- El suministro de seguros;
- Los procedimientos para copias de respaldo y continuidad del negocio;
- Auditoría y seguimiento de la seguridad;
- La revocación de la autoridad y de los derechos de acceso, y la devolución de los equipos cuando las actividades del teletrabajo finalicen.

7.3 Lineamientos Talento Humano

7.3.1 Vinculación de Funcionarios

La Universidad del Valle reconoce la importancia que tiene el factor humano para el cumplimiento de sus objetivos misionales y, con el interés de contar con el personal

 <u>Universidad del Valle</u>	Manual de Procedimientos	Código:	Versión: 1.0
		Página: 12 de 38	
Fecha de Emisión: 01/2019	Título: MANUAL POLITICAS SEGURIDAD DE LA INFORMACIÓN		
Elaborado por: OITEL	Revisado por: César Narváez	Aprobado por: Pablo Emilio Astroz	

mejor calificado, garantizará que la vinculación de nuevos funcionarios se realizara siguiendo un proceso formal de selección, acorde con la legislación vigente, el cual estará orientado a las funciones y roles que deben desempeñar los funcionarios en sus cargos.

- Se deben verificar los antecedentes de todos los funcionarios de acuerdo con las leyes, reglamentos y ética pertinentes, y deberían ser proporcionales a los requisitos de la Universidad, y a la clasificación de la información a que se va a tener acceso.
- El Grupo de Talento Humano debe certificar que los funcionarios de la Universidad del Valle firmen un Acuerdo y/o Cláusula de Confidencialidad y un documento de Aceptación de Políticas de Seguridad de la Información; estos documentos deben ser anexados a los demás documentos relacionados con la ocupación del cargo.
- Cada Supervisor de Contrato, Vicerrectores, Jefes de Oficina, Directores deben verificar la existencia de Acuerdos y/o Cláusulas de Confidencialidad y de la documentación de Aceptación de Políticas para el personal provisto por terceras partes, antes de otorgar acceso a la información de la Universidad del Valle.
- El personal provisto por terceras partes, deben garantizar el cumplimiento de los Acuerdos y/o Cláusulas de Confidencialidad y aceptación de las Políticas de Seguridad de la Información de la Universidad del Valle.

7.3.2 Durante la Vinculación de Funcionarios y Terceras Partes

La Universidad del Valle en su interés por proteger su información y los recursos de procesamiento de la misma demostrará el compromiso del Consejo Superior en este esfuerzo, promoviendo que el personal cuente con el nivel deseado de conciencia en seguridad de la información para la correcta gestión de los activos de información y ejecutando el proceso disciplinario necesario cuando se incumplan las Políticas de seguridad de la información de la institución.

 <u>Universidad del Valle</u>	Manual de Procedimientos	Código:	Versión: 1.0
		Página: 13 de 38	
Fecha de Emisión: 01/2019	Título: MANUAL POLITICAS SEGURIDAD DE LA INFORMACIÓN		
Elaborado por: OITEL	Revisado por: César Narváez	Aprobado por: Pablo Emilio Astroz	

Todos los funcionarios y contratistas de la Universidad del Valle deben ser cuidadosos de no divulgar información confidencial en lugares públicos, en conversaciones o situaciones que pongan en riesgos la seguridad y el buen nombre de la Institución.

- El Consejo Superior debe promover la importancia de la seguridad de la información entre los funcionarios de la Universidad del Valle y el personal provisto por terceras partes, así como motivar el entendimiento, la toma de conciencia y el cumplimiento de las políticas, normas, procedimientos y estándares para la seguridad de la información establecidos.
- La Universidad del Valle, debe definir y establecer el proceso disciplinario o incluir en el proceso disciplinario existente en la Universidad del Valle, el tratamiento de las faltas de cumplimiento a las políticas de seguridad o los incidentes de seguridad que lo ameriten.
- La Universidad del Valle, debe diseñar y gestionar de manera permanente un programa de concientización en seguridad de la información, con el objetivo de apoyar la protección adecuada de la información y de los recursos de procesamiento la misma.
- La Universidad del Valle, debe convocar a los funcionarios a las charlas y eventos programados como parte del programa de concientización en seguridad de la información, proveer los recursos para la ejecución de las capacitaciones y controlar la asistencia a dichas charlas y eventos.
- Los funcionarios y personal provisto por terceras partes que por sus funciones manejen información de la Universidad del Valle, deben dar cumplimiento a las políticas y procedimientos de seguridad de la información, así como asistir a las capacitaciones que sean referentes a la seguridad de la información.

 Universidad del Valle	Manual de Procedimientos	Código:	Versión: 1.0
		Página: 14 de 38	
Fecha de Emisión: 01/2019	Título: MANUAL POLITICAS SEGURIDAD DE LA INFORMACIÓN		
Elaborado por: OITEL	Revisado por: César Narváez	Aprobado por: Pablo Emilio Astroz	

7.3.3 Desvinculación o Cambio de roles de los Funcionarios, estudiantes y Terceras Partes

- La división de Recursos Humanos, la división de contratación y la división de admisiones y registro académico deben reportar la desvinculación o cambio de roles y posteriormente debe solicitar o realizar la modificación o inhabilitación de usuarios a la persona.
- Al momento de devolución de los activos, a cargo del funcionario, la persona responsable lo reporta al jefe directo para control de salida del mismo.
- Para el caso de cambio o retiro de funcionarios, el personal encargado debe solicitar al funcionario o contratista los activos de información pura como (Archivos físicos, carpetas), debe hacer entrega por medio de un informe con el estado y ubicación de los mismos.
- El custodio de la información en cada dependencia, debe realizar copia de seguridad de toda la información sensible almacenada en los activos de información recibidos por parte del empleado teniendo en cuenta el procedimiento y políticas vigentes.
- En caso de entrega y/o traslado de activos de información tipo hardware por obsolescencia, reasignación, daño o para donación, el custodio hará un backup de la información y asegurará la eliminación total de la información sensible contenida en ellos mediante la aplicación de técnicas de borrado seguro, sobreescritura y formateo a bajo nivel de disco duro.

7.4 Uso Aceptable de los Activos

La Universidad del Valle como propietario de la información física así como de la información generada, procesada, almacenada y transmitida con su nube institucional académica de la Universidad del Valle, bajo el control técnico de la OITEL, otorgará responsabilidad a las áreas sobre sus activos de información, asegurando el cumplimiento de las directrices que regulen el uso adecuado de la misma.

 <u>Universidad del Valle</u>	Manual de Procedimientos	Código:	Versión: 1.0
		Página: 15 de 38	
Fecha de Emisión: 01/2019	Título: MANUAL POLITICAS SEGURIDAD DE LA INFORMACIÓN		
Elaborado por: OITEL	Revisado por: César Narváez	Aprobado por: Pablo Emilio Astroz	

La información, archivos físicos, los sistemas, los servicios y los equipos como estaciones de trabajo, equipos portátiles, impresoras, redes, Internet, correo electrónico, herramientas de acceso remoto, aplicaciones, teléfonos y servicios de fax, entre otros, propiedad de la Universidad del Valle, son activos de la institución y se proporcionan a los funcionarios y terceros autorizados, para cumplir con los propósitos del negocio.

Toda la información sensible de la Universidad del Valle, así como los activos donde ésta se almacena y se procesa deben ser asignados a un responsable, inventariados y posteriormente clasificados, de acuerdo con los requerimientos y los criterios por el jefe inmediato siguiendo la metodología de riesgos. Los propietarios de los activos de información deben llevar a cabo el levantamiento y la actualización permanente del inventario de activos de información al interior de sus procesos o áreas.

- La Oficina de Informática y Telecomunicaciones (OITEL) es la propietaria de los activos de información almacenados en la nube institucional académica de la Universidad del Valle y bajo el control técnico de la OITEL, en consecuencia, debe asegurar su apropiada operación y administración.
- La Oficina de Informática y Telecomunicaciones (OITEL) en conjunto con el Comité de Control de Cambios, son quienes deben autorizar la instalación, cambio o eliminación de componentes de la nube institucional académica de la Universidad del Valle, bajo el control técnico de la OITEL.
- La Oficina de Informática y Telecomunicaciones (OITEL) debe establecer una configuración adecuada para los recursos tecnológicos bajo el control técnico de la OITEL, con el fin de preservar la seguridad de la información y hacer un uso adecuado de ellos.
- La Oficina de Informática y Telecomunicaciones (OITEL) es responsable de preparar los requerimientos técnicos necesarios, incluyendo necesidades de hardware y software para incorporar a los procesos de compra y contratación de las estaciones de trabajo fijas y/o portátiles de los funcionarios.

 <u>Universidad del Valle</u>	Manual de Procedimientos	Código:	Versión: 1.0
		Página: 16 de 38	
Fecha de Emisión: 01/2019	Título: MANUAL POLITICAS SEGURIDAD DE LA INFORMACIÓN		
Elaborado por: OITEL	Revisado por: César Narváez	Aprobado por: Pablo Emilio Astroz	

- Los usuarios no deben realizar cambios en las estaciones de trabajo relacionados con la configuración del equipo, tales como conexiones de red, usuarios locales de la máquina, entre otros. Estos cambios pueden ser realizados únicamente por el personal asignado de la Oficina de Informática y Telecomunicaciones (OITEL).
- En caso tal de que algún colaborador requiera para el desempeño de sus funciones realizar instalación de software y/o cambios en la configuración del equipo se debe documentar la autorización caso por caso, indicando la duración de la autorización.
- La Oficina de Informática y Telecomunicaciones (OITEL) y el Comité de Informática y Telecomunicaciones de la Universidad del Valle, recomiendan utilizar alguna de las siguientes alternativas en caso de requerir algún software, para mantener el cumplimiento legal:
 - ✓ Usar software de dominio público amparado bajo la licencia publica general GNU.
 - ✓ Para aplicaciones de ofimática utilizar Open Office, Libre Office y las herramientas de Google.
 - ✓ El instalador debe ser descargado de la página oficial del fabricante.
 - ✓ Como sistema operativo usar cualquier versión libre de Linux.
 - ✓ Para otros casos se debe realizar el proceso formal de adquisición del software comercial debidamente licenciado.
- Todos los equipos de cómputo de la Universidad del Valle, deben ser bloqueados por el funcionario responsable al momento de retirarse de su puesto de trabajo.

 <u>Universidad del Valle</u>	Manual de Procedimientos	Código:	Versión: 1.0
		Página: 17 de 38	
Fecha de Emisión: 01/2019	Título: MANUAL POLITICAS SEGURIDAD DE LA INFORMACIÓN		
Elaborado por: OITEL	Revisado por: César Narváez	Aprobado por: Pablo Emilio Astroz	

- Las claves de acceso a los sistemas de información de la Universidad del Valle son personales e intransferibles, cada funcionario debe responder por las actividades que se lleven a cabo con sus datos de identificación.
- Todo problema mecánico, eléctrico o electrónico sobre los equipos de cómputo de la universidad, debe ser atendido únicamente por el personal asignado por la Oficina de Informática y Telecomunicaciones (OITEL).
- Todas las estaciones de trabajo deben apagarse o dejarse en estado de hibernación al finalizar la jornada laboral.
- Los equipos de cómputo (CPU y monitor), servidores, teléfonos IP y equipos de comunicaciones, deben conectarse a los puntos de corriente eléctrica identificados como regulados.
- Los recursos tecnológicos de la Universidad del Valle, deben ser utilizados de forma ética y en cumplimiento de las leyes y reglamentos vigentes, con el fin de evitar daños o pérdidas sobre la operación o la imagen de la institución.
- Los recursos tecnológicos de la Universidad del Valle entregados a funcionarios y proveedores, son proporcionados con el único fin de llevar a cabo las labores definidas por la Universidad; por consiguiente, no deben ser utilizados para fines personales o ajenos a este.
- Los funcionarios deben de privilegiar el uso de las herramientas y equipos institucionales para el desarrollo de sus actividades.
- Los funcionarios no deben utilizar software no autorizado o de su propiedad en los equipos entregados por la Universidad para el desempeño de sus funciones.
- Todas las estaciones de trabajo, dispositivos móviles y demás recursos tecnológicos son asignados a un responsable, por lo cual es su compromiso hacer uso adecuado y eficiente de dichos recursos.

 Universidad del Valle	Manual de Procedimientos	Código:	Versión: 1.0
		Página: 18 de 38	
Fecha de Emisión: 01/2019	Título: MANUAL POLITICAS SEGURIDAD DE LA INFORMACIÓN		
Elaborado por: OITEL	Revisado por: César Narváez	Aprobado por: Pablo Emilio Astroz	

- El sistema de correo debe ser utilizado solamente para propósitos de la institución y evitarse su uso para tratar asuntos personales.
- Evitar acceder desde redes inalámbricas públicas, pues estas redes al compartir el canal de Internet con todos los usuarios que simultáneamente se conectan a ellas, son altamente inseguras ante ataques de espionaje.
- Es muy importante no abrir correos que provengan de destinatarios desconocidos o que tengan asuntos o archivos adjuntos sospechosos.
- Cada proveedor de servicios de correo electrónico, como Gmail, cuenta con diferentes medidas de seguridad. Específicamente, Gmail, motor del correo institucional, informa cuando se han hecho inicios de sesión desde computadores diferentes a los que el usuario normalmente utiliza. Este es un buen método para enterarse inmediatamente si se presenta actividad inusual en la cuenta. Ante esta situación, cambie inmediatamente la contraseña y reporte la eventualidad mediante el correo de notificación que llega.
- Se deben evitar las acciones en Internet a nombre de la Universidad que no estén previamente aprobadas y no se relacionen con el cumplimiento de objetivos contractuales o académicos, pues de esta manera, se podría estar comprometiendo negativamente el nombre de la Universidad y su reputación.
- La información contenida en las herramientas y equipos asignados por la Universidad para el cumplimiento de sus responsabilidades académicas, administrativas y de investigación son de propiedad de la Universidad y podrán ser revisadas en el momento en que la institución lo determine.

