# SGSI

# POLITICA DE SEGURIDAD DE LA INFORMACIÓN

El contenido de este texto es privado y la presente versión se considera un documento interno de trabajo.

Universidad Francisco de Paula Santander

CONDICIONES DE USO

No se autoriza la reproducción o difusión por ningún
Medio o mecanismo sin el debido control
y autorización de la oficina encargada

| REV | ELABORADO | REVISADO | APROBADO |
|---|---|---|---|
| NOMBRE | Yesica María Pérez Pérez, | Dra. Claudia Toloza | Dr. Héctor Parra |
| CARGO | Auditora de Sistemas | Secretaria General UFPS | Rector UFPS |
| FIRMA | Yesica María Pérez Pérez 1091593033 | | |
| FECHA | Resolucion 1072 del 28 de octubre de 2014 | Politica de la Seguridad de la informacion. | |

# CONTENIDO

# 1. SEGURIDAD DE LOS RECURSOS HUMANOS

Los siguientes controles están orientados a reducir los riesgos de error humano, comisión de ilícitos contra la División de Sistemas o cualquier dependencia donde se procese información en la Universidad, contra el uso inadecuado de instalaciones. El Comité de Seguridad documentará las funciones de seguridad de los empleados y las Responsabilidades con respecto a la seguridad de la información.

## Antes del empleo

- Se verificarán los antecedentes de todos los candidatos a un empleo en la Universidad como parte de los criterios de selección de acuerdo con las leyes, reglamentación y ética pertinentes.
- Como parte de sus términos y condiciones iniciales de empleo, los empleados deberán conocer firmarán un Compromiso de Confidencialidad o no divulgación, en lo que respecta al tratamiento de la información de la Universidad.
- Los acuerdos contractuales con empleados y contratistas de la Universidad deben incluir sus responsabilidades y las de la Universidad en cuanto a la seguridad de la información.

## Durante el empleo

- El Comité de Seguridad desarrollará planes de capacitación de Seguridad de la Información, los cuales se realizarán periódicamente, mínimo una capacitación por semestre.
- Todos los empleados de la Universidad, y cuando sea pertinente, los usuarios externos y los terceros que desempeñen funciones en la misma, recibirán una adecuada capacitación y actualización periódica en materia de la política, normas y procedimientos de la seguridad de la información.
- Todos los funcionarios y/o contratistas serán responsables de proteger la información a la cual accedan y procesen, para evitar su pérdida, alteración, destrucción o uso indebido.
- Los empleados de la Universidad, al momento de tener conocimiento directo o indirecto sobre una debilidad de seguridad, son responsables de registrar y comunicar las mismas al líder de la División de Sistemas o al jefe inmediato de la dependencia.

## Terminación y cambio de empleo

- Cuando un empleado se retire de la Universidad, el líder de la División de Sistemas o dependencia encargada eliminará el usuario y los privilegios de acceso correspondientes al empleado y debe hacer entrega del inventario de activos, carné y credenciales de acceso a su cargo entre otros.

# 2. GESTIÓN DE ACTIVOS

## Responsabilidad por los activos

- Los activos de información de la Universidad serán identificados, clasificados y valorados para establecer los mecanismos de protección necesarios.
- Cada dependencia bajo supervisión del comité de seguridad de la información, debe elaborar y mantener un inventario de los activos de información que poseen, identificando un propietario para cada uno de ellos.
- Se debe brindar a los líderes de proceso y a los encargados de cada dependencia las herramientas tecnológicas y complementarias que permitan la administración del inventario garantizando la disponibilidad, integridad y confidencialidad de los datos que lo componen.

## Manejo de Medios

- Los líderes de procesos, con la asistencia del líder de la división de Sistemas, implementará procedimientos para la administración de medios informáticos removibles, USB, CD´s, DVD e informes impresos y la eliminación segura de los mismos.
- El uso de medios de almacenamiento removibles (ejemplo: CDs, DVDs, USBs, memorias flash, discos duros externos, celulares, cintas) sobre la infraestructura para el procesamiento de la información de la Universidad, estará autorizado para aquellos funcionarios cuyo perfil del cargo y funciones lo requiera.
- El funcionario se compromete a asegurar física y lógicamente el dispositivo a fin de no poner en riesgo la información de la Universidad contenida en el mismo.

