


**POLITICA DE LICENCIAMIENTO Y USO DE SOFTWARE BASE PARA  
SOFTEASY**

**SISTEMAS DE GESTION DE LA SEGURIDAD DE LA INFORMACIÓN  
ING. JOHN ROBERTH CORREA**




**INTEGRANTES DEL GRUPO:  
LUIS FELIPE VELASCO TAO  
JUAN DAVID GONZALEZ DIMATÉ**

**UNIVERSIDAD DE SAN BUENAVENTURA  
FACULTAD DE INGENIERÍA  
INGENIERÍA DE SISTEMAS  
BOGOTÁ  
06 DE ABRIL  
2021**

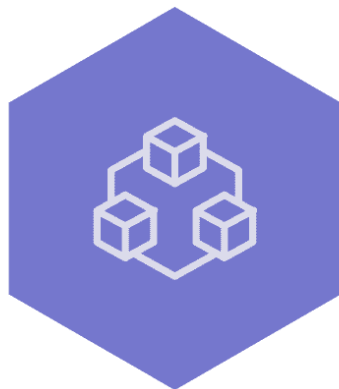
 UNIVERSIDAD DE SAN BUENAVENTURA BOGOTÁ	Universidad de San Buenaventura Facultad de ingeniería Sistemas de la gestión de la seguridad de la información	TALLER 2 SGSI	2021 - 1
---	--	---------------	----------

## Contenido


1. Introducción.....	4
2. Objetivos para el SGSI.....	4
2.1. Objetivo General .....	4
2.2. Objetivos Específicos .....	4
3. Alcance del sistema de gestión de seguridad de la información .....	4
4. Marco regulatorio y normativo .....	5
5. Organización de la seguridad de la información .....	6
5.1. Oficial de seguridad de la información y/o CISO .....	6
5.2. Dependencias y secciones de Softeasy.....	6
5.3. Funcionarios y clientes de Soft-easy.....	7
5.4. Responsables de la información .....	8
5.5. Cooperación interinstitucional .....	8
5.6. Acuerdos de confidencialidad .....	8
6. Apoyo de la alta gerencia.....	9
7. Revisión del SGSI.....	9
8. Política complementaria de licenciamiento e implementación del Software ..	10
8.1. Introducción.....	10
8.2. Licenciamiento del software como prevención de riesgos .....	10
8.3. Antecedentes .....	10
8.4. Política de licenciamiento y uso de software base .....	11
8.4.1. Descripción general .....	11
8.4.2. Propósito .....	11
8.4.3. Ámbito .....	11
8.4.4. Definiciones .....	11
8.4.5. Instalación de software .....	12
8.4.6. Licencias.....	12
8.4.7. Actualización de software .....	12
8.4.8. Información relacionada con el software .....	13
8.4.9. Limitaciones.....	13

 UNIVERSIDAD DE SAN BUENAVENTURA BOGOTÁ	Universidad de San Buenaventura Facultad de ingeniería Sistemas de la gestión de la seguridad de la información	TALLER 2 SGSI	2021 - 1
---	--	---------------	----------

9. Declaración de aplicabilidad del Sistema de gestión de seguridad de la información.....	13
--	----



Soft-easy

 UNIVERSIDAD DE SAN BUENAVENTURA BOGOTÁ	Universidad de San Buenaventura Facultad de ingeniería Sistemas de la gestión de la seguridad de la información	TALLER 2 SGSI	2021 - 1
---	--	---------------	----------

## 1. Introducción

Soft-easy reconoce a los recursos informáticos, tanto a nivel de hardware como software, como una parte imprescindible de la empresa debido a que el objetivo, misión y visión de la empresa se enfocan en el desarrollo de proyectos web, móviles y de escritorio. Por esta razón es necesario establecer una política para la gestión de estos recursos que garantice su integridad, su uso adecuado por parte de los empleados y directivos y su seguridad. Esta política está en cumplimiento con la reglamentación legal vigente, referente al uso de software e incluye parámetros o lineamientos a seguir, referente al uso de los equipos con el fin de mantenerlos seguros e incorruptos. Además, esta política comprende que el uso de datos por parte de los empleados, directivos y/o clientes hace parte de los activos que conforman la empresa, por lo que también deben tomarse medidas para garantizar su integridad y confidencialidad.

## 2. Objetivos para el SGSI

### 2.1. Objetivo General


Establecer los lineamientos y protocolos para el uso de programas o software requerido dentro de la organización.