7.4.1 Asignación de activos de información tipo hardware

- La sección de compras y contratación realiza la entrega oficial del activo de información tipo hardware al personal, de acuerdo con los requerimientos técnicos necesarios incluyendo necesidades de hardware y software definidos por la

 Universidad del Valle	Manual de Procedimientos	Código:	Versión: 1.0
		Página: 19 de 38	
Fecha de Emisión: 01/2019	Título: MANUAL POLITICAS SEGURIDAD DE LA INFORMACIÓN		
Elaborado por: OITEL	Revisado por: César Narváez	Aprobado por: Pablo Emilio Astroz	

OITEL, y a su vez identifica los activos tipo hardware físicamente de acuerdo a los procedimientos utilizados en la Universidad para el etiquetado de estos.

7.4.2 Salida y devolución de activos de información tipo hardware

- Si se requiere para el desempeño de sus funciones, que el funcionario se desplace con el activo de información tipo hardware dentro o fuera del campus Universitario, debe diligenciar en el sistema de inventarios la novedad respectiva.

7.4.3 Entrega y Disposición segura de los activos de información

- Para el caso de cambio de rol, traslado administrativo, ascenso o retiro del funcionario, el custodio del activo de información pertinente al proceso de la Universidad debe solicitar al funcionario los activos de información pura como (Archivos físicos, carpetas).
- En el momento de desvinculación o cambio de labores, los funcionarios deben realizar la entrega de su puesto de trabajo a su jefe inmediato o quien este delegue; así mismo, deben encontrarse a paz y salvo con la entrega de los recursos tecnológicos y otros activos de información suministrados en el momento de su vinculación.

7.5 Control de Acceso

7.5.1 Administración de Acceso de Usuarios

Los líderes de proceso como responsables funcionales de cada una de las dependencias de la Universidad del Valle definirán los perfiles para el control de acceso lógico de cada usuario o grupo de usuarios a las redes de datos, los recursos tecnológicos y los sistemas de información. Así mismo, velará por que estudiantes, docentes, trabajadores, funcionarios, contratistas, proveedores, comunidad en general, jubilados y pensionados tengan acceso únicamente a la información necesaria para el desarrollo de sus labores.

- La Oficina de Informática y Telecomunicaciones (OITEL) debe establecer un

 Universidad del Valle	Manual de Procedimientos	Código:	Versión: 1.0
		Página: 20 de 38	
Fecha de Emisión: 01/2019	Título: MANUAL POLITICAS SEGURIDAD DE LA INFORMACIÓN		
Elaborado por: OITEL	Revisado por: César Narváez	Aprobado por: Pablo Emilio Astroz	

procedimiento formal para la administración de los usuarios en las redes de datos, los recursos tecnológicos y sistemas de información de la institución, que contemple la creación, modificación, bloqueo o eliminación de las cuentas de usuario.

- La Oficina de Informática y Telecomunicaciones (OITEL), previa solicitud de los Jefes inmediatos de los solicitantes de las cuentas de usuario y aprobación de los líderes de proceso como responsables funcionales de cada una de las dependencias de la Universidad del Valle, debe crear, modificar, bloquear o eliminar cuentas de usuarios sobre las redes de datos, los recursos tecnológicos y los sistemas de información administrados, acorde con el procedimiento establecido.
- La Oficina de Informática y Telecomunicaciones (OITEL), debe definir lineamientos para la configuración de contraseñas que aplicaran sobre la nube institucional académica de la Universidad del Valle, bajo el control técnico de la OITEL, los servicios de red y los sistemas de información de la Universidad del Valle; dichos lineamientos deben considerar aspectos como longitud, complejidad, cambio periódico, control histórico, bloqueo por número de intentos fallidos en la autenticación y cambio de contraseña en el primer acceso, entre otros.
 - ✓ La contraseña no debe tener una longitud inferior a 8 caracteres. Entre más larga sea, será más segura.
 - ✓ Al momento de crearla debe intentarse combinar letras mayúsculas y minúsculas, números y caracteres especiales (@, \$, &, por ejemplo).
 - ✓ Debe cambiarse, dependiendo de la criticidad del recurso al que da acceso, cada cierta cantidad de tiempo.
 - ✓ No debe tenerse la misma contraseña para todo. Es altamente recomendable que varíe de un sistema a otro.

 Universidad del Valle	Manual de Procedimientos	Código:	Versión: 1.0
		Página: 21 de 38	
Fecha de Emisión: 01/2019	Título: MANUAL POLITICAS SEGURIDAD DE LA INFORMACIÓN		
Elaborado por: OITEL	Revisado por: César Narváez	Aprobado por: Pablo Emilio Astroz	

- ✓ Se debe evitar crear contraseñas con el nombre del usuario de la cuenta o con información personal obvia como nombre del cónyuge, hijos, fechas de cumpleaños, entre otros. Tampoco debe tener una secuencia previsible de letras o números como abcd o 1234, o una simple palabra en cualquier idioma.
- La Oficina de Informática y Telecomunicaciones (OITEL), debe establecer un procedimiento que asegure la eliminación, actualización o bloqueo de los privilegios de acceso otorgados sobre los recursos tecnológicos, los servicios de red y los sistemas de información de manera oportuna, cuando los líderes de proceso como responsables funcionales de cada una de las dependencias de la Universidad del Valle lo reporten.
- Los líderes de proceso como responsables funcionales de cada una de las dependencias de la Universidad del Valle, deben definir los perfiles de usuario y autorizar las solicitudes de acceso a los sistemas de información de acuerdo con los perfiles establecidos.
- Los usuarios de los servicios de red y los sistemas de información de la Universidad del Valle alojados en la nube institucional académica, bajo el control técnico de la OITEL, deben hacerse responsables de las acciones realizadas en los mismos, así como del usuario y contraseña asignados para el acceso a estos.
- Los usuarios no deben compartir sus cuentas de usuario y contraseñas con otros usuarios. El nombre de usuario y contraseña son intransferibles. Todo lo que se haga con el nombre de usuario y contraseña, es responsabilidad del titular.
- Los usuarios que posean acceso a los servicios de red y los sistemas de información alojados en la nube institucional académica de la Universidad del Valle, bajo el control técnico de la OITEL deben acogerse a lineamientos para la configuración de contraseñas definidos en este documento.

 Universidad del Valle	Manual de Procedimientos	Código:	Versión: 1.0
		Página: 22 de 38	
Fecha de Emisión: 01/2019	Título: MANUAL POLITICAS SEGURIDAD DE LA INFORMACIÓN		
Elaborado por: OITEL	Revisado por: César Narváez	Aprobado por: Pablo Emilio Astroz	

7.5.2 Acceso a Redes y Recursos de Red

La Oficina de Informática y Telecomunicaciones (OITEL) de la Universidad del Valle, como responsables de las redes de datos y los recursos de red, debe disponer que dichas redes sean debidamente protegidas contra accesos no autorizados a través de mecanismos de control de acceso lógico.

- La Oficina de Informática y Telecomunicaciones (OITEL) debe establecer un procedimiento de autorización y controles para proteger el acceso a las subredes donde se encuentran los sistemas de información institucionales.
- La Oficina de Informática y Telecomunicaciones (OITEL) debe asegurar que las redes cableadas de la institución cuenten con controles que eviten accesos no autorizados.
- La Universidad del Valle, debe establecer controles para la identificación de proveedores en las redes o recursos de red de la Universidad del Valle en la Nube institucional académica, así como velar por la aceptación de las responsabilidades de terceros. Además, se debe formalizar la aceptación de las Políticas de Seguridad de la Información por parte de estos.
- La Oficina de Informática y Telecomunicaciones (OITEL) debe autorizar la creación o modificación y cancelación del acceso a la red.
- Los líderes de proceso como responsables funcionales de cada una de las dependencias de la Universidad del Valle deben autorizar la creación o modificación y cancelación de los accesos a los recursos de red de la Universidad del Valle.
- La Oficina de Informática y Telecomunicaciones (OITEL) debe enviar periódicamente reportes a los líderes de proceso como responsables funcionales de cada una de las dependencias de la Universidad del Valle, de los controles de acceso entregados a estudiantes, docentes, trabajadores, funcionarios, contratistas, proveedores, comunidad en general, jubilados y pensionados, con

 Universidad del Valle	Manual de Procedimientos	Código:	Versión: 1.0
		Página: 23 de 38	
Fecha de Emisión: 01/2019	Título: MANUAL POLITICAS SEGURIDAD DE LA INFORMACIÓN		
Elaborado por: OITEL	Revisado por: César Narváez	Aprobado por: Pablo Emilio Astroz	

el fin de revisar que dichos usuarios tengan acceso permitido únicamente a aquellos recursos de red y servicios de la nube institucional académica de la Universidad del Valle, bajo el control técnico de la OITEL para los que fueron autorizados.

- Los estudiantes, docentes, trabajadores, funcionarios, contratistas, proveedores, comunidad en general, jubilados y pensionados, antes de contar con acceso lógico por primera vez a la red de datos de la Universidad del Valle, deben contar con el formato de creación de cuentas de usuario debidamente autorizado y el Acuerdo de Confidencialidad firmado previamente.

7.5.3 Uso de Altos Privilegios y Utilitarios de Administración

La Oficina de Informática y Telecomunicaciones (OITEL) de la Universidad del valle garantizara que los recursos de la nube institucional académica de la Universidad del Valle, bajo el control técnico de la OITEL y los servicios de red sean operados y administrados en condiciones controladas y de seguridad, que permitan un monitoreo posterior de la actividad de los usuarios administradores, poseedores de los más altos privilegios sobre dichos plataforma y servicios.

- La Oficina de Informática y Telecomunicaciones (OITEL), debe otorgar los privilegios para administración de recursos tecnológicos, servicios de red y sistemas de información sólo a aquellos funcionarios designados para dichas funciones.
- La Oficina de Informática y Telecomunicaciones (OITEL), debe establecer cuentas personalizadas con altos privilegios para cada uno de los administradores de los recursos tecnológicos, servicios de red y sistemas de información.
- La Oficina de Informática y Telecomunicaciones (OITEL), debe restringir las conexiones remotas a los recursos de la nube institucional académica de la Universidad del Valle, bajo el control técnico de la OITEL; únicamente se deben permitir estos accesos a personal autorizado, de acuerdo con las labores

 <u>Universidad del Valle</u>	Manual de Procedimientos	Código:	Versión: 1.0
		Página: 24 de 38	
Fecha de Emisión: 01/2019	Título: MANUAL POLITICAS SEGURIDAD DE LA INFORMACIÓN		
Elaborado por: OITEL	Revisado por: César Narváez	Aprobado por: Pablo Emilio Astroz	

desempeñadas.

- La Oficina de Informática y Telecomunicaciones (OITEL), debe asegurarse de que los usuarios o perfiles de usuario que traen por defecto los sistemas operativos, el firmware y las bases de datos alojadas en la nube institucional académica de la Universidad del Valle y bajo el control técnico de la OITEL, sean suspendidos o renombrados y que las contraseñas que traen por defecto dichos usuarios o perfiles sean modificadas.
- Los usuarios finales de los recursos tecnológicos, los servicios de red y los sistemas de información alojados en la nube institucional académica bajo el control técnico de la OITEL, no deben hacer uso de utilitarios que permitan accesos privilegiados a dichos recursos, servicios o sistemas.
- La Oficina de Informática y Telecomunicaciones (OITEL), debe deshabilitar las funcionalidades o servicios no utilizados de los sistemas operativos, el firmware y las bases de datos. Se debe configurar el conjunto mínimo requerido de funcionalidades, servicios y utilitarios.
- La Oficina de Informática y Telecomunicaciones (OITEL) debe generar y mantener actualizado un listado de las cuentas administrativas de los recursos de la nube institucional académica de la Universidad del Valle, bajo el control técnico de la OITEL.
- La Oficina de Informática y Telecomunicaciones (OITEL) debe validar que las políticas de contraseñas establecidas sobre la nube institucional académica de la Universidad del Valle, bajo el control técnico de la OITEL, los servicios de red y los sistemas de información son aplicables a los usuarios administradores; así mismo, debe verificar que el cambio de contraseña de los usuarios administradores acoja el procedimiento definido para tal fin.
- La administración de todos los recursos que no estén bajo el control técnico de la OITEL, deben acogerse a todas las políticas definidas en este numeral.

 <u>Universidad del Valle</u>	Manual de Procedimientos	Código:	Versión: 1.0
		Página: 25 de 38	
Fecha de Emisión: 01/2019	Título: MANUAL POLITICAS SEGURIDAD DE LA INFORMACIÓN		
Elaborado por: OITEL	Revisado por: César Narváez	Aprobado por: Pablo Emilio Astroz	

7.5.4 Accesos a sistemas y aplicativos

- La Oficina de Informática y Telecomunicaciones (OITEL), velara por la asignación, modificación y revocación de privilegios de accesos a sus sistemas o aplicativos de manera controlada.
- La Oficina de Informática y Telecomunicaciones (OITEL), debe garantizar que los sistemas de información y aplicativos que estén en la nube institucional académica y que estén bajo el control técnico de la OITEL, sean debidamente protegidos contra accesos no autorizados a través de mecanismos de control de acceso lógico.
- La Oficina de Informática y Telecomunicaciones (OITEL), debe autorizar los accesos a los sistemas de información y aplicativos que estén en la nube institucional académica y que estén bajo el control técnico de la OITEL, de acuerdo con los perfiles establecidos y las necesidades de uso definidos por los líderes de proceso como responsables funcionales de cada una de las dependencias de la Universidad del Valle.
- La Oficina de Informática y Telecomunicaciones (OITEL), debe emitir reportes periódicamente de los perfiles definidos en los sistemas de información y los privilegios asignados a los usuarios que acceden a ellos e informar a los líderes de proceso como responsables funcionales de cada una de las dependencias de la Universidad del Valle.
- La Oficina de Informática y Telecomunicaciones (OITEL), debe establecer un procedimiento para la asignación de accesos a los sistemas de información y aplicativos que estén en la nube institucional académica y que estén bajo el control técnico de la OITEL.
- La Oficina de Informática y Telecomunicaciones (OITEL), debe establecer ambientes para los sistemas de información y aplicativos que estén en la nube institucional académica y que estén bajo el control técnico de la OITEL, separados a nivel físico y lógico para desarrollo, pruebas y producción, contando cada uno con su plataforma, servidores, aplicaciones, dispositivos

 Universidad del Valle	Manual de Procedimientos	Código:	Versión: 1.0
		Página: 26 de 38	
Fecha de Emisión: 01/2019	Título: MANUAL POLITICAS SEGURIDAD DE LA INFORMACIÓN		
Elaborado por: OITEL	Revisado por: César Narváez	Aprobado por: Pablo Emilio Astroz	

y versiones independientes de los otros ambientes, evitando que las actividades de desarrollo y pruebas puedan poner en riesgo la integridad de la información de producción.

