# MANUAL POLÍTICAS DE SEGURIDAD POR DOMINIO
# DOCUMENTO INSTITUCIONAL

**MACROPROCESO:** PLANEACIÓN ESTRATÉGICA
**PROCESO:** Planeación Institucional
**DEPENDENCIA/ PROGRAMA:** Vicepresidencia
**Versión:** 3

## Contenido

# MANUAL POLÍTICAS DE SEGURIDAD POR DOMINIO DOCUMENTO INSTITUCIONAL

**MACROPROCESO:** PLANEACIÓN ESTRATÉGICA
**PROCESO:** Planeación Institucional
**DEPENDENCIA/ PROGRAMA:** Vicepresidencia
**Versión:** 3

## 1 OBJETO

Establecer y divulgar las Políticas de Seguridad de la Información a todo el personal de la Institución, para que sea de su conocimiento y cumplimiento.

## 2 ALCANCE

Este documento define las Políticas de Seguridad de la Información que deben ser cumplidas por los, Estudiantes, Egresados, Docentes, Personal Administrativo, Contratistas y Proveedores, que:

- Accedan a información confidencial o privada del a UNIVERSIDAD PILOTO DE COLOMBIA.
- Utilicen equipos informáticos y de telecomunicaciones conectados a la infraestructura de la Institución.
- Diseñen, construyan, prueben, implementen, y/o usen herramientas tecnológicas y/o servicios informáticos de la Institución.
- Ingresen de manera física y/o lógica a la Institución.

## 3 POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN POR DOMINIO

Estas Políticas se encuentran vigentes a partir del 12 de septiembre 2017, fecha en la que se publica la primera versión de este documento. La Política Institucional de Seguridad de la Información y las Políticas Generales de Seguridad por cada dominio seguirán un proceso de actualización permanente, de acuerdo con los cambios organizacionales (culturales, estructurales, operativos), del entorno, tecnológicos y las directrices gubernamentales que sean del caso.

La definición, actualización y mantenimiento de estas Políticas, es responsabilidad del Oficial de Seguridad de la Información con la debida aprobación de la Honorable Consiliatura. Este documento se actualizará por lo menos una vez al año y siempre que haya cambios importantes en la Institución. En las revisiones se tendrán en cuenta factores como: incidentes de seguridad, nuevas vulnerabilidades detectadas, cambios dentro de la infraestructura organizacional o tecnológica, cambios en los procesos, en los objetivos de la Institución, entre otros.

El Oficial de Seguridad de la Información es el responsable de gestionar y brindar apoyo en materia de Seguridad de la Información y Continuidad del negocio, y la Dirección de Tecnologías de la Información es el

ente que gestiona y da apoyo técnico en materia de Seguridad Informática y de Telecomunicaciones a las dependencias de la Institución.

Cualquier excepción a lo establecido a estas políticas, deberá contar con la recomendación formal del Oficial de Seguridad de la Información, y la aprobación del Comité de Seguridad de la Información.

La versión oficial de este documento para funcionarios, será la que se encuentre publicada en Sharepoint.

## 3.1 ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

### 3.1.1 Organización Interna

La UNIVERSIDAD PILOTO DE COLOMBIA ha definido una estructura organizacional encargada de la coordinación de las actividades relacionadas con la gestión de la seguridad de la información, la cual cuenta con un Oficial de Seguridad de la Información, el Comité de Seguridad de la Información y la Honorable Consiliatura.

### 3.1.2 Separación de deberes

La UNIVERSIDAD PILOTO DE COLOMBIA, establece que aquellas personas que realizan tareas de operación sobre aplicaciones o sistemas de información críticos de la Institución, no pueden tener a su cargo las labores de administración técnica sobre los sistemas operativos o las bases de datos.

### 3.1.3 Seguridad de la Información en la Gestión de Proyectos

La Gestión de Proyectos dentro de la UNIVERSIDAD PILOTO DE COLOMBIA, contemplará dentro de su planificación la inclusión de los requisitos de seguridad de la información, así como la evaluación de los riesgos que pueden llegar a impactar la confidencialidad, integridad y disponibilidad de los activos de información de la Institución.