# 3. CONTROL DE ACCESO

## Requisitos de la institución para el control de acceso

- Para una efectiva gestión de la seguridad de la información resulta de vital importancia, restringir los accesos y garantizar la adecuada utilización de los recursos informáticos.
- Cada usuario y funcionario es responsable de los mecanismos de control de acceso que le sean proporcionados.

## Gestión de acceso de usuarios

- El acceso a los documentos físicos y digitales estará determinado por las normas relacionadas con el acceso y las restricciones a los documentos públicos, a la competencia del área o dependencia específica y a los permisos y niveles de acceso de los funcionarios y contratistas determinadas por los Jefes de Dependencia.
- Para la consulta de documentos y recursos cargados en los diferentes Sistemas de Información se establecerán privilegios de acceso a los funcionarios y contratistas de acuerdo con el desarrollo de sus funciones y competencias. Dichos privilegios serán establecidos por el Jefe Inmediato, quien comunicará al Jefe de la división de Sistemas el listado con los funcionarios y sus privilegios.
- Corresponde al jefe de la División de Sistemas o a la dependencia a cargo elaborar, mantener y publicar los documentos de servicios de red que ofrece la Universidad a todos los empleados y usuarios.
- El jefe de la División de Sistemas elaborará, mantendrá y publicará los procedimientos de administración de cuentas de usuario para el uso de servicios de la red.
- El Jefe de Recursos Humanos deberá comunicar al oficial de Seguridad de la Información la relación de funcionarios públicos que hayan ingresado a laborar y de los que han dejado de hacerlo, para la activación o desactivación de las cuentas de los usuarios en los sistemas respectivos.
- El oficial de Seguridad de la Información definirá un procedimiento formal de registro de usuarios para otorgar y revocar el acceso a los Sistemas de Información de la Universidad; se limitará y controlará la asignación y uso de privilegios.
- El oficial de Seguridad de la Información o su delegado, configurará alertas de seguridad que permitan reaccionar de forma urgente ante determinados tipos de ataque e intentos de intrusión.
- Las contraseñas serán cambiadas periódicamente y suministradas al Administrador de los Sistemas, cada vez que se haga el cambio.
- Todos los empleados, contratistas y usuarios en general de los sistemas de la Universidad deben seguir buenas prácticas de seguridad en la selección y uso de contraseñas, los sistemas de información deben implementar mecanismos tecnológicos que vayan en concordancia con dichas buenas prácticas.

- El oficial de Seguridad de la Información, conjuntamente con los líderes de cada proceso, realizarán una evaluación de riesgos a fin de determinar el mecanismo de autenticación para los sistemas que correspondan en cada caso. El acceso a los recursos de TI institucionales deben estar restringidos según los perfiles de usuario definidos por el Comité de Seguridad de la Información.
- El oficial de Seguridad de la Información debe coordinar con el Jefe de Recursos Humanos el listado de tareas de concientización y la frecuencia de la capacitación que se brindará a todos los usuarios y contratistas de la Universidad, acerca de los requerimientos y procedimientos de seguridad para la protección de equipos desatendidos, así como de sus funciones en relación a la implementación de dicha protección.
- Se podrán implementar controles para limitar la capacidad de conexión de los usuarios, de acuerdo a las políticas que se establecen a tal efecto.
- El oficial de Seguridad de la Información junto con los líderes de cada proceso realizarán una evaluación de riesgos a fin de determinar el método de protección adecuado para el acceso a los Sistemas Operativos.
- Se generarán registros de auditoría que contengan excepciones y otros eventos relativos a la seguridad. Los registros de auditoría deberán incluir la identificación del usuario, la fecha y hora de inicio y terminación, la identidad o ubicación de la terminal, un registro de intentos exitosos y fallidos de acceso al sistema y un registro de intentos exitosos y fallidos de acceso a datos y otros recursos.
- Se desarrollarán procedimientos para monitorear el uso de las instalaciones de procesamiento de la información, a fin de garantizar que los empleados del Área de Control y Vigilancia sólo estén desempeñando actividades que hayan sido autorizadas explícitamente.
- El proceso de autenticación a los sistemas de la Universidad debe ser el adecuado, máximo tres intentos para una autenticación satisfactoria, después de éste número de intentos, se deshabilitará el ingreso de usuario.