- La Oficina de Informática y Telecomunicaciones (OITEL), debe asegurar, mediante los controles necesarios, que los usuarios utilicen diferentes usuarios para los ambientes de desarrollo, pruebas y producción, y así mismo que los menús muestren los mensajes de identificación apropiados para reducir los riesgos de error.
- Los sistemas de información y aplicativos que estén en la nube institucional académica y que estén bajo el control técnico de la OITEL deben implementar medidas visuales que distingan los ambientes de desarrollo, pruebas y producción.

7.6 Seguridad de la información en la gestión de proyectos

La seguridad de la información se debe integrar a la gestión de proyectos para asegurar que los riesgos de seguridad de la información se identifiquen y traten como parte de los proyectos. Lo anterior aplica a cualquier proyecto, independientemente de su naturaleza. Por lo tanto, es responsabilidad del personal que va a presentar un proyecto asegurar que se sigan las siguientes directrices:

- Incluir objetivos de seguridad de la información en los objetivos del proyecto.
- Realizar valoración de los riesgos de seguridad de la información en la fase de estudios previos del proyecto, para identificar los controles necesarios.
- Hacer seguimiento a los riesgos y controles aplicados para tratar los riesgos, durante todas las fases del proyecto.

7.7 Uso de controles criptográficos y llaves

 <u>Universidad del Valle</u>	Manual de Procedimientos	Código:	Versión: 1.0
		Página: 27 de 38	
Fecha de Emisión: 01/2019	Título: MANUAL POLITICAS SEGURIDAD DE LA INFORMACIÓN		
Elaborado por: OITEL	Revisado por: César Narváez	Aprobado por: Pablo Emilio Astroz	

- La Oficina de Informática y Telecomunicaciones (OITEL), debe almacenar y/o transmitir la información digital bajo el control de la OITEL y que este clasificada como reservada o restringida bajo técnicas de cifrado con el propósito de proteger su confidencialidad e integridad.
- La Oficina de Informática y Telecomunicaciones (OITEL), debe verificar que todo los sistemas de información y aplicativos que estén en la nube institucional académica y que estén bajo el control técnico de la OITEL que requiera realizar transmisión de información reservada o restringida, cuente con mecanismos de cifrado de datos.
- La Oficina de Informática y Telecomunicaciones (OITEL), debe desarrollar y establecer un procedimiento para el manejo y la administración de llaves de cifrado.
- La Oficina de Informática y Telecomunicaciones (OITEL), debe desarrollar y establecer estándares para la aplicación de controles criptográficos en los sistemas de información y aplicativos que estén en la nube institucional académica y que estén bajo el control técnico de la OITEL.
- Los custodios de la información clasificada como reservada o restringida deben cifrarla y garantizar la confiabilidad de los sistemas de almacenamiento de dicha información.
- Los desarrolladores de software deben asegurar que los controles criptográficos de los sistemas construidos cumplen con los estándares establecidos por la Oficina de Informática y Telecomunicaciones (OITEL).
- La Oficina de Informática y Telecomunicaciones (OITEL), debe establecer procesos para la gestión apropiada de las llaves en todas sus etapas: generación, almacenamiento, archivo, recuperación, distribución, retiro y destrucción. De este modo se protegen contra modificación, pérdida. uso y divulgación no autorizados.

 <u>Universidad del Valle</u>	Manual de Procedimientos	Código:	Versión: 1.0
		Página: 28 de 38	
Fecha de Emisión: 01/2019	Título: MANUAL POLITICAS SEGURIDAD DE LA INFORMACIÓN		
Elaborado por: OITEL	Revisado por: César Narváez	Aprobado por: Pablo Emilio Astroz	

- Los equipos usados para generar, almacenar y archivar las llaves, deben estar protegidos físicamente.

7.8 Escritorio Limpio y Pantalla Limpia

- Todos los estudiantes, docentes, trabajadores, funcionarios, contratistas, proveedores, jubilados, pensionados y comunidad en general deben mantener la información restringida o confidencial bajo llave cuando sus puestos de trabajo se encuentren desatendidos o en horas no laborales. Esto incluye: documentos impresos, CDs, dispositivos de almacenamiento USB y medios removibles en general. Adicionalmente, se requiere que la información sensible que se envía a las impresoras sea recogida de manera inmediata.
- Todos los estudiantes, docentes, trabajadores, funcionarios, contratistas, proveedores, jubilados, pensionados y comunidad en general son responsables de bloquear la sesión de su estación de trabajo en el momento en que se retiren del puesto de trabajo, la cual se podrá desbloquear sólo con la contraseña del usuario o huella dactilar en las estaciones de trabajo que soporten dicho sistema. Cuando finalicen sus actividades, se deben cerrar todas las aplicaciones y dejar los equipos apagados.
- La información clasificada como altamente confidencial no debe ser nunca enviada a una impresora de la red, sin que exista una persona autorizada para cuidarla durante y después de la impresión. La variedad de la información que se envía a las impresoras puede alternar entre información pública e información confidencial, dado que información confidencial no puede ser revelada a personas no autorizadas.
- El escritorio lógico debe estar libre de información sensible o confidencial.

7.9 Respaldo de la Información

La Oficina de Informática y Telecomunicaciones (OITEL), debe asegurar que la información definida y contenida en la nube institucional académica de la Universidad del Valle, bajo el control técnico de la OITEL, como servidores, dispositivos de red para

 <u>Universidad del Valle</u>	Manual de Procedimientos	Código:	Versión: 1.0
		Página: 29 de 38	
Fecha de Emisión: 01/2019	Título: MANUAL POLITICAS SEGURIDAD DE LA INFORMACIÓN		
Elaborado por: OITEL	Revisado por: César Narváez	Aprobado por: Pablo Emilio Astroz	

almacenamiento de información, estaciones de trabajo, archivos de configuración de dispositivos de red y seguridad, entre otros, sea periódicamente resguardada mediante mecanismos y controles adecuados que garanticen su identificación, protección, integridad y disponibilidad.

Así mismo, garantizara que los medios magnéticos que contienen la información crítica sean almacenados en una ubicación diferente a las instalaciones donde se encuentra dispuesta. El sitio externo donde se resguarden las copias de respaldo debe contar con los controles de seguridad física y medioambiental apropiados.

- La Oficina de Informática y Telecomunicaciones (OITEL), a través de sus funcionarios, debe generar y adoptar los procedimientos para la generación, restauración, almacenamiento y tratamiento para las copias de respaldo de la información, velando por su integridad y disponibilidad.
- La Oficina de Informática y Telecomunicaciones (OITEL), debe disponer de los recursos necesarios para permitir la identificación de los medios de almacenamiento, la información contenida en ellos y la ubicación física de los mismos para permitir un rápido y eficiente acceso a los medios que contienen la información resguardada.
- La Oficina de Informática y Telecomunicaciones (OITEL), a través de sus funcionarios, debe llevar a cabo los procedimientos para realizar pruebas de recuperación a las copias de respaldo, para así comprobar su integridad y posibilidad de uso en caso de ser necesario.
- Se definen las condiciones de transporte o transmisión y custodia de las copias de respaldo de la información que son almacenadas externamente, en contratos y/o acuerdos a nivel de servicio, si es el caso.
- La Oficina de Informática y Telecomunicaciones (OITEL), debe proporcionar apoyo para la definición de las estrategias de generación, retención y rotación de las copias de respaldo de la los activos información de la Universidad del Valle.

 Universidad del Valle	Manual de Procedimientos	Código:	Versión: 1.0
		Página: 30 de 38	
Fecha de Emisión: 01/2019	Título: MANUAL POLITICAS SEGURIDAD DE LA INFORMACIÓN		
Elaborado por: OITEL	Revisado por: César Narváez	Aprobado por: Pablo Emilio Astroz	

- La Oficina de Informática y Telecomunicaciones (OITEL), debe identificar la información crítica de los sistemas de información y aplicativos que estén en la nube institucional académica y que estén bajo el control técnico de la OITEL, que debe ser respaldada y almacenada de acuerdo con su nivel de clasificación.

7.10 Transferencia de Información

Los líderes de proceso como responsables funcionales de cada una de las dependencias de la Universidad del Valle, asegurarán la protección de la información en el momento de ser transferida o intercambiada con otras entidades y establecerán los controles necesarios para el intercambio de información.

La Universidad establecerá Acuerdos de Confidencialidad o de Intercambio de Información con los proveedores con los que se realice dicho intercambio.

La OITEL definirá el uso de tecnologías informáticas y de telecomunicaciones para llevar a cabo el intercambio de información sobre los sistemas de información y aplicativos que estén en la nube institucional académica y que estén bajo el control técnico de la OITEL.

- La oficina jurídica de la Universidad del Valle, debe definir los modelos de Acuerdos de Confidencialidad y de intercambio de información entre la Universidad del Valle y proveedores incluyendo los compromisos adquiridos y las penalidades civiles o penales por el incumplimiento de dichos acuerdos.
- Entre los aspectos a considerar se debe incluir:
 - ✓ La prohibición de divulgar la información entregada por la Universidad del Valle por parte de los terceros con quienes se establecen estos acuerdos.
 - ✓ La destrucción de dicha información una vez cumpla su cometido.
- La División de contratación de la Universidad del Valle, debe incluir en los contratos que se constituyan con proveedores, los Acuerdos de Confidencialidad o Acuerdos de intercambio dejando explícitas las responsabilidades y obligaciones

 <u>Universidad del Valle</u>	Manual de Procedimientos	Código:	Versión: 1.0
		Página: 31 de 38	
Fecha de Emisión: 01/2019	Título: MANUAL POLITICAS SEGURIDAD DE LA INFORMACIÓN		
Elaborado por: OITEL	Revisado por: César Narváez	Aprobado por: Pablo Emilio Astroz	

legales asignadas a dichos terceros por la divulgación no autorizada de información de la Universidad del Valle que les ha sido entregada.

- Los líderes de proceso como responsables funcionales de cada una de las dependencias de la Universidad del Valle, deben velar porque el intercambio de información con entidades externas se realice en cumplimiento de este Manual de Políticas de Seguridad, los Acuerdos de Intercambio de Información y el procedimiento definido para dicho intercambio de información.
- Los estudiantes, docentes, trabajadores, funcionarios, contratistas, proveedores, comunidad en general, jubilados y pensionados deben utilizar únicamente los mecanismos y herramientas proporcionadas por la Oficina de Informática y Telecomunicaciones (OITEL), para el envío o recepción de información confidencial para la Universidad del Valle.
- Los estudiantes, docentes, trabajadores, funcionarios, contratistas, proveedores, comunidad en general, jubilados y pensionados no deben revelar o intercambiar información confidencial de la Universidad del Valle por ningún medio, sin contar con la debida autorización del jefe inmediato.
- Los estudiantes, docentes, trabajadores, funcionarios, contratistas, proveedores, comunidad en general, jubilados y pensionados deben evitar enviar información restringida a través de correo electrónico, pero en el caso de que sea estrictamente necesario debe cifrar la información enviada por correo con la debida autorización del jefe inmediato.

7.11 Política de Desarrollo Seguro

La Oficina de Informática y Telecomunicaciones (OITEL), debe garantizar que el desarrollo interno o externo de los sistemas de información cumpla con los requerimientos de seguridad esperados, con las buenas prácticas para desarrollo seguro de aplicativos, así como con metodologías para la realización de pruebas de aceptación y seguridad al software desarrollado. Además, se asegurará que todo software desarrollado o adquirido, interna o externamente cuenta con el soporte, actualización y mantenimiento requeridos.

 Universidad del Valle	Manual de Procedimientos	Código:	Versión: 1.0
		Página: 32 de 38	
Fecha de Emisión: 01/2019	Título: MANUAL POLITICAS SEGURIDAD DE LA INFORMACIÓN		
Elaborado por: OITEL	Revisado por: César Narváez	Aprobado por: Pablo Emilio Astroz	

- La Oficina de Informática y Telecomunicaciones (OITEL) debe implantar los controles necesarios para asegurar que las migraciones entre los ambientes de desarrollo, pruebas y producción han sido aprobadas, de acuerdo con el procedimiento de control de cambios.
- La Oficina de Informática y Telecomunicaciones (OITEL) debe contar con sistemas de control de versiones para administrar los cambios de los sistemas de información de la Universidad del Valle.
- La Oficina de Informática y Telecomunicaciones (OITEL) debe asegurarse que los sistemas de información adquiridos o desarrollados por terceros, cuenten con un acuerdo de licenciamiento el cual debe especificar las condiciones de uso del software y los derechos de propiedad intelectual.
- La Oficina de Informática y Telecomunicaciones (OITEL) debe usar metodologías para la realización de pruebas al software desarrollado, que contengan pautas para la selección de escenarios, niveles, tipos, datos de pruebas y sugerencias de documentación.
- La Oficina de Informática y Telecomunicaciones (OITEL), a través de sus funcionarios, se debe asegurar que la nube institucional académica de la Universidad del Valle, bajo el control técnico de la OITEL, las herramientas de desarrollo y los componentes de cada sistema de información estén actualizados con todos los parches generados para las versiones en uso y que estén ejecutando la última versión aprobada del sistema.
- La Oficina de Informática y Telecomunicaciones (OITEL), debe verificar que las pruebas de seguridad sobre los sistemas de información y aplicativos que estén en la nube institucional académica y que estén bajo el control técnico de la OITEL, se realicen de acuerdo con las metodologías definidas, contando con pruebas debidamente documentadas.
- La Oficina de Informática y Telecomunicaciones (OITEL), debe aprobar las migraciones entre los ambientes de desarrollo y pruebas de sistemas de información nuevos y/o de cambios o nuevas funcionalidades.