### 3.1.4 Dispositivos Móviles

Los equipos de computación y comunicación móvil de la Institución se han adquirido específicamente para facilitar el desarrollo de actividades laborales directamente relacionadas con la Institución. Su uso debe estar directamente relacionado con las actividades del área a la cual ha sido asignado y el uso para propósitos personales debe ser ocasional, racional y no debe obstaculizar las actividades laborales.

Por lo anterior la Dirección de Tecnologías de la Información ha dispuesto los siguientes lineamientos:

- La Dirección de Tecnologías de la Información de la información definirá la línea base de configuración para los dispositivos móviles, teniendo en cuenta los controles acceso (identificación y autenticación), las técnicas criptográficas y protección contra virus y malware.
- La Dirección de Tecnologías de la Información de la información definirá y parametrizar la instalación de aplicaciones en los dispositivos móviles.
- Solamente funcionarios autorizados por la Dirección de Tecnologías de la Información la Institución, deben realizar la configuración de los dispositivos móviles por medio de un sistema centralizado de configuración y control de dispositivos móviles.
- La Institución por medio de la Dirección de Tecnologías de la Información debe mantener un inventario actualizado de dispositivos móviles que han sido autorizados y tienen acceso a sistemas de información la Institución.
- Los discos duros de los equipos de computación y comunicación móviles (y consecuentemente la información contenida) deben estar cifrados de acuerdo a los procedimientos predefinidos del área de Tecnología, por lo que es una obligación conjunta validar esta aplicación al recibir este activo, con lo que se busca la confidencialidad de la información.

Los Estudiantes, Egresados, Docentes, Personal Administrativo, Contratistas y Proveedores de Institución que tienen a su cargo equipos de computación y comunicación móvil asignados y/o autorizados, deberán custodiar dichos equipos para evitar la fuga, pérdida o alteración de la información consignada en los mismos y propia de su labor, teniendo en cuenta:

- En situaciones de robo o pérdida el funcionario es responsable de informar a Tecnología para gestionar el bloqueo de los mismos, y reportar al Centro de servicio de Tecnología el incidente.
- La instalación, configuración, modificación o eliminación de software aplicativo sobre los equipos de computación y comunicación móvil de la Institución es responsabilidad exclusiva del área de Tecnología.
- Evitar el acceso a redes públicas.
- No acceder a paginas no autorizadas (Pornografía, Redes sociales, Paginas de Música o descargas, etc.) que pueda generar riesgo para la información de la Institución.
- Cambiar periódicamente la contraseña.
- Abstenerse de instalar aplicaciones o programas no autorizados.
- Devolver el equipo al finalizar su relación contractual con la Institución.
- Reportar los incidentes de seguridad de la información asociados a su dispositivo móvil.

3.1.5 Trabajo Remoto.

El trabajo remoto sólo será autorizado por el Director o Líder del proceso correspondiente al cual pertenezca el funcionario solicitante, previa verificación de que son adoptadas todas las medidas que correspondan en materia de seguridad de la información, de modo que se cumplan con las políticas, normas y procedimientos existentes.

Estos casos serán de excepción y serán contemplados en situaciones que justifiquen la imposibilidad de otra forma de acceso y la urgencia, tales como horarios de la Institución, actividades de soporte que requieren atención inmediata, etc. Para ello, se establecerán normas y procedimientos para el trabajo remoto, que consideren los siguientes aspectos:

- Los requisitos de seguridad de las comunicaciones, teniendo en cuenta la necesidad de acceso remoto a los sistemas internos de la Universidad.
- 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 trabajador está autorizado a acceder.
- Auditoría y seguimiento de la seguridad de la información.
- La revocación de la autoridad y de los derechos de acceso, y la devolución de los equipos cuando las actividades del trabajo remoto finalicen.