### 2.2. Objetivos Específicos

- Establecer las necesidades de uso de los activos de la organización.
- Evaluar la capacidad necesaria de los equipos para su uso en la organización.
- Verificar el licenciamiento de los programas a utilizar en la organización.
- Implementar medidas relacionadas con el correcto uso de software dentro de la organización

## 3. Alcance del sistema de gestión de seguridad de la información


La política de Seguridad de la Información es aplicable en cualquier etapa de uso de software, desde su instalación, distribución dentro de la organización y licenciamiento. De igual forma para todos los funcionarios, proveedores, clientes y terceros que tengan algún vínculo con la compañía. El alcance abarca desde el enunciado de la política, pasando por los lineamientos para la implementación del Sistema Seguridad y Privacidad de la Información, la matriz de riesgo, la definición de los indicadores para el monitoreo de cumplimiento de la política

 UNIVERSIDAD DE SAN BUENAVENTURA BOGOTÁ	Universidad de San Buenaventura Facultad de ingeniería Sistemas de la gestión de la seguridad de la información	TALLER 2 SGSI	2021 - 1
---	--	---------------	----------

#### 4. Marco regulatorio y normativo

Softeasy, al ser una empresa que no solo tendrá contacto con información sensible de clientes y proveedores, sino que realizara uso de software para la producción de servicios de software a los clientes, se acoge a normativas relacionadas con la seguridad de la información, derechos de autor y demás normativas relacionadas con el consumidor y la información, como son las siguientes:

- Ley 44 de 1993, que señala las sanciones relacionadas con los derechos de autor de soporte lógico o software.
- Ley 527 de 1999, que señala el uso y validez del mensaje de datos.
- Ley 599 de 2000 “Por la cual se expide el Código Penal (cláusulas 257, 270, 271 y 272)”.
- Ley 603 de 2000 en la cual se indica que todas las empresas deben reportar en sus informes anuales de gestión el cumplimiento de las normas de propiedad intelectual y de derechos de autor.
- Ley 1450 de 2011 “Por la cual se expide el Plan Nacional de Desarrollo (PND) 2010 – 2014”
- Ley 1480 de 2011 o Estatuto del Consumidor Ley 1273 de 2009 en cuanto a la protección de la información y los datos. (cláusula 269A, Acceso Abusivo a Sistema Informático, cláusula 269D, Daño Informático, cláusula 269F, Violación de datos personales, cláusula 269E Uso de software malicioso).
- Ley 1266 de 2008 “Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales”.
- Decreto 1151 de 2008 “Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en Línea de la República de Colombia, se reglamenta parcialmente la Ley 962 de 2005, y se dictan otras disposiciones”.
- Acuerdo 279 de 2007 “Por el cual se dictan los lineamientos para la Política de Promoción y Uso del Software libre en el Sector Central, el Sector Descentralizado y el Sector de las Localidades del Distrito Capital”.
- Ley 1581 de 2012 “Establece los principios relacionados con el tratamiento de datos personales en Colombia, definiciones, los sujetos relacionados con la ley, los deberes y obligaciones de los distintos sujetos y las sanciones en caso de violación de derechos.”
- NTC-ISO/IEC 27001- 27002:2013, en donde se finen los sistemas de seguridad de la información y distintos controles a aplicar sobre estos.
- Decreto 1414 de 2017 del Min TIC, normativa por medio de la cual se busca “contribuir al desarrollo económico, social y político de la nación y elevar el bienestar de los colombianos”.

 UNIVERSIDAD DE SAN BUENAVENTURA BOGOTÁ	Universidad de San Buenaventura Facultad de ingeniería Sistemas de la gestión de la seguridad de la información	TALLER 2 SGSI	2021 - 1
---	--	---------------	----------

- Acuerdo 060 de 2001 para instituciones que son cubiertas por la Ley 594 de 2000 Gestión del correo electrónico.

## 5. Organización de la seguridad de la información

### 5.1. Oficial de seguridad de la información y/o CISO

Es definido como el responsable máximo en planificar, desarrollar, controlar y gestionar las políticas, procedimientos y acciones con el fin de mejorar la seguridad de la información dentro de sus pilares fundamentales de confidencialidad, integridad y disponibilidad.

Sus responsabilidades son:

- Decidir acerca de la seguridad de TI.
- Decidir acerca del cumplimiento regulatorio y la continuidad del negocio.
- Decidir acerca de la seguridad corporativa (comprende la seguridad física, seguridad de las instalaciones e investigaciones).