 <u>Universidad del Valle</u>	Manual de Procedimientos	Código:	Versión: 1.0
		Página: 33 de 38	
Fecha de Emisión: 01/2019	Título: MANUAL POLITICAS SEGURIDAD DE LA INFORMACIÓN		
Elaborado por: OITEL	Revisado por: César Narváez	Aprobado por: Pablo Emilio Astroz	

- Los líderes de proceso como responsables funcionales de cada una de las dependencias de la Universidad del Valle, deben aprobar las migraciones entre los ambientes de pruebas y producción de sistemas de información nuevos y/o de cambios o nuevas funcionalidades.
- La Oficina de Informática y Telecomunicaciones (OITEL), debe garantizar que la información entregada a los desarrolladores para sus pruebas será enmascarada y no revelará información confidencial de los ambientes de producción.
- La Oficina de Informática y Telecomunicaciones (OITEL), debe eliminar la información de los ambientes de pruebas que no estén en constante uso, una vez éstas han concluido.
- Los desarrolladores de los sistemas de información deben considerar las buenas prácticas y lineamientos de desarrollo seguro durante el ciclo de vida de los mismos, pasando desde el diseño hasta la puesta en marcha.
- Los desarrolladores y proveedores de software deben construir los aplicativos de tal manera que efectúen las validaciones de datos de entrada y la generación de los datos de salida de manera confiable, utilizando rutinas de validación centralizadas y estandarizadas.
- Los desarrolladores y proveedores de software deben asegurar que los sistemas de información construidos validen la información suministrada por los usuarios antes de procesarla, teniendo en cuenta aspectos como: tipos de datos, rangos válidos, longitud, listas de caracteres aceptados, caracteres considerados peligrosos y caracteres de alteración de rutas, entre otros.
- Los desarrolladores y proveedores de software, deben asegurar que los sistemas de información construidos no puedan cambiar la estructura ni el contenido de la base de datos desde el código fuente de dicha aplicación.
- Los desarrolladores y proveedores deben incluir en los sistemas a su cargo opciones de desconexión o cierre de sesión de los aplicativos, que permitan terminar completamente con la sesión o conexión asociada, las cuales deben encontrarse disponibles en todas las páginas protegidas por autenticación.

 Universidad del Valle	Manual de Procedimientos	Código:	Versión: 1.0
		Página: 34 de 38	
Fecha de Emisión: 01/2019	Título: MANUAL POLITICAS SEGURIDAD DE LA INFORMACIÓN		
Elaborado por: OITEL	Revisado por: César Narváez	Aprobado por: Pablo Emilio Astroz	

- Los desarrolladores y proveedores deben incluir en los sistemas a su cargo funcionalidades que terminen la sesión en el sistema de información después de un lapso de tiempo de máximo 20 min de inactividad, que solo podrá ser aumentado con base en un análisis de riesgos aceptado por el área funcional.
- Los desarrolladores y proveedores deben asegurar el manejo de operaciones sensibles o críticas en los aplicativos desarrollados con base en un análisis de riesgos aceptado por el área funcional, incluyendo en los sistemas a su cargo el uso de dispositivos adicionales y el ingreso de parámetros adicionales de verificación.
- Los desarrolladores y proveedores deben asegurar que los aplicativos proporcionen la mínima información de la sesión establecida con o sin autenticación, almacenada en cookies, variables del lado del cliente y complementos, entre otros.
- Los desarrolladores y proveedores deben garantizar que no se divulgue información sensible en respuestas de error, incluyendo detalles del sistema, identificadores de sesión o información de las cuentas de usuarios; así mismo, deben implementar mensajes de error genéricos.
- Los desarrolladores y proveedores deben remover todas las funcionalidades y archivos que no sean necesarios para los aplicativos, previo a la puesta en producción.
- Los desarrolladores y proveedores deben prevenir la revelación de la estructura de directorios de los sistemas de información construidos.
- Los desarrolladores y proveedores deben remover información innecesaria en los encabezados de respuesta que se refieran a los sistemas operativos y versiones del software utilizado.
- Los desarrolladores y proveedores deben evitar incluir las cadenas de conexión a las bases de datos en el código de los aplicativos. Dichas cadenas de conexión deben estar en archivos de configuración independientes, los cuales se recomienda que estén cifrados.

 <u>Universidad del Valle</u>	Manual de Procedimientos	Código:	Versión: 1.0
		Página: 35 de 38	
Fecha de Emisión: 01/2019	Título: MANUAL POLITICAS SEGURIDAD DE LA INFORMACIÓN		
Elaborado por: OITEL	Revisado por: César Narváez	Aprobado por: Pablo Emilio Astroz	

- Los desarrolladores y proveedores deben garantizar el cierre de la conexión a las bases de datos desde los aplicativos tan pronto como estas no sean requeridas.
- Los desarrolladores y proveedores deben desarrollar los controles necesarios para la transferencia de archivos desde los sistemas de información, como exigir autenticación, vigilar los tipos de archivos a transmitir, almacenar los archivos transferidos en repositorios destinados para este fin o en bases de datos, eliminar privilegios de ejecución a los archivos transferidos y asegurar que dichos archivos solo tengan privilegios de lectura.
- Los desarrolladores y proveedores deben proteger el código fuente de los aplicativos construidos, de tal forma de que no pueda ser descargado ni modificado por los usuarios.
- Los desarrolladores y proveedores deben asegurar que no se permite que los aplicativos desarrollados ejecuten comandos directamente en el sistema operativo.

7.12 Relación con Proveedores

La Universidad del Valle, establecerá mecanismos de control en sus relaciones con proveedores, con el objetivo de asegurar que la información a la que tengan acceso o servicios que sean suministradas por las mismas, cumpla con las políticas, normas y procedimientos de seguridad de la información.

Las dependencias de la Universidad del Valle responsables de la realización de contratos o convenios con proveedores se asegurarán de la divulgación de las políticas, normas y procedimientos de seguridad de la información a dichos proveedores.

- La Oficina de Informática y Telecomunicaciones (OITEL), con apoyo de la Oficina Jurídica deben generar un modelo base para los Acuerdos de Niveles de Servicio y requisitos de Seguridad de la Información, con los que deben cumplir proveedores de servicios; dicho modelo, debe ser divulgado a todas las áreas que adquieran o supervisen recursos y/o servicios tecnológicos.

 Universidad del Valle	Manual de Procedimientos	Código:	Versión: 1.0
		Página: 36 de 38	
Fecha de Emisión: 01/2019	Título: MANUAL POLITICAS SEGURIDAD DE LA INFORMACIÓN		
Elaborado por: OITEL	Revisado por: César Narváez	Aprobado por: Pablo Emilio Astroz	

- La Oficina Jurídica debe elaborar modelos de Acuerdos de Confidencialidad, con los que deben cumplir proveedores de servicios; dichos modelos, deben ser divulgados a todas las áreas que adquieran o supervisen recursos y/o servicios tecnológicos. De dichos acuerdos deberá derivarse una responsabilidad tanto civil como penal para el proveedor contratado,
- La Oficina de Informática y Telecomunicaciones (OITEL), con apoyo de la Oficina Jurídica deben generar un modelo base para Acuerdos de Intercambio de Información con proveedores, con los que deben cumplir dicho proveedor; estos, deben ser divulgados a todas las áreas que adquieran o supervisen recursos y/o servicios tecnológicos.
- Todo sistema externo utilizado por los proveedores para acceder a la información de la Universidad del Valle, debe ser autorizado por los líderes de proceso como responsables funcionales de cada una de las dependencias de la Universidad del Valle con el apoyo técnico de la Oficina de Informática y Telecomunicaciones (OITEL).
- La Oficina de Informática y Telecomunicaciones (OITEL), debe establecer las condiciones de conexión adecuada para los equipos de cómputo y dispositivos móviles de los proveedores en la red de datos de la Universidad del Valle.
- La Oficina de Informática y Telecomunicaciones (OITEL), debe establecer las condiciones de comunicación segura, cifrado y transmisión de información desde y hacia los proveedores de servicios.
- Los líderes de proceso como responsables funcionales de cada una de las dependencias de la Universidad del Valle deben evaluar y aprobar los accesos a la información de la Universidad requeridos por terceras partes, con el apoyo técnico de la Oficina de Informática y Telecomunicaciones (OITEL).
- Las dependencias de la Universidad del Valle responsables de la realización de contratos o convenios con proveedores, deben identificar y monitorear los riesgos

 Universidad del Valle	Manual de Procedimientos	Código:	Versión: 1.0
		Página: 37 de 38	
Fecha de Emisión: 01/2019	Título: MANUAL POLITICAS SEGURIDAD DE LA INFORMACIÓN		
Elaborado por: OITEL	Revisado por: César Narváez	Aprobado por: Pablo Emilio Astroz	

relacionados con estos, haciendo extensiva esta actividad a la cadena de suministro de los servicios de tecnología.

- Las dependencias de la Universidad del Valle responsables de la realización de contratos o convenios con proveedores, deben mitigar los riesgos relacionados con dichos proveedores, que tengan acceso a información de la Universidad.
- Las dependencias de la Universidad del Valle responsables de la realización de contratos o convenios con proveedores, deben divulgar y asegurar el cumplimiento de las políticas, normas y procedimientos de seguridad de la información a dichos proveedores.
- los Supervisores de contratos con proveedores, deben monitorear periódicamente, el cumplimiento de los Acuerdos de Niveles de Servicio, Acuerdos de Confidencialidad, Acuerdos de Intercambio de información y los requisitos de Seguridad de la Información.
- Los Supervisores de contratos y las dependencias de la Universidad del Valle responsables de la realización de contratos o convenios con proveedores, deben administrar los cambios en el suministro de servicios por parte de los proveedores, manteniendo los niveles de cumplimiento de servicio y seguridad establecidos con ellos y monitoreando la aparición de nuevos riesgos.
- Cualquier actividad realizada por un proveedor en los sistemas de información y aplicativos que estén en la nube institucional académica y que estén bajo el control técnico de la OITEL, debe ser monitoreada por La Oficina de Informática y Telecomunicaciones (OITEL). En el caso que se identifiquen riesgos de seguridad sobre la información, inmediatamente será revocada su autorización.

7.13 Cumplimiento de Requisitos Legales y Contractuales

7.13.1 Privacidad y protección de información de datos personales

 Universidad del Valle	Manual de Procedimientos	Código:	Versión: 1.0
		Página: 38 de 38	
Fecha de Emisión: 01/2019	Título: MANUAL POLITICAS SEGURIDAD DE LA INFORMACIÓN		
Elaborado por: OITEL	Revisado por: César Narváez	Aprobado por: Pablo Emilio Astroz	

- La Universidad del Valle, quien será el responsable del tratamiento de los Datos Personales, tal y como este término se define en la Ley 1581 de 2012, respeta la privacidad de cada uno de los terceros que le suministren sus Datos Personales a través de los diferentes puntos de recolección y captura de dicha información.

7.13.2 Reglamentación de controles criptográficos

- La Oficina de Informática y Telecomunicaciones (OITEL), se registrará por la legislación vigente para el uso de controles criptográficos, según aplique.

7.14 Notificación de Incidentes de Seguridad de la Información

Toda violación de estas políticas se deberá notificar inmediatamente través de la cuenta **(POR DEFINIR)**, de modo que se pueda resolver debidamente el asunto. Se busca asegurar que todos comprendan y respeten las políticas con el fin de reducir al mínimo el riesgo, protegiendo a todas las personas, así como a la Oficina de Informática y Telecomunicaciones (OITEL).

Se deberán notificar situaciones tales como: personas ajenas a la Oficina de Informática y Telecomunicaciones (OITEL) en centros de cómputo, correos con virus, reinicio de los equipos de cómputo o enrutadores, mala utilización de recursos, uso ilegal del software, mal uso de información corporativa, alteración de información, entre otros.

- La administración de todos los recursos que no estén bajo el control técnico de la OITEL, deben acogerse a todas las políticas definidas en este documento.



Contenido

INFORMACIÓN DE LOS RESPONSABLES	2
1. INTRODUCCIÓN	2
2. OBJETIVOS	2
3. ANTECEDENTES	3
4. ÁMBITO DE APLICACIÓN	3
5. POLÍTICA DE BORRADO SEGURO DE INFORMACIÓN	4
6. DEFINICIONES	5
7. CONTROL DE CAMBIOS	6
8. ANEXOS	6
9. INCUMPLIMIENTO	6

INFORMACIÓN DE LOS RESPONSABLES

ROL	NOMBRE	CARGO	FECHA	FIRMA
Elaboración	César Augusto Narvaez Barco	Coordinador de Infraestructura	25/08/2021	
Revisión	Laura Sofía Rodríguez Pulecio	Directora OITEL	02/09/2021	
Aprobación	Laura Sofía Rodríguez Pulecio	Directora OITEL	08/09/2021	

1. INTRODUCCIÓN

La Universidad del Valle, entidad pública identificada con el NIT 890399010-6, cuyo domicilio principal es en la ciudad de Santiago de Cali en la dirección, Calle 13 # 100-00, en condición de responsable del tratamiento de datos personales, se permite informar por medio de la presente política, lo relacionado con la información personal que recolectamos de nuestros estudiantes, aspirantes, graduados, egresados, proveedores, funcionarios, docentes, empleados, trabajadores oficiales, jubilados, pensionados, contratistas, comunidad en general, el tipo de tratamiento que le damos y las finalidades del mismo.

2. OBJETIVOS

- Definir los lineamientos para eliminar de forma segura la información de la Universidad del Valle o de cualquier otro tercero bajo su responsabilidad que tenga carácter confidencial, garantizando los niveles de seguridad de la misma y poder minimizar el riesgo de que a través de basura, dispositivos o software se pueda recuperar información confidencial que sobre estos medios se haya podido grabar.
- Dar cumplimiento a los lineamientos estipulados en el control **A.8.3.2 – Eliminación de Soportes** de la norma **ISO/IEC 27001:2013**.