## 3.2 SEGURIDAD DE LOS RECURSOS HUMANOS

### 3.2.1 Responsabilidad del personal

Todos Estudiantes, Egresados, Docentes, Personal Administrativo, Contratistas y Proveedores de LA UNIVERSIDAD PILOTO DE COLOMBIA autorizados para acceder a la infraestructura de procesamiento de información, son responsables del cumplimiento de las políticas y procedimientos de seguridad de la información definidos por la Institución.

La información almacenada en los equipos de cómputo de la Institución es de propiedad de la UNIVERSIDAD PILOTO DE COLOMBIA y cada usuario es responsable por proteger su integridad, confidencialidad y disponibilidad.

### 3.2.2 Procesos disciplinarios

Los incidentes de seguridad de la información ocurridos en la UNIVERSIDAD PILOTO DE COLOMBIA serán registrados e investigados con el fin de determinar sus causas y responsables. Aquellos funcionarios que hayan sido relacionados con incidentes de seguridad de la información o violaciones a las políticas de seguridad establecidas, serán citados a descargos y se aplicará el respectivo proceso disciplinario. Los procesos

disciplinarios derivados de los reportes y del análisis de los Incidentes de Seguridad serán manejados teniendo en cuenta la gravedad y el nivel de responsabilidad identificadas.

### 3.2.3 Terminación o cambio de la contratación laboral

La responsabilidad de custodia de cualquier activo de información mantenido, usado o producido por el personal que se retira, o cambia de cargo recae en el Jefe directo o Supervisor del contrato que cambio o se termina.

Tras la finalización o cambio en la contratación laboral se revisarán los derechos de acceso de los funcionarios, contratistas y/o terceras partes a los activos asociados con los sistemas y servicios de información, esto determinará si es necesario remover los derechos de acceso.

## 3.3 GESTIÓN DE ACTIVOS DE INFORMACIÓN

### 3.3.1 Inventario de activos de información y propiedad de los activos

Todos los procesos en el alcance del Sistema de Gestión de Seguridad de la Información, con el apoyo del Oficial de Seguridad de la Información, mantendrán un inventario actualizado de los activos de información.

### 3.3.2 Uso adecuado de los activos y recursos de información

Toda la información de la UNIVERSIDAD PILOTO DE COLOMBIA será procesada y almacenada de acuerdo con su nivel de clasificación, de manera que se protejan las propiedades de confidencialidad, integridad y disponibilidad.

### 3.3.3 Uso de Internet, correo electrónico y recursos tecnológicos

La UNIVERSIDAD PILOTO DE COLOMBIA, suministra a los estudiantes, egresados, docentes, personal administrativo, contratistas y proveedores diferentes recursos tecnológicos y servicios. La Universidad controlará, verificará y monitoreará el uso adecuado de estos recursos. Así mismo asignara una cuenta de correo electrónico institucional como único buzón autorizado para el envío de mensajes para realizar su trabajo y cumplir con sus funciones.

### 3.3.4 Devolución de Activos

Todos Estudiantes, Egresados, Docentes, Personal Administrativo, Contratistas y Proveedores deben devolver todos los activos de información de la Institución en su poder (software, documentos institucionales, equipamiento, dispositivos de computación móviles, tarjetas de crédito, tarjetas de ingreso, etc.) tras la terminación de su empleo, contrato o acuerdo.

3.3.5 Clasificación de la Información

Toda información perteneciente al UNIVERSIDAD PILOTO DE COLOMBIA deberá ser identificada, clasificada y documentada con base en los criterios de clasificación definidos en la Guía de clasificación de activos de información.

Los propietarios de los activos de información serán los responsables de establecer el nivel de clasificación de cada activo y dichos activos se protegerán de acuerdo con el nivel asignado.

3.3.6 Manejo de Medios

En los equipos de cómputo de la UNIVERSIDAD PILOTO DE COLOMBIA, únicamente se restringirá la conexión de dispositivos o medios de almacenamiento extraíble (USB) acorde a la clasificación de la información y al resultado de un análisis de riesgo realizado al activo de información.

Toda la información almacenada en medios magnéticos removibles, e impresa, estará controlada en cuanto a su acceso, uso, transporte, almacenamiento y eliminación, acorde con su nivel de clasificación.