El alcance de sus funciones está determinado por:

- Seguridad de la información.
- Auditorías.
- Investigaciones.
- Recuperación de desastres.
- Seguridad de las instalaciones.
- Seguridad personal.
- Protección de la propiedad intelectual.
- Protección ejecutiva.
- Prevención del fraude.
- Privacidad.
- Verificación de perfiles de seguridad.

### 5.2. Dependencias y secciones de Softeasy.

Soft-easy, como empresa de desarrollo de software, debe garantizar que los recursos a su disposición estén proveídos de un estricto cumplimiento de la política de seguridad, ya que de estos depende el correcto funcionamiento de ella. Bajo este concepto, las dependencias a las cuales se les debe dar prioridad al momento de aplicar la política de seguridad son:

- Equipos físicos: Comprendido como todo equipo en uso por parte de la empresa, desde teléfonos móviles y ordenadores hasta servidores y dispositivos de red. Estos equipos son los que le permitirán a los miembros de la organización desempeñar adecuadamente su función dentro de ella,

 UNIVERSIDAD DE SAN BUENAVENTURA BOGOTÁ	Universidad de San Buenaventura Facultad de ingeniería Sistemas de la gestión de la seguridad de la información	TALLER 2 SGSI	2021 - 1
---	--	---------------	----------

por lo que es imprescindible que estén en buenas condiciones y que estén protegidos contra cualquier amenaza, tanto interna como externa.

- Programas y aplicaciones: Comprendido como todo el software en uso por parte de la aplicación, desde sistemas operativos hasta aplicaciones y programas de escritorio. De esta sección dependen gran parte de las funciones de la empresa, por lo que es necesario capacitar adecuadamente al personal para que se utilicen adecuadamente, con el fin de evitar que el programa se desconfigure y provoque errores que afecten a su funcionamiento. También es necesario proveer la licencia adecuada a los programas en uso para evitar caer en problemas legales (en caso de que el software sea de pago). Por último, es necesario verificar que los programas y aplicaciones provengan de una fuente confiable.

### 5.3. Funcionarios y clientes de Soft-easy


Los funcionarios de la empresa se definen como el personal necesario para el correcto funcionamiento de la organización. Bajo este concepto, los funcionarios que conforman a la empresa son:

- Presidente: Aquel que representa legalmente a la empresa y es el encargado de tomar las decisiones corporativas dentro de ella, incluyendo misiones, objetivos, tratos, salarios, entre otros.
- Junta directiva.
- Junta administrativa.
- CISO.
- Gerente: Encargado de un grupo de trabajo en específico dentro de la organización. Es el que se asegurará de que los objetivos determinados se realicen.
- Desarrolladores: Son los empleados sobre los cuales recae la función principal de la empresa, que es el desarrollo de software. Trabajan en equipos supervisados por un gerente.
- Mantenimiento: Son los empleados encargados de realizar una revisión periódica de los equipos y los programas en uso de la empresa.

Los clientes de la empresa pueden ser:

- Personas (individuos).
- Empresas pequeñas (Tiendas de ropa, tiendas de alimentos, Bufetes de abogados, restaurantes, cafeterías).

Es responsabilidad de la empresa que los datos que sean provistos por cualquiera de estas entidades sean confidenciales, permanezcan íntegros y que sean accesibles única y exclusivamente por los funcionarios en caso de ser necesario su uso.

 UNIVERSIDAD DE SAN BUENAVENTURA BOGOTÁ	Universidad de San Buenaventura Facultad de ingeniería Sistemas de la gestión de la seguridad de la información	TALLER 2 SGSI	2021 - 1
---	--	---------------	----------

#### 5.4. Responsables de la información

Son responsables de la información dentro de la organización:

- El administrador de la base de datos en uso de la empresa, ya que es el que tendrá acceso casi ilimitado a los datos de los funcionarios y los clientes. Sobre él recae la responsabilidad de mantener los datos confidenciales e íntegros, además de decidir si un funcionario tendrá acceso o no a estos datos. En cualquier caso, deberá recibir la aprobación directa del CISO para cualquier solicitud que le llegue por parte de los funcionarios.
- El personal de mantenimiento, ya que sobre ellos recae la responsabilidad de mantener los equipos físicos de la empresa en buen estado, con el fin de evitar cualquier tipo de error o daño que pueda afectar el funcionamiento de la empresa o el desempeño de sus funciones.
- Los desarrolladores, ya que sobre ellos recae la responsabilidad del correcto uso de los datos que provea el administrador de la base de datos. Toda acción que involucre la manipulación de datos por parte de estos funcionarios debe estar debidamente supervisada, y debe informarse mediante un reporte y/o un registro de actividades al CISO.