3. ANTECEDENTES

La Universidad del Valle reconoce la información como un activo vital para la institución. La protección y seguridad de esta información tiene una importancia primordial en muchos aspectos de su entorno. Así, para disminuir los riesgos y proteger la información, es necesario que estén implementados un conjunto de controles y procedimientos para mantener y mejorar los niveles de seguridad de la información, independientemente de la forma en la que ésta es manejada, procesada, transportada o almacenada.

Este documento describe las políticas de Borrado Seguro de Información, para prevenir el acceso no autorizado a información que se encuentra en equipos que vayan a ser trasladados, dados de baja, o que, por sus características, sea constantemente transportado y que pueden contener información confidencial susceptible de ser recuperada por terceros.

4. ÁMBITO DE APLICACIÓN

La Universidad del Valle, de acuerdo con los principios y reglas establecidas en el Régimen General de Protección de Datos Personales, ha desarrollado la presente Política para el tratamiento de los datos personales y así garantizar los derechos de los titulares de información personal.

Este documento, contiene parámetros de autorregulación que permitirán que el tratamiento que efectuamos en sus datos personales respete todos los derechos y garantías que indica la Ley 1581 del 2012 y los Decretos Reglamentarios 1377 del 2013 y 886 del 2014 – hoy contenidos en los capítulos 25 y 26 del Decreto Único Reglamentario 1074 del 2015 del Sector Comercio, Industria y Turismo, y demás normas que desarrollaran el marco general de protección de datos en Colombia.



5. POLÍTICA DE BORRADO SEGURO DE INFORMACIÓN

- 5.1.** Deberá existir una solicitud formal indicando los medios o información a destruir dirigida al propietario del activo. La solicitud debe identificar en forma unívoca al medio o la información que requiere destrucción.
- 5.2.** El responsable de la información debe revisar que se hayan realizado las copias de seguridad, las pruebas y el borrado seguro de la información.
- 5.3.** En cada proceso de destrucción se debe generar un reporte de actuación que identifique al personal actuante y la metodología empleada para la destrucción de la información, así como las observaciones que éste considere pertinente. Se deberá identificar claramente que el proceso se ha efectuado.
- 5.4.** Cuando se haya dado la autorización por el responsable de la información, el área responsable debe realizar un borrado de la información dependiendo del medio en que reposa; para cumplir con este requerimiento se pueden utilizar cualquiera de los siguientes métodos según sea conveniente.
 - **Desmagnetización:** La desmagnetización consiste en la exposición de los soportes de almacenamiento a un potente campo magnético, proceso que elimina los datos almacenados en el dispositivo. Este método es válido para la destrucción de datos de los dispositivos magnéticos.
 - **Destrucción Física:** El objetivo de la destrucción física es la inutilización del soporte que almacena la información en el dispositivo para evitar la recuperación posterior de los datos que almacena.
 - **Desintegración, pulverización, fusión e incineración:** son métodos diseñados para destruir por completo los medios de almacenamiento. Estos métodos suelen llevarse a cabo en una destructora de metal o en una planta de incineración autorizada, con las capacidades específicas para realizar estas actividades de manera eficaz, segura y sin peligro.
 - **Trituración:** las trituradoras de papel se pueden utilizar para destruir los medios de almacenamiento flexibles. El tamaño del fragmento de la basura debe ser lo suficientemente pequeño para que haya una seguridad razonable en proporción a la confidencialidad de los datos que no pueden ser reconstruidos. Los medios ópticos de almacenamiento (CD, DVD, magneto-ópticos), deben ser destruidos por pulverización, trituración de corte transversal o incineración.



- **Sobre-escritura:** La sobre-escritura consiste en la escritura de un patrón de datos sobre los datos contenidos en los dispositivos de almacenamiento. Para asegurar la completa destrucción de los datos se debe escribir la totalidad de la superficie de almacenamiento, para dispositivos electrónicos se debe utilizar un software que efectúe borrado a bajo nivel, guardando los registros como evidencia de la destrucción de la información.

5.5. Para la disposición de los documentos físicos se debe seguir los lineamientos de Gestión Documental.

6. DEFINICIONES

Para mejor comprensión de la presente política, se definen los siguientes conceptos generales:

- a) Activo de información:** Cualquier componente (humano, tecnológico, software, documental o de infraestructura) que soporta uno o más procesos de negocios de la Entidad y, en consecuencia, debe ser protegido.
- b) Control:** es toda actividad o proceso encaminado a mitigar o evitar un riesgo. Incluye políticas, procedimientos, guías, estructuras organizacionales y buenas prácticas, que pueden ser de carácter administrativo, tecnológico, físico o legal.
- c) Custodio del activo de información:** es la unidad organizacional o proceso, designado por los propietarios, encargado de mantener las medidas de protección establecidas sobre los activos de información confiados.
- d) Confidencialidad:** es la garantía de que la información no está disponible o divulgada a personas, entidades o procesos no autorizados.
- e) Integridad:** es la protección de la exactitud y estado completo de los activos.
- f) Disponibilidad:** es la garantía de que los usuarios autorizados tienen acceso a la información y a los activos asociados cuando lo requieren.

- g) **Inventario de activos de información:** es una lista ordenada y documentada de los activos de información pertenecientes a la Entidad.
- h) **Propietario de la información:** es la unidad organizacional o proceso donde se crean los activos de información.
- i) **Recursos tecnológicos:** son aquellos componentes de hardware y software tales como: servidores (de aplicaciones y de servicios de red), estaciones de trabajo, equipos portátiles, dispositivos de comunicaciones y de seguridad, servicios de red de datos y bases de datos, entre otros, los cuales tienen como finalidad apoyar las tareas administrativas necesarias para el buen funcionamiento y la optimización del trabajo al interior de la Superintendencia Nacional de Salud.
- j) **Responsable por el activo de información:** es la persona o grupo de personas, designadas por los propietarios, encargados de velar por la confidencialidad, la integridad y disponibilidad de los activos de información y decidir la forma de usar, identificar, clasificar y proteger dichos activos a su cargo.

7. CONTROL DE CAMBIOS

FECHA	VERSIÓN	DESCRIPCIÓN DEL CAMBIO
08/09/2021	1.0	Versión original

8. ANEXOS

9. INCUMPLIMIENTO

El incumplimiento a la política de Seguridad y Privacidad de la Información, traerá consigo, las consecuencias legales que apliquen a la normativa de la Entidad,

 Universidad del Valle	POLÍTICA DE BORRADO SEGURO DE INFORMACIÓN UNIVERSIDAD DEL VALLE		
	Versión 1.0	2021090801	08/09/2021

incluyendo lo establecido en las normas que competen al Gobierno nacional y territorial en cuanto a Seguridad y Privacidad de la Información se refiere.

Fin de la política.

COPIA NO CONTROLADA



Contenido

INFORMACIÓN DE LOS RESPONSABLES	2
1. INTRODUCCIÓN	2
2. OBJETIVOS	2
3. ANTECEDENTES	2
4. ÁMBITO DE APLICACIÓN	3
5. POLÍTICA DE ESCRITORIO LIMPIO Y PANTALLA LIMPIA	3
6. DEFINICIONES	4
7. CONTROL DE CAMBIOS	6
8. ANEXOS	6
9. INCUMPLIMIENTO	6

INFORMACIÓN DE LOS RESPONSABLES

ROL	NOMBRE	CARGO	FECHA	FIRMA
Elaboración				
Revisión				
Aprobación				

1. INTRODUCCIÓN

La Universidad del Valle, entidad pública identificada con el NIT 890399010-6, cuyo domicilio principal es en la ciudad de Santiago de Cali en la dirección, Calle 13 # 100-00, en condición de responsable del tratamiento de datos personales, se permite informar por medio de la presente política, lo relacionado con la información personal que recolectamos de nuestros estudiantes, aspirantes, graduados, egresados, proveedores, funcionarios, docentes, empleados, trabajadores oficiales, jubilados, pensionados, contratistas, comunidad en general, el tipo de tratamiento que le damos y las finalidades del mismo.

2. OBJETIVOS

Establecer la política de Escritorio y Pantalla Limpia para prevenir el acceso no autorizado, pérdida y/o daño de la información que se encuentra en los puestos de trabajo, equipos de cómputo, medios extraíbles, dispositivos de impresión y digitalización de documentos, durante y fuera del horario laboral.

3. ANTECEDENTES

La Universidad del Valle reconoce la información como un activo vital para la institución. La protección y seguridad de esta información tiene una importancia primordial en muchos aspectos de su entorno. Así, para disminuir los riesgos y proteger la información, es necesario que estén implementados un conjunto de controles y procedimientos para mantener y mejorar los niveles de seguridad de la información, independientemente de la forma en la que ésta es manejada, procesada, transportada o almacenada.

Este documento describe las políticas de Escritorio y Pantalla Limpia para prevenir el acceso no autorizado, pérdida y/o daño de la información que se encuentra en los puestos de trabajo, equipos de cómputo, medios extraíbles, dispositivos de impresión y digitalización de documentos, durante y fuera del horario laboral, tomando como base el control **A.11.2.9 - Política de puesto de trabajo despejado y pantalla limpia** de la norma **ISO/IEC 27001:2013**.

4. ÁMBITO DE APLICACIÓN

La Universidad del Valle, de acuerdo con los principios y reglas establecidas en el Régimen General de Protección de Datos Personales, ha desarrollado la presente Política para el tratamiento de los datos personales y así garantizar los derechos de los titulares de información personal.

Este documento, contiene parámetros de autorregulación que permitirán que el tratamiento que efectuamos en sus datos personales respete todos los derechos y garantías que indica la Ley 1581 del 2012 y los Decretos Reglamentarios 1377 del 2013 y 886 del 2014 – hoy contenidos en los capítulos 25 y 26 del Decreto Único Reglamentario 1074 del 2015 del Sector Comercio, Industria y Turismo, y demás normas que desarrollaran el marco general de protección de datos en Colombia.

5. POLÍTICA DE ESCRITORIO LIMPIO Y PANTALLA LIMPIA

- 5.1.** Todos los estudiantes, docentes, trabajadores, funcionarios, contratistas, proveedores, jubilados, pensionados y comunidad en general deben mantener la información restringida o confidencial bajo llave cuando sus



puestos de trabajo se encuentren desatendidos o en horas no laborales. Esto incluye: documentos impresos, CDs, dispositivos de almacenamiento USB y medios removibles en general. Adicionalmente, se requiere que la información sensible que se envía a las impresoras sea recogida de manera inmediata.

- 5.2.** Todos los estudiantes, docentes, trabajadores, funcionarios, contratistas, proveedores, jubilados, pensionados y comunidad en general son responsables de bloquear la sesión de su estación de trabajo en el momento en que se retiren del puesto de trabajo, la cual se podrá desbloquear sólo con la contraseña del usuario o huella dactilar en las estaciones de trabajo que soporten dicho sistema. Cuando finalicen sus actividades, se deben cerrar todas las aplicaciones y dejar los equipos apagados.
- 5.3.** La información clasificada como altamente confidencial no debe ser nunca enviada a una impresora de la red, sin que exista una persona autorizada para cuidarla durante y después de la impresión. La variedad de la información que se envía a las impresoras puede alternar entre información pública e información confidencial, dado que información confidencial no puede ser revelada a personas no autorizadas. Así mismo, cuando los documentos sean impresos, éstos deben retirarse inmediatamente de dichos dispositivos.
- 5.4.** La pantalla del computador (escritorio lógico) debe estar libre de información sensible o confidencial.
- 5.5.** Los puestos de trabajo deben permanecer limpios y ordenados
- 5.6.** Los dispositivos de impresión y digitalización deben permanecer limpios de documentos.
- 5.7.** Todos los equipos de cómputo y dispositivos portátiles deberán tener aplicado el bloqueo de sesión por inactividad, definido por el equipo de seguridad de la información.

6. DEFINICIONES

 Universidad del Valle	POLÍTICA DE ESCRITORIO LIMPIO Y PANTALLA LIMPIA UNIVERSIDAD DEL VALLE		
Versión 1.0	(código)	(fecha)	

Para mejor comprensión de la presente política, se definen los siguientes conceptos generales:

- a) **Dato biométrico:** son aquellos datos personales que informan sobre determinados aspectos físicos que, mediante un análisis técnico, permiten distinguir las singularidades que identifican a una persona. Estos se dividen en datos i) biométricos fisiológicos, que son aquellos derivados de la medida de una parte de la anatomía de una persona; por ejemplo: la huella dactilar, rostro, retina; y ii) los datos biométricos del comportamiento, como son la voz, o la firma.
- b) **Dato personal o información personal:** cualquier información que, de manera individual o vinculada, permita determinar, identificar o asociarse a una o varias personas naturales determinadas o determinables.
- c) **Dato privado:** es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular de la información personal.
- d) **Dato público:** es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva.
- e) **Dato semiprivado:** es aquel que no tiene naturaleza íntima, reservada, ni pública y cuyo conocimiento o divulgación puede interesar no sólo al titular sino a cierto sector o grupo de personas o a la sociedad en general, como el dato financiero y crediticio de actividad comercial o de servicios.
- f) **Dato sensible:** se entiende por datos sensibles aquellos que afectan la intimidad del titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de Partidos políticos de oposición así como los datos relativos a la salud, a la vida sexual y los datos biométricos, entre otros, la captura de imagen fija o en movimiento, huellas digitales, fotografías, iris, reconocimiento de voz, facial o de palma de mano, etc.



- g) **Medio Extraíble:** Dispositivo que permite almacenar o transportar información como memorias USB, tarjetas de memoria, cintas magnéticas, CD, DVD, discos duros externos.
- h) **Puesto de Trabajo:** Lugar dispuesto para que los funcionarios o contratistas realicen las labores relacionadas con las funciones o el cumplimiento de las obligaciones contractuales, según el caso.
- i) **Escritorio Lógico:** Es la interfaz de software con la que interactúa el usuario al trabajar con una computadora.