# 4. SEGURIDAD FÍSICA Y DEL ENTORNO

## Áreas seguras

- Para el acceso a los sitios y áreas restringidas en la Universidad, debe gestionarse la autorización correspondiente, y así proteger la información y los bienes informáticos, muebles e inmuebles y demás elementos.
- La protección física se llevará a cabo mediante la creación de diversas barreras o perímetros de seguridad en las instalaciones de la división de Sistemas y demás instalaciones administrativas que contengan información confidencial o crítica.
- Las áreas protegidas se resguardarán mediante el empleo de controles de acceso físico y protección (control biométrico para el ingreso, vigilancia personal, sistemas de video vigilancia), los que serán determinados por el líder de la división de Sistemas, a fin de permitir el acceso sólo al personal autorizado.
- Para la selección y el diseño de un área protegida se tendrá en cuenta la posibilidad de daño producido por incendio, inundación, explosión, agitación civil, y otras formas de desastres naturales o provocados por el hombre. También se tomarán en cuenta las disposiciones y normas generales de la Universidad en materia de sanidad y seguridad.
- Para incrementar la seguridad de las áreas protegidas, se establecerán controles y lineamientos adicionales, para el personal que trabaja en la división de Sistemas, así como para las actividades de terceros que tengan lugar allí.

## Equipos

- El equipamiento será ubicado y protegido de tal manera que se reduzcan los riesgos ocasionados por amenazas y peligros ambientales, y las oportunidades de acceso no autorizado.
- El equipamiento estará protegido y respaldado con respecto a las posibles fallas en el suministro de energía u otras anomalías eléctricas. El suministro de energía funcionará de acuerdo con las especificaciones del fabricante o proveedor de cada equipo.
- El cableado de energía eléctrica y de comunicaciones que transporta datos o brinda apoyo a los servicios de información estará protegido contra intercepción o daño.
- Disponer de pólizas de protección de equipos actualizadas.
- El Comité de Seguridad de la información, establecerá un plan de mantenimiento preventivo para los equipos y velará por el cumplimiento del mismo.
- El uso de equipamiento destinado al procesamiento de información, fuera del ámbito de la Universidad será autorizado por el responsable patrimonial. En el caso de que en el mismo se almacene información clasificada, deberá ser aprobado además por el líder del proceso y por el líder de la división de Sistemas.

- La información puede verse comprometida por una desafectación o una reutilización descuidada del equipamiento o los medios de almacenamiento que contengan material sensible.
- El equipamiento, la información y el software no serán retirados de la división de sistemas, ni de ninguna dependencia de la Universidad sin autorización formal. Se llevarán a cabo comprobaciones puntuales para detectar el retiro no autorizado de activos.
- Las estaciones de trabajo deben estar correctamente aseguradas y operadas por personal de la institución el cual debe estar capacitado en las políticas de seguridad y las responsabilidades personales en el uso y administración de la información Institucional.

## Escritorio y pantalla limpia

- Se adopta una política de escritorios limpios para proteger documentos en papel y dispositivos de almacenamiento removibles y una política de pantallas limpias en las instalaciones de procesamiento de información, a fin de reducir los riesgos de acceso no autorizado, pérdida y daño de la información, tanto durante el horario normal de trabajo como fuera del mismo.
- Con el fin de evitar pérdidas, daños o accesos no autorizados a la información, todos los funcionarios de la Universidad 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. La información sensible que se envía a las impresoras se debe recoger de manera inmediata.
- Todos los usuarios son responsables de bloquear la sesión de su estación de trabajo en el momento en que se retiren del puesto, la cual se podrá desbloquear sólo con la contraseña del usuario. Cuando finalicen sus actividades, se deben cerrar todas las aplicaciones y dejar los equipos apagados.
- Todas las estaciones de trabajo deberán usar el papel tapiz y el protector de pantalla corporativo, el cual se activará automáticamente después de cinco (5) minutos de inactividad y se podrá desbloquear únicamente con la contraseña del usuario.