#### 5.5. Cooperación interinstitucional

Para funciones dentro de la empresa, el área de mantenimiento debe mantener informado en todo momento al área de desarrollo sobre el estado de los equipos, el estado de las aplicaciones y programas y el estado de los servidores. En caso de haber un cambio en cualquiera de estos aspectos, el personal de mantenimiento debe capacitar a los desarrolladores sobre el nuevo uso que deben darle.

El área de desarrollo debe realizar una solicitud formal para el uso de datos personales (en caso de ser necesario) al área de administración, con el fin de mantener siempre la trazabilidad de los datos dentro de la organización.


#### 5.6. Acuerdos de confidencialidad

Todos los datos personales que sean provistos y registrados dentro de la base de datos, ya sean de funcionarios o clientes, deben mantenerse dentro de la organización, y quien sea el administrador debe garantizar que estos datos permanezcan confidenciales.

Todo funcionario dentro de la organización debe asegurarse que cualquier tipo de información, ya sean datos personales, equipos o programas, solo deben ser conocidos dentro de la propia organización, y deben permanecer así.

Todo cliente que haya hecho un acuerdo con la empresa debe conocer que los únicos datos que le serán provistos por parte de la empresa serán el ID del



 UNIVERSIDAD DE SAN BUENAVENTURA BOGOTÁ	Universidad de San Buenaventura Facultad de ingeniería Sistemas de la gestión de la seguridad de la información	TALLER 2 SGSI	2021 - 1
---	--	---------------	----------

proyecto del cual solicitó su desarrollo y el nombre del gerente encargado de dicho proyecto. Esta información debe ser conocida única y exclusivamente por dicho cliente y el gerente del proyecto.

Todo funcionario dentro y fuera de la organización debe conocer, entender, firmar y aceptar el correspondiente acuerdo de confidencialidad de la información.

## 6. Apoyo de la alta gerencia

Las directivas de la organización (entiéndase como: Junta directiva, Presidencia, gerencia, Junta administrativa, entre otros) tiene como responsabilidad:


- Proveer los equipos físicos necesarios para el desarrollo de las funciones de la empresa.
- Proveer el licenciamiento adecuado para el uso de los programas necesarios para el desarrollo de las funciones de la empresa.
- Capacitar al personal de mantenimiento para la revisión de equipos y programas en uso de la empresa.
- Tomar decisiones con respecto al manejo de personal de la organización (desarrolladores, mantenimiento, junta directiva, etc.).
- Establecer los lineamientos y regulaciones necesarios para el uso de recursos de la empresa.
- En caso de ser necesario, actualizar cualquier recurso que sea solicitado por los funcionarios de la empresa y que sean estrictamente necesarios para el correcto desempeño de sus funciones.

## 7. Revisión del SGSI

La dirección de Softeasy debe revisar el estado del Sistema de Gestión de seguridad de la información en intervalos planificados, por lo menos una vez semestralmente, de modo tal se pueda evaluar su conveniencia y pertinencia con relación a amenazas, vulnerabilidades y demás novedades relacionadas con la seguridad de la información, las cuales involucren alguna actualización en el SGSI y la modificación de políticas de seguridad o la creación de nuevas, además de tener presente la correcta documentación de las revisiones realizadas.

Esta revisión cumplirá con los lineamientos establecidos en el procedimiento de revisión del Sistema Integrado de Gestión.

A la par, las políticas de seguridad de la información, normas, procedimientos, estándares, controles, formatos y procedimientos deberán ser revisados y actualizados constantemente, todo esto de forma periódica y previamente

 UNIVERSIDAD DE SAN BUENAVENTURA BOGOTÁ	Universidad de San Buenaventura Facultad de ingeniería Sistemas de la gestión de la seguridad de la información	TALLER 2 SGSI	2021 - 1
---	--	---------------	----------

planificada, siguiendo los lineamientos pertinentes para la mejora continua, además de tener en cuenta la continua administración de los nuevos activos y su integración al Sistema de Gestión de Seguridad de la información, por parte del oficial de seguridad de la información o CISO, teniendo presente la realización de revisiones por parte de entidades externas especializadas apegadas a la norma NTCISO/IEC 27001:2013 y debe ser realizada por alguien con las credenciales de AUDITORLIDER vigentes.