7. CONTROL DE CAMBIOS

FECHA	VERSIÓN	DESCRIPCIÓN DEL CAMBIO

8. ANEXOS

9. INCUMPLIMIENTO

El incumplimiento a la política de Seguridad y Privacidad de la Información, traerá consigo, las consecuencias legales que apliquen a la normativa de la Entidad, incluyendo lo establecido en las normas que competen al Gobierno nacional y territorial en cuanto a Seguridad y Privacidad de la Información se refiere.

Fin de la política.



Contenido

1. INTRODUCCION	2
2. CONSIDERACIONES PREVIAS	2
3. DEFINICIONES	3
4. ÁMBITO DE APLICACIÓN	4
5. POLÍTICA DE USO DE DISPOSITIVOS MÓVILES	4

COPIA NO CONTROLADA

1. INTRODUCCION

La Universidad del Valle, entidad pública identificada con el NIT 890399010-6, cuyo domicilio principal es en la ciudad de Santiago de Cali en la dirección, Calle 13 # 100-00, en condición de responsable del tratamiento de datos personales, se permite informar por medio de la presente política, lo relacionado con la información personal que recolectamos de nuestros estudiantes, aspirantes, graduados, egresados, proveedores, funcionarios, docentes, empleados, trabajadores oficiales, jubilados, pensionados, contratistas, comunidad en general, el tipo de tratamiento que le damos y las finalidades del mismo.

2. CONSIDERACIONES PREVIAS

La Universidad del Valle reconoce la información como activo vital para la institución. La protección y seguridad de esta información tiene una importancia primordial en muchos aspectos de su entorno. Así, para disminuir los riesgos y proteger la información, es necesario que estén implementadas un conjunto de controles y procedimientos para mantener y mejorar los niveles de seguridad de la información, independientemente de la forma en la que ésta es manejada, procesada, transportada o almacenada.

Este documento describe las políticas de Borrado Seguro de Información, para prevenir el acceso no autorizado a información que se encuentra en equipos que vayan a ser trasladados, dados de baja, o que, por sus características, sea constantemente transportado y que pueden contener información confidencial susceptible de ser recuperada por terceros.

Esta política da cumplimiento a los lineamientos estipulados en el control **A.6.2.1 –Política de dispositivos móviles** de la norma **ISO/IEC 27001:2013**.

 Universidad del Valle	BORRADOR POLÍTICA DE USO DE DISPOSITIVOS MÓVILES UNIVERSIDAD DEL VALLE		
	Versión 1.0		

3. DEFINICIONES

Para mejor comprensión de la presente política, se definen los siguientes conceptos generales:

- a) **Activo de información:** Cualquier componente (humano, tecnológico, software, documental o de infraestructura) que soporta uno o más procesos de negocios de la Entidad y, en consecuencia, debe ser protegido.
- b) **Control:** es toda actividad o proceso encaminado a mitigar o evitar un riesgo. Incluye políticas, procedimientos, guías, estructuras organizacionales y buenas prácticas, que pueden ser de carácter administrativo, tecnológico, físico o legal.
- c) **Custodio del activo de información:** es la unidad organizacional o proceso, designado por los propietarios, encargado de mantener las medidas de protección establecidas sobre los activos de información confiados.
- d) **Confidencialidad:** es la garantía de que la información no está disponible o divulgada a personas, entidades o procesos no autorizados.
- e) **Integridad:** es la protección de la exactitud y estado completo de los activos.
- f) **Disponibilidad:** es la garantía de que los usuarios autorizados tienen acceso a la información y a los activos asociados cuando lo requieren.
- g) **Inventario de activos de información:** es una lista ordenada y documentada de los activos de información pertenecientes a la Entidad.
- h) **Propietario de la información:** es la unidad organizacional o proceso donde se crean los activos de información.
- i) **Recursos tecnológicos:** son aquellos componentes de hardware y software tales como: servidores (de aplicaciones y de servicios de red), estaciones de trabajo, equipos portátiles, dispositivos de comunicaciones y de seguridad, servicios de red de datos y bases de datos, entre otros, los cuales tienen como finalidad apoyar las tareas administrativas necesarias para el buen funcionamiento y la

optimización del trabajo al interior de la Superintendencia Nacional de Salud.

- j) Responsable por el activo de información: es la persona o grupo de personas, designadas por los propietarios, encargados de velar por la confidencialidad, la integridad y disponibilidad de los activos de información y decidir la forma de usar, identificar, clasificar y proteger dichos activos a su cargo.

4. ÁMBITO DE APLICACIÓN

La Universidad del Valle, de acuerdo con los principios y reglas establecidas en el Régimen General de Protección de Datos Personales, ha desarrollado la presente Política para el tratamiento de los datos personales y así garantizar los derechos de los titulares de información personal.

Este documento, contiene parámetros de autorregulación que permitirán que el tratamiento que efectuamos en sus datos personales respete todos los derechos y garantías que indica la Ley 1581 del 2012 y los Decretos Reglamentarios 1377 del 2013 y 886 del 2014 – hoy contenidos en los capítulos 25 y 26 del Decreto Único Reglamentario 1074 del 2015 del Sector Comercio, Industria y Turismo, y demás normas que desarrollaran el marco general de protección de datos en Colombia.

5. POLÍTICA DE USO DE DISPOSITIVOS MÓVILES

La Oficina de Informática y Telecomunicaciones (OITEL), proveerá las condiciones para el manejo de los dispositivos móviles (teléfonos inteligentes y tabletas, entre otros) siempre y cuando estén bajo el control de la misma, que hagan uso de servicios de la Universidad del Valle y que hagan parte del inventario de la Universidad. Así mismo, velará porque los funcionarios hagan un uso responsable de los servicios y equipos proporcionados por la misma.

- La Oficina de Informática y Telecomunicaciones (OITEL) establece los lineamientos aceptables para los dispositivos móviles institucionales que hagan uso de los servicios entregados por la Universidad del Valle que son:



- Los funcionarios deben de aplicar el método de bloqueo recomendado por la OITEL, para la protección de los dispositivos móviles institucionales que serán entregados a los funcionarios. Se debe configurar estos dispositivos para que pasado un tiempo de inactividad pasen automáticamente a modo de suspensión y, en consecuencia, se active el bloqueo de la pantalla el cual requerirá el método de desbloqueo por usuario y contraseña.
- Los funcionarios deben activar la opción de cifrado en los dispositivos móviles institucionales haciendo imposible la copia o extracción de datos si no se conoce el método de desbloqueo.
- Los funcionarios deben evitar usar los dispositivos móviles institucionales en lugares que no les ofrezcan las garantías de seguridad física necesarias para evitar pérdida o robo de estos.
- Los funcionarios no deben modificar las configuraciones de seguridad de los dispositivos móviles institucionales bajo su responsabilidad, ni desinstalar el software provisto con ellos al momento de su entrega.
- Los funcionarios deben evitar la instalación de programas desde fuentes desconocidas; se deben instalar aplicaciones únicamente desde los repositorios oficiales de los dispositivos móviles institucionales.
- Los funcionarios deben evitar hacer uso de redes inalámbricas de uso público.
- Los usuarios deben evitar conectar los dispositivos móviles institucionales asignados por puerto USB a cualquier computador público, de hoteles o cafés internet, entre otros.

Los funcionarios no deben almacenar videos, fotografías o información personal en los dispositivos móviles institucionales asignados.

 Universidad del Valle	POLÍTICA DE USO DE CORREO ELECTRÓNICO UNIVERSIDAD DEL VALLE		
	Versión 2.0	(código)	2022/05/26

Contenido

1.	INFORMACIÓN DE LOS RESPONSABLES	2
2.	INTRODUCCIÓN	2
3.	OBJETIVOS	2
4.	ANTECEDENTES	3
5.	ALCANCE	3
6.	POLÍTICA DE USO Y GESTIÓN DEL CORREO ELECTRÓNICO	3
6.1.	Política general de uso para cuentas institucionales	4
6.2.	Política particular de uso para cuentas estudiantiles	6
6.3.	Política particular de uso para cuentas de egresados	7
6.4.	Política particular de uso para cuentas temporales e institucionales	7
6.5.	Condiciones Generales de Uso	8
6.6.	Creación de cuentas de correo.	8
7.	CONTROL DE CAMBIOS	11
8.	INCUMPLIMIENTO	11

 Universidad del Valle	POLÍTICA DE USO DE CORREO ELECTRÓNICO UNIVERSIDAD DEL VALLE		
	Versión 2.0	(código)	2022/05/26

1. INFORMACIÓN DE LOS RESPONSABLES

ROL	NOMBRE	CARGO	FECHA	FIRMA
Elaboración	Nelson Vidales	Administrador de correo	26/05/2022	
	César Narváez	Coordinador de área		
Revisión	Fernando Prieto	Web Manager	1/06/2022	
Aprobación	William Sánchez	Director		

2. INTRODUCCIÓN

El correo electrónico institucional, los servicios y todas las herramientas colaborativas integradas al mismo, son asignados a los miembros de la comunidad universitaria como medio institucional de comunicación.

Esta política define los lineamientos que deben ser tenidos en cuenta por la comunidad universitaria, en la creación, uso y eliminación de los correos electrónicos en la Universidad del Valle.

3. OBJETIVOS

Establecer los lineamientos y el uso aceptable para las cuentas correo electrónico institucionales, los servicios y las herramientas asociadas, con el objetivo de salvaguardar la disponibilidad, integridad y confidencialidad de la información de la Universidad del Valle, además de velar por el buen uso de los recursos institucionales.

 Universidad del Valle	POLÍTICA DE USO DE CORREO ELECTRÓNICO UNIVERSIDAD DEL VALLE		
	Versión 2.0	(código)	2022/05/26

4. ANTECEDENTES

La Universidad del Valle reconoce la información como un activo fundamental para la institución. La protección y seguridad de esta información tiene una importancia primordial en muchos aspectos de su entorno. Así, para disminuir los riesgos y proteger la información, es necesario que estén implementados un conjunto de controles y procedimientos para mantener y mejorar los niveles de seguridad de la información, independientemente de la forma en la que ésta es manejada, procesada, transportada o almacenada.

Este documento describe las políticas y normas para el uso del correo electrónico institucional, tomando como base el Manual de Seguridad de la Información de la Universidad del Valle, las leyes y demás regulaciones aplicables vigentes, la norma ISO/IEC 27001:2013 y las recomendaciones del estándar ISO/IEC 27002:2013.

Esta política da cumplimiento a los lineamientos estipulados en el control **A.13.2 – Transferencia de Información**, particularmente el control **A.13.2.3 – Mensajes Electrónicos** de la norma **ISO/IEC 27001:2013**.

5. ALCANCE

Esta política aplica para todos los integrantes de la comunidad universitaria que tenga asignado un correo electrónico institucional para el apoyo a la realización de sus funciones académicas, administrativas y de investigación.

6. POLÍTICA DE USO Y GESTIÓN DEL CORREO ELECTRÓNICO

Según sea el caso, se deben cumplir las siguientes políticas y condiciones generales.

 Universidad del Valle	POLÍTICA DE USO DE CORREO ELECTRÓNICO UNIVERSIDAD DEL VALLE		
	Versión 2.0	(código)	2022/05/26

6.1. Política general de uso para cuentas institucionales

- 6.1.1.** Las cuentas creadas para estudiantes, docentes y empleados tienen la siguiente sintaxis: @correounivalle.edu.co. El nombre del usuario se crea de forma automática por el sistema de información de la universidad, siguiendo el formato a continuación: primer nombre + punto + primer apellido; siempre reemplazando los caracteres con tildes por los mismos caracteres sin tilde y la ñ por la letra n. En el caso de homónimos, el Sistema realizará combinación empleando segundo nombre y/o segundo apellido.
- 6.1.2.** El nombre de usuario de la cuenta de correo depende de la información que se encuentre registrada en las fuentes de autoridad de la Universidad del Valle (Registro Académico para estudiantes, Recursos Humanos para docentes y empleados). En caso de que el usuario haya cambiado su nombre, este cambio debe ser reportado a la fuente de autoridad, para poder realizar el cambio correspondiente en el correo electrónico.
- 6.1.3.** Las cuentas de Google Workspace for Education son un recurso tecnológico a disposición de la Comunidad Universitaria para la gestión administrativa, académica de formación e investigación.
- 6.1.4.** Los servicios o cualquier herramienta adicional disponible de Google Workspace for Education para usuarios finales, deben ser utilizados únicamente con fines educativos autorizados por la institución y evitarse su uso para tratar asuntos personales.
- 6.1.5.** El uso de la cuenta de correo electrónico de Google Workspace for Education es obligatorio para el envío y recepción de comunicaciones a nivel Institucional, para la realización de trámites internos que requieran del uso de este medio y para interacción con los Sistemas de Información Institucionales.
- 6.1.6.** La Universidad se reserva el derecho de suspender o cancelar el uso de la cuenta de Google Workspace for Education asignada al usuario, en cualquier momento, sin necesidad de aviso previo.