# 5. SEGURIDAD DE LAS OPERACIONES

**Procedimientos operacionales y responsabilidades**

- Se documentarán y mantendrán actualizados los procedimientos operativos identificados en esta Política y sus cambios serán autorizados por el líder de la división de Sistemas.
- El líder de la división de Sistemas controlará que los cambios en los componentes operativos no afecten la seguridad de los mismos ni de la información que soportan.
- Se establecerán funciones y procedimientos de manejo de incidentes garantizando una respuesta rápida, eficaz y sistemática a los incidentes relativos a seguridad.
- Se contemplará la separación de la gestión o ejecución de tareas o áreas de responsabilidad, en la medida de que la misma reduzca el riesgo de modificaciones no autorizadas o mal uso de la información o los servicios por falta de independencia en la ejecución de funciones críticas.
- El líder de la División de Sistemas y los líderes de proceso sugerirán criterios de aprobación de nuevos sistemas de información para las dependencias de la Universidad, además de actualizaciones y nuevas versiones, solicitando la realización de las pruebas necesarias antes de su aprobación definitiva.
- El líder de la División de Sistemas o su delegado, instalará antivirus en equipos de procesamiento de información de las dependencias críticas para actualizaciones diarias, para lo cual definirá cronograma al iniciar cada año.
- Los líderes de proceso desarrollarán y verificarán el cumplimiento de procedimientos para comunicar las fallas en el procesamiento de la información o los sistemas de comunicaciones, que permita tomar medidas correctivas.

**Protección contra software malicioso**

- La universidad determina a través de la División de Sistemas los recursos y procedimientos para que todos los recursos informáticos deben estar protegidos mediante herramientas y software de seguridad como antivirus, antispam, antispyware y otras aplicaciones que brindan protección contra código malicioso, en donde se cuente con los controles adecuados para detectar, prevenir y recuperar posibles fallos causados por código móvil y malicioso.
- Será responsabilidad del jefe de la división de sistemas autorizar el uso de las herramientas y asegurar que estas y el software de seguridad no sean deshabilitados bajo ninguna circunstancia, así como de su actualización permanente.
- No se permite la desinstalación y/o desactivación de software y herramientas de seguridad avaladas previamente por la Universidad.
- No se permite escribir, generar, compilar, copiar, propagar, ejecutar o intentar introducir cualquier código diseñado para auto replicarse, dañar o afectar el desempeño de cualquier dispositivo o infraestructura tecnológica de la Universidad.

- No se permite el uso de código móvil. Éste sólo podrá ser utilizado si opera de acuerdo con las políticas y normas de seguridad definidas y debidamente autorizado por la División de sistemas, con usuarios restringidos.

**Copias de respaldo**

- Los medios que alojan copias de seguridad deben estar correctamente conservados de acuerdo a las políticas y estándares definidos por el comité de seguridad de la información.
- El líder de la División de Sistemas, elaborará copias de seguridad diarias a los sistemas de información y las guardará en sitios bajo llave.
- Los medios magnéticos que contienen la información crítica deben ser almacenados en otra ubicación diferente a las instalaciones donde se encuentra dispuesta. El sitio externo donde se resguardan dichas copias, debe tener los controles de seguridad adecuados, cumplir con máximas medidas de protección y seguridad física apropiados.
- Se deberá establecer un plan de restauración de copias de seguridad que serán probados a intervalos regulares con el fin de asegurar que son confiables en caso de emergencia y retenidas por un periodo de tiempo determinado, por ejemplo: El líder de la división de sistemas o su delegado revisará semanalmente las copias de seguridad y llevará un registro de dicho procedimiento.
- El jefe de la División de Sistemas establecerá procedimientos explícitos de resguardo y recuperación de la información que incluyan especificaciones acerca del traslado, frecuencia, identificación y definirá conjuntamente con las dependencias los períodos de retención de la misma. Adicionalmente, debe disponer de los recursos necesarios para permitir la identificación relacionada 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.
- Las dependencias que administren sistemas de información tienen la responsabilidad de adoptar y cumplir las normas definidas para la creación y el manejo de copias de seguridad.