## 8. Política complementaria de licenciamiento e implementación del Software

### 8.1. Introducción

Dentro de Softeasy debemos de tener muy en cuenta la importancia del software que se usa en la producción, vigilando de forma correcta las fuentes de donde se obtienen los aplicativos, las herramientas instaladas dentro de cada equipo, los requerimientos de software y hardware requerido para su instalación y el licenciamiento, esto con el fin de trabajar de forma legal la producción de software para todos nuestros clientes, apegado a las normativas del país asociadas con la tecnología y principalmente asegurándonos de que no se dará cabida a la pérdida de información.


### 8.2. Licenciamiento del software como prevención de riesgos

Dentro del mundo de la producción de software de forma profesional debemos conocer que el uso de software con licencia y de forma legal le dará a los desarrolladores y a los clientes la seguridad de que la información que se manipule dentro de cada programa no se encontrara vulnerable ante los ataques que usan, de modo tal prevengamos:

- Uso de software pirata el cual pueda generar un daño o pérdida de los equipos y la información contenida den estos
- Problemas legales relacionados con derechos de autor
- Problemas en el desempeño de los productos realizados con el software.
- Posible pérdida de información al momento de la ejecución de los productos por parte de los clientes.

### 8.3. Antecedentes

Em Softeasy se usan de programas o software gratuito en su mayoría, instalado por cada uno de los desarrolladores, además de usar programas sin verificar su fuente.

 UNIVERSIDAD DE SAN BUENAVENTURA BOGOTÁ	Universidad de San Buenaventura Facultad de ingeniería Sistemas de la gestión de la seguridad de la información	TALLER 2 SGSI	2021 - 1
---	--	---------------	----------

## 8.4. Política de licenciamiento y uso de software base

### 8.4.1. Descripción general

En este documento se presentan todos los procesos relacionados con la instalación y gestión de licencias del software requerido en Softeasy, con el fin de tener un control pleno de la información y la calidad de los productos de la organización.

### 8.4.2. Propósito


Esta política esta diseñada para proteger los datos a los cuales Softeasy tiene acceso para la producción de software, los cuales pueden afectar a la empresa, todo esto debido al uso indebido de software para la producción y gestión de distintas actividades relacionadas con la información.

### 8.4.3. Ámbito

Esta política tendrá su campo de ejecución en los equipos dentro de la oficina encargados de la producción de software y la gestión de los datos de los clientes y proveedores. De modo tal se tratará software enfocado a la producción y a ofimática.

### 8.4.4. Definiciones

- Licencia: termino por medio del cual se indica que un autor o los autores de un programa les permite a terceros el acceso a las funcionalidades del software, delimitando la modificación y distribución del programa. Las licencias no solo hacen referencia a la autorización brindada después de la adquisición de un software de tipo comercial, también existen las licencias por tiempo limitado de forma gratuita o de forma libre, pero todas estas siempre dejándole constancia al autor de que se hará uso del software de su propiedad.
- Software libre: hace referencia a la libertad de los usuarios a ejecutar, distribuir, copiar, estudiar y/o modificar a su conveniencia y sin ninguna implicación legal.
- Software de producción: hace relación a todos los programas o aplicativos que permitan la creación de nuevo software, tales como sistemas operativos IDEs, programas de edición de imágenes, video y sonido, entre otros que se involucren en los procesos de diseño, construcción despliegue y pruebas de software.
- Productos: hace referencia a todo el software que será realizado a petición de los clientes con el fin de satisfacer una necesidad.

 UNIVERSIDAD DE SAN BUENAVENTURA BOGOTÁ	Universidad de San Buenaventura Facultad de ingeniería Sistemas de la gestión de la seguridad de la información	TALLER 2 SGSI	2021 - 1
---	--	---------------	----------

- Software comercial: todo tipo de programa o aplicativo a desplegar en un equipo el cual sea distribuido con fines comerciales por parte de una organización.

#### 8.4.5. Instalación de software

La instalación de software en los equipos de la oficina estará a cargo del administrador de esta, el cual estará al pendiente de las peticiones o requerimientos de software de los desarrolladores. Dichas peticiones se les comunicara a los directivos los cuales serán los encargados de autorizar la compra e instalación del software.

Cabe resaltar que siempre se debe documentar el proceso de instalación de software, en donde se definan fechas, periodos de actualización de licencias, fuentes, proceso de instalación y ubicación de los archivos de instalación.