3.4 CONTROL DE ACCESO

3.4.1 Política para el control de Acceso

El acceso a los sistemas de información de la UNIVERSIDAD PILOTO DE COLOMBIA, cuenta con un mecanismo de identificación individual (usuario y contraseña), las cuales con personales e intransferibles

3.4.2 Acceso a redes y a servicios de red

El acceso a la red de datos de la UNIVERSIDAD PILOTO DE COLOMBIA se realizará utilizando la cuenta de red de cada usuario. Los funcionarios deben proteger y no compartir sus credenciales de acceso a la red y servicios de red que le son conferidos de acuerdo con su perfil. Es responsabilidad de cada usuario solicitar el cambio de su contraseña cuando sospeche que puede estar en conocimiento de terceras personas.

3.4.3 Administración de Cuentas de Usuario y Contraseñas

La creación y cancelación de cuentas de usuario, así como la entrega de las contraseñas a los mismos se controla a través de un proceso formal a cargo de la Dirección de Tecnología.

La UNIVERSIDAD PILOTO DE COLOMBIA no se hace responsable del uso mal intencionado o ilegal que los usuarios puedan realizar con cada Identificador de Usuario asignado.

## 3.5 CRIPTOGRAFÍA

### 3.5.1 Política sobre el uso de controles criptográficos

Se utilizarán sistemas y técnicas criptográficas para la protección de la información de la UNIVERSIDAD PILOTO DE COLOMBIA con el fin de asegurar una adecuada protección de su confidencialidad e integridad.

Se aplicarán controles criptográficos en la protección de claves de acceso a sistemas, datos y servicios y cuando se presente la transmisión o intercambio de información confidencial.

En la UNIVERSIDAD PILOTO DE COLOMBIA no se permitirá el uso de herramientas o mecanismos de cifrado de información diferentes a las autorizadas por la Dirección de Tecnología.

### 3.5.2 Gestión de Llaves

La Dirección de Tecnología mantendrá la administración de claves criptográficas y certificados digitales utilizados por parte de la UNIVERSIDAD PILOTO DE COLOMBIA. Todas las claves serán protegidas contra modificación y destrucción, las claves secretas y privadas serán protegidas contra copia o divulgación no autorizada. La UNIVERSIDAD PILOTO DE COLOMBIA aplicará un aseguramiento adecuado al equipo utilizado para generar, almacenar, y archivar claves, clasificándolo como un activo crítico y de riesgo alto.

## 3.6 SEGURIDAD FÍSICA Y AMBIENTAL

### 3.6.1 Áreas Seguras

El centro de datos, centros de cableado y áreas de archivo de la UNIVERSIDAD PILOTO DE COLOMBIA se definen como áreas seguras.

Todo acceso a las áreas seguras debe ser autorizado por la Dirección del proceso a cargo de las mismas, así mismo, deben registrarse los accesos a dichas áreas.

### 3.6.2 Seguridad de Equipos

La UNIVERSIDAD PILOTO DE COLOMBIA, protegerá la disponibilidad e integridad de la infraestructura de procesamiento de información mediante labores de mantenimiento y soporte.

3.6.3 El control de acceso en los sistemas de gestión de documentos

El acceso a los documentos puede estar restringido para proteger: la información personal y la intimidad; los derechos de propiedad intelectual y el secreto comercial. Cada usuario tiene permiso de acceso de acuerdo a las responsabilidades y funciones de su cargo.

3.6.4 Retiro de activos

Los equipos, información y software propiedad de la UNIVERSIDAD PILOTO DE COLOMBIA no serán retirados de las instalaciones de la Institución sin antes dejar el registro y evidencia de la autorización de salida, la autorización debe ser solicitada al Jefe Inmediato, excepto para los cargos de Dirección, Subdirección y Coordinación, quienes están autorizados por requerimientos propios de su labor.

3.6.5 Equipos de usuario desatendido

Los usuarios deberán bloquear su equipo o estación cada vez que se retiren de su sitio de trabajo y solo se podrán desbloquear con la contraseña del usuario. Todas las estaciones de trabajo deberán usar el papel tapiz y el protector de pantalla institucional.