## Control de software operacional

- No se permite la instalación de software que viole las leyes de propiedad intelectual y derechos de autor, en especial la ley 23 de 1982 y su modificación, la ley 44 de 1993 y la Decisión 351 de 1993. Ver la normatividad en la página: *www.cecolda.org.co/index.php/derecho-de-autor/normasjurisprudencia/normas-nacionales*
- Las instalaciones de software deben ser aprobadas por el líder de la división de Sistemas y en el caso de encontrarse software ilegal en la Universidad, será reportado como incidente de seguridad y posteriormente investigado.

# 6. SEGURIDAD DE LAS COMUNICACIONES

Los usuarios y funcionarios deben proteger la información utilizada en la infraestructura tecnológica de la Universidad. De igual forma, deberán proteger la información reservada o confidencial que por necesidades de la institución deba ser guardada, almacenada o transmitida, ya sea dentro de la red interna a otras dependencias o redes externas como internet.

**Gestión de la seguridad de las redes**

- La plataforma de Tecnologías de la Información de la Universidad que soporta los sistemas de Información debe estar separada en segmentos de red físicos y lógicos e independientes de los segmentos de red de usuarios, de conexiones con redes de terceros y del acceso a Internet. La división de estos segmentos debe ser realizada por medio de dispositivos perimetrales e internos de enrutamiento y de seguridad si así se requiere.
- El líder de comunicaciones o quien tenga a cargo la seguridad de la información en el área, monitoreará permanentemente el tráfico de la red para detectar actividades inusuales o detrimento en el desempeño de la red.
- Todo equipo de TI debe ser revisado, registrado y aprobado por el líder de la división de Sistemas antes de conectarse a cualquier nodo de la red de comunicaciones, así mismo, desconectará aquellos dispositivos que no estén aprobados y reportará tal conexión como un incidente de seguridad a ser investigado.
- Se implementarán normas, procedimientos y controles para proteger el intercambio de información a través de medios de comunicaciones de voz, fax y vídeo.

## 7. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS

Todos los sistemas informáticos, tanto desarrollos propios o de terceros, y a todos los Sistemas Operativos, Bases de Datos y Aplicaciones de software que se utilicen en la Universidad deben tener inmersos controles de seguridad de la información.

- Las empresas con las cuales se realicen adquisiciones de software, deben tener reconocimiento a nivel nacional.
- Las aplicaciones contarán con mecanismos como Log de Auditoría, en el cual quedará registrado el usuario, la fecha, hora, módulo y opción a la que ingresó, facilitando al Oficial de seguridad de la información, la revisión de incidentes en el manejo de las aplicaciones.
- Se debe llevar una Bitácora con el control de cambios de las aplicaciones, indicando la fecha, hora, aplicación a la que se realizó el cambio, la causa, los cambios realizados y la persona que lo realizó.
- Se establecerán procedimientos para validar la salida de los datos de las aplicaciones, incluyendo: Comprobaciones de la razonabilidad para probar si los datos de salida son plausibles; control de conciliación de cuentas para asegurar el procesamiento de todos los datos, provisión de información suficiente, para que el lector o sistema de procesamiento subsiguiente determine la exactitud, totalidad, precisión y clasificación de la información; procedimientos para responder a las pruebas de validación de salidas, definición de las responsabilidades de todo el personal involucrado en el proceso de salida de datos.
- Se garantizará que las actividades de soporte a los Sistemas existentes y a los que se desarrollen o adquieran se lleven a cabo de manera segura, controlando el acceso a los archivos del mismo.
- Toda vez que sea necesario realizar un cambio en un Sistema Operativo, los sistemas serán revisados para asegurar que no se produzca un impacto en su funcionamiento o seguridad.