#### 8.4.6. Licencias

Las licencias de los sistemas operativos de todos los equipos de la oficina serán renovadas anualmente, esto debido a que todos los equipos estarán bajo una licencia de organización o empresarial de Windows. Dichas licencias estarán a cargo del administrador encargado del mantenimiento de la oficina, el cual debe comunicarles a los directivos sobre cualquier inconveniente. Con relación al paquete de programas de Office, la licencia será renovada cada año, entrando cada año como parte de los gastos de la organización.

Con relación al paquete de programas de Adobe, la licencia será renovada cada año, atendiendo a las mejoras de software y hardware requeridas para su correcto funcionamiento.


Programas como NetBeans, Eclipse y demás IDEs de desarrollo serán usados en su licencia gratuita, siempre que sea el caso que se pueda conseguir desde la pagina encargada de su distribución legal.

Todo tipo de licencia debe encontrarse documentada con el fin de conocer su periodo de vigencia, su tipo y demás información requerida.

#### 8.4.7. Actualización de software

Con relación a los sistemas operativos, las actualizaciones deben realizarse teniendo en cuenta los siguientes aspectos:

- Realizar un punto de restauración de cada equipo, con el fin de poder revertir errores ocurridos por la actualización de los equipos. Esto deberá estar a cargo del administrador.

 UNIVERSIDAD DE SAN BUENAVENTURA BOGOTÁ	Universidad de San Buenaventura Facultad de ingeniería Sistemas de la gestión de la seguridad de la información	TALLER 2 SGSI	2021 - 1
---	--	---------------	----------

- El administrador debe documentarse regularmente con relación a las actualizaciones, esto con el fin de evitar inconvenientes ocurridos después de la instalación de las actualizaciones de los So de los equipos

Por otro lado, demás las actualizaciones de programas de ofimática o producción de software deberán ser estudiadas por parte del administrador, esto con el fin de tener versiones de software que sean optimas para los equipos y que sean pertinentes para el desarrollo correcto de los productos.

Los procesos de actualización de software deben encontrarse documentados, evidenciando la búsqueda de información que permita conocer el porque se realizan o no las actualizaciones.

#### 8.4.8. Información relacionada con el software

En el proceso de desarrollo no se puede hacer uso de información real de los clientes, exceptuando en la producción de componentes gráficos, esto con el fin de minimizar la perdida de la confidencialidad de la información suministrada por los clientes.

#### 8.4.9. Limitaciones


El administrador tiene prohibido suministrar licencias a los desarrolladores y demás funcionarios de la oficina para que estos hagan uso de estas en sus equipos personales.

### 9. Declaración de aplicabilidad del Sistema de gestión de seguridad de la información

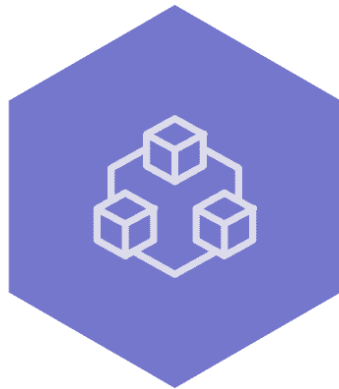
Toda la información presentada en este documento es de obligatorio cumplimiento y conocimiento de todos los empleados de la empresa, clientes, proveedores y terceros los cuales tengan una relación con la misma.

Dado sea el caso que se vulneren o rompan alguno de los lineamientos presentados en las políticas de seguridad implementadas para el sistema de gestión de seguridad de la información de Softeasy, sea de forma intencional o por negligencia, se tomaran las medidas pertinentes, tanto disciplinarias como legales, por parte de las directivas de la organización.

La política de seguridad de la información debe prevenir el incumplimiento de las leyes, estatutos, regulaciones u obligaciones contractuales que se relacionen con los controles de seguridad establecidos para Softeasy. Como las políticas y lineamientos de seguridad definidos en el presente documento, como son:

 UNIVERSIDAD DE SAN BUENAVENTURA BOGOTÁ	Universidad de San Buenaventura Facultad de ingeniería Sistemas de la gestión de la seguridad de la información	TALLER 2 SGSI	2021 - 1
---	--	---------------	----------

- El Objetivo del SGSI.
- El alcance del SGSI.
- El Marco normativo y regulatorio.
- La organización de roles y responsabilidades para el SGSI.
- El apoyo de la alta dirección.
- La revisión del SGSI.



Soft-easy