3.6.6 Escritorio y Pantalla Limpia

En horas no hábiles o cuando los sitios de trabajo se encuentren desatendidos, los usuarios deberán dejar la información confidencial protegida bajo llave.

3.7 SEGURIDAD DE LAS OPERACIONES

3.7.1 Procedimientos de operación documentados

Se contará con procedimientos, registros e instructivos de trabajo debidamente documentados, con el fin de asegurar el mantenimiento y operación adecuada de la UNIVERSIDAD PILOTO DE COLOMBIA.

Todas las tareas relacionadas con el mantenimiento de la infraestructura de procesamiento de información se realizarán de forma programada, de manera que sean debidamente planeadas, autorizadas y documentadas.

3.7.2 Gestión de Cambios

Los cambios a la plataforma tecnológica que soporta la operación de los servicios críticos, deberán ser planeados y documentados para no afectar la disponibilidad, integridad o confidencialidad de la información.

3.7.3 Gestión de Capacidad

La Dirección de Tecnología de la UNIVERSIDAD PILOTO DE COLOMBIA monitoreará periódicamente la capacidad y rendimiento de la infraestructura de procesamiento de información, con el objeto de garantizar la disponibilidad de los recursos tecnológicos requeridos por los procesos del negocio.

3.7.4 Separación de los ambientes de desarrollo, pruebas y operación

La UNIVERSIDAD PILOTO DE COLOMBIA cuenta en su infraestructura de procesamiento de información con ambientes separados para desarrollo, pruebas y producción. Así mismo, controlará el paso de software y aplicaciones de un ambiente a otro.

No deben realizarse pruebas, instalaciones o desarrollos de software, directamente sobre el entorno de producción. Así mismo, en los ambientes de desarrollo y pruebas no se deberán utilizar datos reales del ambiente de producción.

3.7.5 Protección contra códigos maliciosos

Todos los servidores y las estaciones de trabajo de la UNIVERSIDAD PILOTO DE COLOMBIA mantendrán instalado y actualizado un sistema de Antivirus.

3.7.6 Copias de Respaldo

Copias de Respaldo y de restauración de información crítica y privada de la Institución contenida en los servidores y sistemas de información de la UNIVERSIDAD PILOTO DE COLOMBIA, se deben implementar los controles necesarios para garantizar la confidencialidad, integridad y disponibilidad de la información definidos en Lineamiento para copias de seguridad.

El personal técnico de la Dirección de Tecnología dejará registro y evidencia de las pruebas de restauración aleatorias que efectúe para validar la integridad de los datos respaldados.

3.7.7 Controles de auditorías de sistemas de información

Las auditorías internas a intervalos planificados a los procesos definidos para el Sistema de Gestión de Seguridad de la Información de la Universidad serán llevadas a cabo por auditores independientes. Se entenderá como tales a aquellos que no participen directamente de los procesos incluidos en el alcance del SGSI que se esté auditando. Las tareas y actividades se acordarán con las áreas involucradas con el fin de minimizar el riesgo de interrupciones en las operaciones.

## 3.8 SEGURIDAD DE LAS COMUNICACIONES

### 3.8.1 Controles de redes y Seguridad de los servicios de red

La administración de la red y de las estaciones de trabajo de los usuarios estará a cargo de la Dirección de Tecnología de la UNIVERSIDAD PILOTO DE COLOMBIA.

1. El acceso remoto a la red de datos de la UNIVERSIDAD PILOTO DE COLOMBIA se permitirá para acceder a recursos como el correo electrónico, únicamente a los Funcionarios, Estudiantes o Terceros autorizados por el Director, Subdirector o Coordinador de la Universidad. Separación en las redes

La plataforma tecnológica de la UNIVERSIDAD PILOTO DE COLOMBIA estará distribuida en segmentos de red independientes para cada servicio, separando las redes de servicios internos de la Institución, de las conexiones con terceros y del acceso a Internet. El tráfico entre estos segmentos de red estará controlado mediante un Firewall.