 Universidad del Valle	POLÍTICA DE USO DE CORREO ELECTRÓNICO UNIVERSIDAD DEL VALLE		
	Versión 2.0	(código)	2022/05/26

- 6.1.7.** La información enviada a través de los servicios de las cuentas institucionales está regida por la Política de Protección de Datos Personales de la universidad del valle, y las [Condiciones de Uso y Política de Privacidad de Google](#), de la Ley de Protección de Datos Personales de la República de Colombia (Ley 1581 de 2012) y otras normativas relacionadas.
- 6.1.8.** La Universidad se reserva el derecho de deshabilitar, modificar o eliminar las cuentas institucionales, en las cuales se evidencie un uso inadecuado o que incurran en el incumplimiento de las políticas y condiciones plasmadas en el presente documento [Privacidad y Términos definidos por Google Workspace](#)
- 6.1.9.** Por medio del Correo electrónico o cualquiera de los servicios de Google Workspace for Education no está permitido publicar, compartir, enviar o retransmitir mensajes que puedan constituir acoso, considerado difamatorio, explícitamente sexual o que pueda ofender a alguien con base en su raza, género, nacionalidad, orientación sexual, religión, política o discapacidad, como tampoco abrir correos que provengan de destinatarios desconocidos o que tengan asuntos o archivos adjuntos sospechosos.
- 6.1.10.** El servicio ofrecido a través de Google Workspace for Education cuenta con diferentes medidas de seguridad que deben ser tenidas en cuenta y configuradas por los usuarios (correo alterno de recuperación, doble factor de autenticación, registro de número telefónico, etc.). Estos métodos permitirán al usuario enterarse inmediatamente, si se presenta actividad inusual en la cuenta. Si llega a presentarse tal situación, cambie inmediatamente la contraseña y reporte la eventualidad a la OITEL.
- 6.1.11.** Está prohibido el usar la cuenta de correo electrónico institucional o cualquiera de los servicios de Google Workspace for Education con propósitos diferentes a los contractuales, académicos o de comunicación con la institución, según sea el caso.
- 6.1.12.** La información contenida en el correo electrónico institucional o en cualquiera de los servicios de Google Workspace for Education asignado por la Universidad para el cumplimiento de sus responsabilidades académicas, administrativas y de investigación, son de propiedad de la Universidad y

 Universidad del Valle	POLÍTICA DE USO DE CORREO ELECTRÓNICO UNIVERSIDAD DEL VALLE		
	Versión 2.0	(código)	2022/05/26

podrán ser revisadas en el momento en que la institución lo determine, de acuerdo lo establecido en la RESOLUCIÓN No. 2.224 de junio 28 de 2019 “Por medio de la cual se adopta La Política de Tratamiento de Información y Protección de Datos Personales de la Universidad del Valle”.

6.1.13. Los mensajes de correo electrónico revisten la misma fuerza probatoria que tienen los documentos físicos, según lo establecido por artículo 10 de la ley 527 de 1999, el cual indica que Los mensajes de datos serán admisibles como medios de prueba y su fuerza probatoria es la otorgada en las disposiciones del Código de Procedimiento Civil, hoy Código General del Proceso.

6.1.14. Se prohíbe copiar o reenviar correos electrónicos que se encuentren clasificados como CONFIDENCIALES, CON RESERVA o PRIVADOS en el asunto del mensaje, sin tener la autorización del remitente.

6.1.15. Se prohíbe copiar, descargar, compartir o imprimir documentos digitales almacenados en Google Workspace for Education que se encuentren clasificados como CONFIDENCIALES, CON RESERVA o PRIVADOS, sin tener la autorización del remitente.

6.2. Política particular de uso para cuentas estudiantiles

6.2.1. Después de 12 meses sin realizar Matrícula Académica, el estudiante será considerado inactivo y perderá el acceso a la cuenta de Google Workspace for Education asignada por la Universidad.

6.2.2. Las cuentas de egresados se conservarán hasta por seis (6) meses después del grado, con el fin de que el usuario tenga el tiempo suficiente para hacer una copia de seguridad de su información. Pasado este tiempo, la cuenta de correo será migrada al dominio **egresadosunivalle.edu.co**, y debe usada únicamente para mantener comunicación con la Universidad del Valle.

 Universidad del Valle	POLÍTICA DE USO DE CORREO ELECTRÓNICO UNIVERSIDAD DEL VALLE		
	Versión 2.0	(código)	2022/05/26

6.3. Política particular de uso para cuentas de egresados

- 6.3.1. Después de seis (6) meses del grado, la cuenta estudiantil será trasladada al dominio @egresadosunivalle.edu.co. No se trasladará información contenida en el drive o en fotos.
- 6.3.2. La cuenta de correo electrónico de egresado se mantendrá única y exclusivamente para mantener comunicación con la Institución. En ese orden de ideas, está prohibido su uso para fines personales o comerciales
- 6.3.3. La capacidad de almacenamiento de las cuentas de egresado será de 1 GB

6.4. Política particular de uso para cuentas temporales e institucionales

- 6.4.1. Las cuentas de correo pertenecientes a dependencias y/o eventos, solo deben ser utilizadas por la persona a quien designe el jefe de la dependencia responsable de dicha cuenta.
- 6.4.2. El nombre de usuario (login) de las cuentas de correo creadas para el apoyo a las actividades de contratistas administrativos, no estará relacionado con el nombre del contratista sino con el nombre de la dependencia o proceso que apoya el contratista. Por ejemplo: contratista.soprote@correounivalle.edu.co
- 6.4.3. Los nombres de usuario (login) de las cuentas de correo creadas para el apoyo a las actividades de docentes contratistas (hora cátedra), serán creados empleando el mismo criterio de creación de las cuentas de correo institucionales para estudiantes y empleados.
- 6.4.4. Las cuentas de jubilados y pensionados se conservarán hasta por seis (6) meses después de la jubilación, con el fin de que el usuario tenga el tiempo suficiente para hacer una copia de seguridad de su información

 Universidad del Valle	POLÍTICA DE USO DE CORREO ELECTRÓNICO UNIVERSIDAD DEL VALLE		
	Versión 2.0	(código)	2022/05/26

6.5. Condiciones Generales de Uso

- 6.5.1. El titular de la cuenta debe realizar copias de respaldo de la información almacenada en su cuenta de correo electrónico. [Más información sobre cómo descargar tus datos en un archivo.](#)
- 6.5.2. De acuerdo a las políticas de Google Workspace for Education, cada cuenta de correo tiene una capacidad de almacenamiento de 20 GB compartidos entre los servicios de correo, Google Fotos y Google Drive.
- 6.5.3. Cada facultad o dependencia de la Universidad del Valle deberá notificar la finalización de contrato (prestación de servicios, docente hora cátedra, funcionario nombrado, trabajador oficial, etc.) o el cierre del proyecto o evento, a la OITEL, dentro de los quince (15) días hábiles posteriores a la finalización del evento.
- 6.5.4. Se debe revisar y depurar periódicamente la bandeja de entrada o de mensajes recibidos.
- 6.5.5. Es necesario eliminar o depurar los mensajes que no se requieran conservar, dado el caso de que se requiera conservar dichos mensajes, se deben crear etiquetas o carpetas para su almacenamiento.
- 6.5.6. Se debe depurar la bandeja de mensajes eliminados periódicamente.
- 6.5.7. Las unidades compartidas deben ser solicitadas mediante correo electrónico a usuarios@correounivalle.edu.co. La capacidad de almacenamiento de cada unidad compartida es de 20 GB.

6.6. Creación de cuentas de correo.

6.6.1. Estudiantes.

- La creación y notificación de cuentas de institucional en la plataforma en la nube de Google Workspace for Education para estudiantes nuevos, se llevará a cabo según el calendario académico de la División de Admisiones y Registro Académico.
- El área de Registro Académico envía a través de SIRA la solicitud para creación de nuevas cuentas de correo. La OITEL tendrá un tiempo aproximado de quince (15) días hábiles para realizar la creación las cuentas y la notificación a los estudiantes.

 Universidad del Valle	POLÍTICA DE USO DE CORREO ELECTRÓNICO UNIVERSIDAD DEL VALLE		
	Versión 2.0	(código)	2022/05/26

- Una vez creada la cuenta de correo institucional, las credenciales de ingreso serán enviadas a la cuenta de correo personal que haya sido registrada por el estudiante en el proceso de admisión.

6.6.2. Empleados, docentes y trabajadores oficiales.

- La creación y notificación de cuentas de Google Workspace for Education institucional para empleados, docentes y trabajadores oficiales nuevos, se llevará a cabo en la medida que se vayan realizando los nombramientos.
- El área de Recursos Humanos envía a través de SARA la solicitud para creación de nuevas cuentas de correo. La OITEL tendrá un tiempo aproximado de quince (15) días hábiles para realizar la creación las cuentas y notificar a los usuarios.
- Una vez creada la cuenta, los datos de acceso serán enviados a la cuenta de correo personal que haya sido registrada por el usuario en el proceso de nombramiento.

6.6.3. Dependencias, eventos y contratistas.

- Las cuentas temporales o para dependencias, deben ser solicitadas por el coordinador administrativo o el jefe de la dependencia, diligenciando el formato de Solicitud de Cuenta de Correo Temporal F-01-MP-11-05-01, el cual se puede descargar del sitio web <http://planeacion.univalle.edu.co/index.php/formatos-oficina-de-informatica-y-comunicaciones>. El responsable de la cuenta debe diligenciar el formato de solicitud completamente y con información veraz.
- El formulario diligenciado debe ser enviado al correo electrónico usuarios@correounivalle.edu.co o entregado en la Oficina de Informática y Telecomunicaciones.
- La OITEL enviará notificación de la creación de la cuenta y las credenciales de acceso al responsable de la Cuenta.

 Universidad del Valle	POLÍTICA DE USO DE CORREO ELECTRÓNICO UNIVERSIDAD DEL VALLE		
	Versión 2.0	(código)	2022/05/26

- Cada miembro de la comunidad universitaria tiene derecho a solo una cuenta de correo electrónico institucional, para uso exclusivo del titular, independientemente de la cantidad de vinculaciones que tenga con la universidad.
- Para empleados con vinculación temporal (contratistas, docentes hora cátedra, empleados provisionales, etc.) se creará una cuenta de correo electrónico institucional, cuya vigencia estará regida por el tiempo de duración del contrato con la universidad.

6.6.4. Cancelación de Cuentas de Correo

La Universidad procederá a la cancelación de las cuentas de correo en los siguientes casos:

6.6.4.1. Estudiantes.

- Situaciones de deserción por parte del estudiante.

6.6.4.2. Empleados, docentes y trabajadores oficiales.

- Finalización de la relación o vinculación contractual con la universidad para funcionarios, docentes y contratistas.
- Ante la evidencia de incumplimiento de las políticas definidas en este documento.

6.6.4.3. Dependencias, eventos y contratistas.

- Se eliminarán las cuentas 60 días después de la finalización del contrato o el evento, previa notificación al responsable de la Cuenta.

6.6.5. No Se Crean Cuentas de Correo en los siguientes casos:

- A terceros que presten servicios a empresas que tengan contratos de obra, consultoría, compraventa, etc. con la Universidad del Valle.
- A personas que se vinculen a diplomados y cursos de extensión.
- A personas que asistan a programas de capacitación en modalidad de convenio con otras instituciones públicas o privadas realizadas a través de extensión.

 Universidad del Valle	POLÍTICA DE USO DE CORREO ELECTRÓNICO UNIVERSIDAD DEL VALLE		
	Versión 2.0	(código)	2022/05/26

- A personas que asistan a programas no formales que ejecuten las áreas académicas.
- Estudiantes de intercambio.
- Egresados que no hayan tenido cuenta de correo electrónico en el dominio correounivalle.edu.co

7. CONTROL DE CAMBIOS

FECHA	VERSIÓN	DESCRIPCIÓN DEL CAMBIO
2020-02-25	1.0	Versión inicial, embebida en el procedimiento “Gestión de Cuentas de Correos Institucionales” MP-11-05-01
2022-05-26	2.0	Política actualizada

8. INCUMPLIMIENTO

El incumplimiento a la política de Seguridad y Privacidad de la Información traerá consigo, las consecuencias legales que apliquen a la normativa de la Entidad, incluyendo lo establecido en las normas que competen al Gobierno nacional y territorial en cuanto a Seguridad y Privacidad de la Información se refiere.

 Universidad del Valle	POLÍTICA DE USO DE CORREO ELECTRÓNICO UNIVERSIDAD DEL VALLE		
	Versión 2.0	(código)	2022/05/26

Fin de la política.

 Universidad del Valle	POLÍTICA GENERAL DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	
	Versión 2.0	Actualizado: 08/06/2023
Elaboró: OITel	Revisó: William Sánchez Peña	Aprobó: William Sánchez Peña

POLÍTICA GENERAL DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

La dirección de LA UNIVERSIDAD DEL VALLE, 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, la Comunidad universitaria y los ciudadanos, todo enmarcado en el estricto cumplimiento de las leyes y en concordancia con la misión y visión de la Institución.

Para LA UNIVERSIDAD DEL VALLE, 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 Institución según como se defina en el alcance, sus funcionarios, terceros, estudiantes, docentes y la comunidad universitaria en general, teniendo en cuenta que los principios sobre los que se basa el desarrollo de las acciones o toma de decisiones alrededor del SGSI¹ estarán determinadas por las siguientes premisas:

- ☐ Minimizar el riesgo en las funciones más importantes de la Institución.
- ☐ Cumplir con los principios de seguridad de la información.
- ☐ Cumplir con los principios de la función administrativa.
- ☐ Mantener la confianza de su comunidad universitaria, funcionarios, terceros y la ciudadanía en general.
- ☐ Proteger los activos tecnológicos.
- ☐ Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.

¹ Sistema de Gestión de Seguridad de la Información (SGSI)

 Universidad del Valle	POLÍTICA GENERAL DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	
	Versión 2.0	Actualizado: 08/06/2023
Elaboró: OITel	Revisó: William Sánchez Peña	Aprobó: William Sánchez Peña

- Fortalecer la cultura de seguridad de la información en los funcionarios, terceros, y la comunidad universitaria en general.
- Garantizar la continuidad del servicio frente a incidentes.
- LA UNIVERSIDAD DEL VALLE 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 servicio, y a los requerimientos regulatorios.

A continuación se establecen 12 principios de seguridad que soportan el SGSI de LA UNIVERSIDAD DEL VALLE:

- Las responsabilidades frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de los funcionarios, proveedores, terceros y la comunidad universitaria en general.
- LA UNIVERSIDAD DEL VALLE 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, contratistas), o como resultado de un servicio interno en outsourcing.
- LA UNIVERSIDAD DEL VALLE protegerá la información creada, procesada, transmitida o resguardada por sus procesos institucionales, 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 DEL VALLE protegerá su información de las amenazas originadas por parte del personal.
- LA UNIVERSIDAD DEL VALLE protegerá las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.
- LA UNIVERSIDAD DEL VALLE controlará la operación de sus procesos de negocio garantizando la seguridad de los recursos tecnológicos y las redes de datos.