### 3.8.2 Transferencia de Información

La UNIVERSIDAD PILOTO DE COLOMBIA firma acuerdos de confidencialidad con Funcionarios y Terceros que por diferentes razones requieren conocer o intercambiar información privada o confidencial de la UNIVERSIDAD PILOTO DE COLOMBIA.

### 3.8.3 Acuerdos de Confidencialidad o de no divulgación

Todos los Docentes, Personal Administrativo, Contratistas y Proveedores deberán firmar la cláusula y/o acuerdo de confidencialidad definida por la UNIVERSIDAD PILOTO DE COLOMBIA y este deberá ser parte integral de cada uno de los contratos.

## 3.9 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS

### 3.9.1 Política de Desarrollo Seguro

La UNIVERSIDAD PILOTO DE COLOMBIA, incluirá los requisitos relacionados con seguridad de la información para nuevos sistemas de información o para mejoras a los sistemas de información existentes, de acuerdo a las necesidades del negocio y la clasificación de la información.

Algunos de los aspectos de seguridad que se tomarán en cuenta son:

a) La seguridad del entorno de desarrollo
b) La orientación sobre la seguridad en el ciclo de vida de desarrollo del software
c) Los requisitos de seguridad en la fase diseño;

d) Los puntos de chequeo de seguridad dentro de los hitos del proyecto;
e) Repositorios seguros para almacenar código;
f) La seguridad en el control de las versiones;
g) El conocimiento requerido sobre seguridad de la aplicación;
h) La capacidad de los desarrolladores para evitar, encontrar y resolver las vulnerabilidades.

### 3.9.2 Análisis y especificación de requisitos de seguridad de la información

La inclusión o desarrollo de un nuevo producto de software o aplicativo en la UNIVERSIDAD PILOTO DE COLOMBIA, o los cambios y/o actualizaciones a los sistemas existentes, deberán estar precedidas de la inclusión de los requisitos y controles de seguridad definidos por el Oficial de Seguridad de la Información.

Todas las solicitudes para compra, actualización y/o desarrollo de software deberán especificar la necesidad de controles de seguridad de la información.

Los procesos de adquisición de aplicaciones y paquetes de software cumplirán con los requerimientos y obligaciones derivados de las leyes de propiedad intelectual y derechos de autor.

## 3.10 RELACIONES CON LOS PROVEEDORES

### 3.10.1 Seguridad de la Información en las relaciones con los proveedores

El Oficial de Seguridad de la Información revisará y documentará los requisitos de seguridad de la información relacionados con el acceso de proveedores a los activos de información de la UNIVERSIDAD PILOTO DE COLOMBIA, los cuales se incluirán como parte integral del contrato de acuerdo al alcance del servicio prestado por el proveedor.

El acceso a la información y a la infraestructura de procesamiento de información de la UNIVERSIDAD PILOTO DE COLOMBIA por parte de proveedores, deberá ser solicitado por el área respectiva y autorizado por el Oficial de Seguridad de la Información.

El Oficial de Seguridad de la Información se apoyará en el proceso de Contratación para efectuar el seguimiento y revisión a la prestación de los servicios de los proveedores dentro del marco de cumplimiento con los requisitos de seguridad establecidos en los acuerdos.

El Oficial de Seguridad de la Información revisará los cambios en el suministro de servicios por parte de los proveedores, basado en la criticidad de la información, los sistemas y procesos del negocio, realizando una reevaluación de los riesgos de seguridad de la información que puedan afectar la cadena de suministro de tecnología de información y comunicación.

## 3.11 GESTIÓN DE INCIDENTES DE SEGURIDAD

### 3.11.1 Responsabilidades, procedimientos, reporte de eventos y debilidades de Seguridad de la información

Los Estudiantes, Egresados, Docentes, Personal Administrativo, Contratistas y Proveedores de Institución de la UNIVERSIDAD PILOTO DE COLOMBIA deben informar inmediatamente al Centro de Servicios de Tecnología cualquier situación sospechosa, o incidente de seguridad que comprometa la confidencialidad, integridad y/o disponibilidad de la información.