 Universidad del Valle	POLÍTICA GENERAL DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	
	Versión 2.0	Actualizado: 08/06/2023
Elaboró: OITel	Revisó: William Sánchez Peña	Aprobó: William Sánchez Peña

- LA UNIVERSIDAD DEL VALLE implementará control de acceso a la información, sistemas y recursos de red.
- LA UNIVERSIDAD DEL VALLE garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información.
- LA UNIVERSIDAD DEL VALLE 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 DEL VALLE 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 DEL VALLE garantizará el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas.

Los siguientes son los objetivos definidos para el SGSI:

1. Realizar una adecuada gestión de riesgos con el fin de proteger la confidencialidad, integridad y disponibilidad de la información.
2. Capacitar y sensibilizar al personal en temas relacionados con seguridad de la información, buscando un aumento progresivo en la cultura de seguridad al interior de la Institución, reflejado en el nivel de cumplimiento de políticas y procedimientos y, el reporte de eventos e incidentes de seguridad.
3. Gestionar de manera adecuada los incidentes de seguridad de la información generando, documentando y aplicando las lecciones aprendidas, con el fin de reducir la posibilidad o el impacto de incidentes futuros.
4. Mejorar continuamente el desempeño del SGSI mediante la implementación de acciones correctivas eficaces, auditorías internas y las revisiones de seguridad de la información.

 Universidad del Valle	POLÍTICA GENERAL DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	
Elaboró: OITel	Versión 2.0 Revisó: William Sánchez Peña	Actualizado: 08/06/2023 Aprobó: William Sánchez Peña

Complementando la gestión de la Seguridad de la Información:

1. La Universidad del Valle se acoge a lo estipulado por la ley estatutaria 1581 de 2012 o ley de Habeas Data por lo cual protege, salvaguarda y custodia las bases de datos que contienen información general y/o sensible de la comunidad universitaria en todos sus estamentos.
2. El personal técnico operativo y profesional presta su servicio en diferentes modalidades de contratación a la Oficina de Informática y Telecomunicaciones (O.I.Tel.) de la Universidad del Valle está formado y es consciente de su rol y sentido de responsabilidad para la data, equipos e información institucional a la que en un momento u otro podrían tener acceso por lo cual el proceso de selección respeta y se fundamenta en valores.
3. La gestión de las plataformas tecnológicas de uso masivo en la Universidad son encargadas a funcionarios idóneos debidamente seleccionados, monitoreados y entrenados por los proveedores más competentes disponibles en el mercado.
4. La universidad cuenta con controles de intervención a través de firewalls que filtran la llegada o acceso a los sistemas de información relevantes para la institución. El uso de estos recursos y su gestión es de acceso restringido de personal que cuenta con perfiles definidos y competencias en seguridad de la información.
5. El coordinador de Infraestructura tecnológica de la O.I.Tel. tiene competencias y formación en gestión de la seguridad de la información y tiene el perfil de oficial de seguridad de la información según los estándares nacionales.

 Universidad del Valle	POLÍTICA GENERAL DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	
	Versión 2.0	Actualizado: 08/06/2023
	Elaboró: OITel	Revisó: William Sánchez Peña
		Aprobó: William Sánchez Peña

6. La dirección de la O.I.Tel lidera y participa en la transformación digital y ciberseguridad que puede ser de beneficio no solo para la Universidad del Valle, sino para otras universidades o instituciones estatales de educación superior públicas y la coordinación de infraestructura tecnológica

7. La dirección de la O.I.Tel desde el año 2010 hace parte de la asociación Red Universitaria de Alta Velocidad (RUAV) en donde no solamente se han agremiado universidades, sino otras instituciones de la región, a través de cuya alianza se promueven buenas prácticas de gestión universitaria y manejo de tecnologías para el apoyo misional; así como, capacitaciones para el personal y experiencias, contratos y formas de abordar temas de ciberseguridad.

8. La universidad del Valle maneja con regularidad, discreción y confianza múltiples opciones de respaldo de la información.

9. Las prácticas de desarrollo de software y el modelo institucional empleado consideran la división de responsabilidades, el monitoreo y uso de diferentes ambientes de desarrollo, pruebas y producción que permiten aumentar la confianza en las soluciones tecnológicas que requiere la Universidad para su gestión.

10. La Universidad cuenta con acreditación institucional de alta calidad reconocida por el CNA y el MEN para el lapso máximo posible (10 años) en la franja 2014 a 2024; así como, con la acreditación de programas de formación universitaria de pregrado y posgrado e igualmente con la certificación de calidad en sus procesos otorgados sistemáticamente por el ICONTEC.

 Universidad del Valle	POLÍTICA GENERAL DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	
	Versión 2.0	Actualizado: 08/06/2023
Elaboró: OITel	Revisó: William Sánchez Peña	Aprobó: William Sánchez Peña

Alcance/Aplicabilidad

Esta política aplica a toda la Institución, sus funcionarios, contratistas y terceros de LA UNIVERSIDAD DEL VALLE, así como a la comunidad universitaria en general.

Nivel de cumplimiento

Todas las personas cubiertas por el alcance y aplicabilidad deberán dar Cumplimiento un 100% de la política.

 Universidad del Valle	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DE LOS SITIOS WEB INSTITUCIONALES DE LA UNIVERSIDAD DEL VALLE	
	Versión 1.0	Actualizado: 01/10/2020
Elaboró: César A. Narváez Barco	Revisó: Fernando Prieto Barbosa	Aprobó: Laura S. Rodríguez Pulecio

Contenido

Objetivo	2
Alcance	2
Generalidades	2
Definiciones	2
Términos y condiciones de uso	3
Propiedad de los contenidos publicados	4
Responsables de los contenidos publicados	5
Protección de Datos	5
Contáctenos	5

 Universidad del Valle	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DE LOS SITIOS WEB INSTITUCIONALES DE LA UNIVERSIDAD DEL VALLE	
	Versión 1.0	Actualizado: 01/10/2020
Elaboró: César A. Narváez Barco	Revisó: Fernando Prieto Barbosa	Aprobó: Laura S. Rodríguez Pulecio

Objetivo

Definir condiciones de uso de la información contenida en los sitios web pertenecientes a la Universidad del Valle

Alcance

La presente política aplica para todos los usuarios que accedan a cualquiera de las páginas que se encuentran bajo los dominios **univalle.edu.co** y **correounivalle.edu.co**, los cuales están registrados a nombre de la Universidad del Valle ante los organismos competentes.

Generalidades

Conforme a los lineamientos establecidos por la Estrategia de Gobierno Digital, las páginas web de la Universidad del Valle, cuyo portal principal es www.univalle.edu.co (en adelante los sitios web) tienen como función principal comunicar a la sociedad información concerniente a su misión, visión y objetivos institucionales.

Definiciones

Para facilitar la comprensión de estas Condiciones de Uso del Sitio Web, se hace necesario aclarar el significado de las siguientes palabras:

- a. **Contenidos.** Implican todas las formas de información o datos que se divulgan en la página web, entre los que se encuentran: textos, imágenes, fotos, logos, diseños, animaciones.
- b. **Derechos de Propiedad Intelectual.** incluye lo relativo a marcas, nombres comerciales, logos, enseñas, lemas, nombres de dominio, secretos empresariales, saber-hacer, diseños industriales, patentes, modelos de utilidad y derecho de autor.
- c. **Foro.** Servicio automatizado de mensajes, a menudo moderado por un propietario, a través del cual los suscriptores reciben mensajes dejados por otros suscriptores por un tema dado. Los mensajes se envían por correo electrónico.

 Universidad del Valle	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DE LOS SITIOS WEB INSTITUCIONALES DE LA UNIVERSIDAD DEL VALLE	
	Versión 1.0	Actualizado: 01/10/2020
Elaboró: César A. Narváez Barco	Revisó: Fernando Prieto Barbosa	Aprobó: Laura S. Rodríguez Pulecio

d. **Internet.** Herramienta de comunicación con decenas de miles de redes de computadoras unidas por el protocolo TCP/IP. Sobre esta red se pueden utilizar múltiples servicios como por ejemplo correos electrónicos, www, etc.

e. **Sitio web o página web.** Resultado en hipertexto o hipermedia que proporciona un navegador del www después de obtener la información solicitada. Su contenido puede ir desde un texto corto a un voluminoso conjunto de textos, gráficos estáticos o en movimiento, sonido, etc.

f. **Publicar.** Hacer que un documento sea visible desde el Sitio Web.

g. **Servicios.** Son las ayudas en línea que la MINTIC provee actualmente o que piensa proveer en el futuro a los usuarios, por medio de esta página web, como publicación de noticias o actividades propias de la gestión institucional; trámites en línea; consultas; foros y buzón de quejas y reclamos, entre otros.

h. **Usuario.** Es toda persona que ingresa al Sitio Web. Puede registrarse en caso de que requiera realizar un trámite o recibir un servicio de la entidad; o para poner una queja mediante el uso del buzón de Quejas y Reclamos, creado para este efecto.

i. **Vínculo (link en inglés).** Apuntadores hipertexto que sirven para saltar de una información a otra, o de un servidor web a otro, cuando se navega por Internet.

Términos y condiciones de uso

Para todos los efectos y por el solo hecho de acceder a los sitios web de la Universidad del Valle, el usuario acepta y reconoce que lo hace bajo su total responsabilidad y que, por tanto, acepta plenamente y sin reservas el contenido de los términos y condiciones de uso del sitio web de esta entidad. La Universidad del Valle se reserva, en todos los sentidos, el derecho de actualizar y modificar en cualquier momento y de cualquier forma, de manera unilateral y sin previo aviso, las presentes políticas de privacidad y términos de uso para adaptarlas a novedades legislativas o jurisprudenciales, así como a prácticas generales de la industria; de igual forma podrá hacerlo con los contenidos de sus sitios web.

El sitio web institucional tiene por finalidad brindar al usuario todo tipo de información relacionada con sus productos, programas, trámites y servicios. En ningún caso esta información deberá considerarse como exhaustiva, completa o que de cualquier forma satisfaga todas las necesidades del usuario.

 Universidad del Valle	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DE LOS SITIOS WEB INSTITUCIONALES DE LA UNIVERSIDAD DEL VALLE	
	Versión 1.0	Actualizado: 01/10/2020
Elaboró: César A. Narváez Barco	Revisó: Fernando Prieto Barbosa	Aprobó: Laura S. Rodríguez Pulecio

Este sitio web puede tener enlaces a otros sitios de interés o a documentos localizados en otras páginas o sitios web de propiedad de otras entidades, personas u organizaciones diferentes a la Universidad del Valle. Solamente por el hecho de que el usuario acceda a otro sitio web o a un documento localizado en otra página, a través de un link o un vínculo establecido en los sitios web institucionales de la Universidad del Valle, el usuario deberá someterse a las condiciones de uso y a la política de privacidad de la página o sitio web a la que envía el link.

La Universidad del Valle no persigue ningún lucro, ganancia o interés comercial con los contenidos y enlaces que se publican en su sitio web institucional y en los sitios web de los diferentes productos y servicios que son parte de la entidad y a los cuales pertenecen a los dominios **univalle.edu.co** y **correounivalle.edu.co**.

Toda la información publicada a través de los sitios web de la Universidad del Valle, es gratuita y no utiliza ningún tipo de intermediarios para acceder a ella. Por favor denuncie cualquier irregularidad.

Propiedad de los contenidos publicados

Los sitios web que se encuentran en los dominios **univalle.edu.co** y **correounivalle.edu.co** y sus contenidos, son de propiedad de la Universidad del Valle. Está prohibida su reproducción total o parcial, su traducción, inclusión, transmisión o almacenamiento con fines lucrativos. Es posible descargar el contenido para uso personal y no comercial, siempre y cuando se haga expresa mención de la propiedad de esta institución.

Con relación a los contenidos que aparecen en los sitios web de la Universidad del Valle, el usuario se obliga a:

- Usar los contenidos de forma diligente, adecuada y lícita.
- No suprimir o manipular el copyright (derechos de autor) y demás datos que son propios de la Universidad del Valle.
- No emplear los contenidos y, en particular, la información obtenida a través del a página web de la Universidad del Valle o de los servicios que presta, para emitir publicidad.
- El usuario de los sitios web, no alterará, bloqueará o realizará cualquier otro acto que impida mostrar o acceder a cualquier contenido, información o servicios de los sitios Web o que estén incorporados en las páginas web vinculadas, además de que no deberá atentar contra su plataforma tecnológica, sus sistemas de información ni tampoco interferirá en su normal funcionamiento, pues el usuario será el único

 Universidad del Valle	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DE LOS SITIOS WEB INSTITUCIONALES DE LA UNIVERSIDAD DEL VALLE	
	Versión 1.0	Actualizado: 01/10/2020
Elaboró: César A. Narváez Barco	Revisó: Fernando Prieto Barbosa	Aprobó: Laura S. Rodríguez Pulecio

responsable por el uso indebido que haga de los sitios web de la Universidad del Valle y sus contenidos.

Responsables de los contenidos publicados

La responsabilidad de los servicios y la información publicada en los sitios web de la Universidad del Valle, se encuentra delegada de la siguiente manera:

- Administrador del sitio web de la Universidad: Dirección de Comunicaciones Universitarias (Ver [Acuerdo Consejo Superior 005 de 2015](#))
- Responsables de los contenidos de los sitios web de facultades y dependencias: los directores, jefes, decanos o coordinadores de cada dependencia
- Responsable del servicio de hospedaje: Oficina de Informática y Telecomunicaciones

Protección de Datos

En el siguiente enlace puede usted consultar la Política de Tratamiento de la Información Personal:

<https://www.univalle.edu.co/politica-de-tratamiento-de-la-informacion-personal>

Contáctenos

Si el usuario desea hacer sugerencias a la Universidad del Valle para mejorar los contenidos de los sitios web de la Institución, o si tiene alguna duda o comentario respecto al tratamiento de la información en general, puede comunicarse a través del enlace de Atención al Ciudadano. <http://atencionalciudadano.univalle.edu.co/>