El Oficial de Seguridad de la Información es el responsable de realizar la investigación y seguimiento a los eventos e incidentes de seguridad reportados, con el apoyo de otras áreas de la Institución o de entidades externas.

El Comité de Seguridad de la Información y ante su ausencia la Oficina de Comunicaciones son los únicos autorizados por parte de la UNIVERSIDAD PILOTO DE COLOMBIA para reportar incidentes de seguridad ante las autoridades.

Todos los Estudiantes, Egresados, Docentes, Personal Administrativo, Contratistas y Proveedores deben mantener confidencialidad de la información relacionada con el manejo, investigación y seguimiento de los incidentes.

## 3.12 ADMINISTRACIÓN DE LA CONTINUIDAD DEL NEGOCIO

Para la UNIVERSIDAD PILOTO DE COLOMBIA es un compromiso con sus usuarios mantener la continuidad de las operaciones de la Institución, a través de la implementación de estrategias para el desarrollo del Plan de Continuidad del Negocio, buscando mejorar la respuesta de la Universidad ante eventos de interrupción de servicios y/o procesos de negocio.

En la planeación de Continuidad del Negocio, se detallan las políticas relacionadas con la Seguridad de la Información en la Continuidad de Negocio, así como las políticas de pruebas y mantenimiento del Plan.

## 3.13 CUMPLIMIENTO DE REQUERIMIENTOS

### 3.13.1 Cumplimiento de las Obligaciones Legales

La UNIVERSIDAD PILOTO DE COLOMBIA cumple con la legislación aplicable propia de las leyes colombianas, las regulaciones generadas por otros entes gubernamentales o nacionales que apliquen y las obligaciones contractuales con funcionarios, proveedores, contratistas y terceros.

Estará prohibido el uso de software no licenciado o autorizado por la Dirección de Tecnología de la Universidad. Los usuarios serán responsables por la instalación y utilización de software no autorizado en sus estaciones de trabajo.

### 3.13.2 Derechos de propiedad intelectual

La UNIVERSIDAD PILOTO DE COLOMBIA cumple con la reglamentación de propiedad intelectual y ejecuta revisiones periódicas para asegurar que se estén respetando los derechos de propiedad intelectual.

### 3.13.3 Privacidad y protección de información de datos personales

En cumplimiento de las regulaciones vigentes, la UNIVERSIDAD PILOTO DE COLOMBIA ha adoptado las medidas técnicas y administrativas necesarias para mantener el nivel de seguridad requerido en atención a los datos personales tratados.

### 3.13.4 Revisiones de Seguridad de la Información

El Oficial de Seguridad de la Información verificará el cumplimiento de las Políticas de Seguridad apoyada en el equipo de auditoría y los líderes de proceso mediante revisiones periódicas al cumplimiento de los procesos y procedimientos, dentro del marco de las políticas, normas y cualquier otro requisito de seguridad aplicable.

## 4 GLOSARIO DE TÉRMINOS

- Activo de Información: Cualquier información o sistema relacionado con el tratamiento de la misma que tenga valor para la organización. Es todo activo que contiene información, la cual posee un valor y es necesaria para realizar los procesos misionales y operativos de LA UNIVERSIDAD PILOTO DE COLOMBIA.
- Alcance: Ámbito de la organización que queda sometido al SGSI. Debe incluir la identificación clara de las dependencias, interfaces y límites con el entorno, sobre todo si sólo incluye una parte de la organización.
- Análisis de riesgos: Uso sistemático de la información para identificar fuentes y estimar el riesgo.
- Incidente: Evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.
- Integridad: Mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.
- Confidencialidad: Acceso a la información por parte únicamente de quienes estén autorizados.
- Disponibilidad: Característica o propiedad de permanecer accesible y disponible para su uso cuando lo requiera una entidad autorizada.

- Riesgo: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño.

## 5 ANEXOS

- Metodología de Gestión de Riesgos de Seguridad de la Información
- Guía de clasificación de activos de información