# 8. GESTION DE INCIDENTES

Eventos aleatorios, causados por el hombre o por la naturaleza, previsibles o no, tales como el terrorismo, terremotos, fallas de la tecnología, entre otros, pueden generar interrupciones a la Universidad en la entrega de productos y servicios. La posibilidad de que se presenten estos eventos, unido a la extrema dificultad para su predicción, incentiva desde hace muchos años a las organizaciones a que establezcan lineamientos para la gestión de continuidad del negocio, con el fin de seguir entregando sus productos y servicios a un nivel aceptable. Una adecuada gestión de incidentes relacionados con la administración de la información le permitirá a la Universidad Francisco de Paula Santander:

- Responder a los incidentes de manera sistemática, eficiente y rápida.
- Estar preparado ante la materialización de incidentes inesperados con el fin de volver a la normalidad en poco tiempo.
- Evitar al máximo la pérdida de información y de activos relacionados con el tratamiento, procesamiento y almacenamiento de la misma.
- Trabajar continuamente por mejorar en la gestión y tratamiento de incidentes.
- Generar una base de conocimientos sobre Incidentes.
- Evitar en lo posible, incidentes repetitivos.

**Reportes de Incidencias de seguridad informática.**

El oficial de Seguridad de la Información designado por la Universidad, comunicará cualquier incidencia al Comité de Seguridad de la Información y diligenciará un formato donde quede consignados los datos de reporte del incidente y de la persona que reportó:

| REPORTE DE INCIDENTES |
|---|
| Datos del reporte de incidencia<br>• Número<br>• Fecha<br>• Hora<br>• Descripción del incidente<br>• Efectos Producidos<br>• Responsable del activo afectado<br>• Causas del incidente (se diligencia, una vez se recupere la normalidad del proceso afectado) |
| Datos del reportante:<br>• Nombre<br>• Cargo<br>• Dependencia<br>• Correo |

- Todos los funcionarios de la Universidad, contratistas y terceros que son usuarios de los sistemas y servicios de información deben anotar y comunicar cualquier debilidad observada o sospechada en la seguridad de los mismos.
- Una vez verificada una incidencia, el oficial de Seguridad de la Información recolectará la información que le permitirá determinar el alcance del incidente, qué redes y que sistemas y aplicaciones fueron afectados, y que fue lo que generó el incidente, como ocurrió o está ocurriendo, también nos permite saber que originó el hecho, cómo ocurrió y las herramientas utilizadas; qué vulnerabilidades fueron explotadas y el impacto negativo que pueda tener sobre la Universidad.

Para determinar el alcance, el oficial de Seguridad de la Información puede hacerse las siguientes preguntas:

- ¿Cuántos equipos fueron comprometidos?

- ¿Cuántas redes y subredes se vieron afectadas?

- ¿Hasta qué punto de la red logró penetrar el atacante?

- ¿Qué nivel de privilegio logró el atacante?

- ¿Qué es lo que está en riesgo?

- ¿Cómo impacta este incidente en el desarrollo normal de las actividades misionales y de soporte de la Universidad?

- ¿Se encuentran en riesgo aplicaciones críticas?

- ¿Cuán conocida es la vulnerabilidad explotada por el atacante?

- ¿Hay otros equipos con la misma vulnerabilidad?

- Se deberían establecer las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, efectiva y ordenada a los incidentes en la seguridad de información.
- Determinado el alcance del incidente de seguridad, el oficial de Seguridad de la Información procederá a la contención, respuesta y puesta en marcha de las operaciones afectadas por el incidente.

La **contención,** evitará que el incidente siga produciendo daños. La **erradicación** eliminará la causa del incidente y todo rastro de los daños y la **recuperación**, consiste en volver el entorno afectado a su estado original.

Para llevar a cabo estas acciones, se tendrán que contar con estrategias que permitan realizar las operaciones de manera organizada, rápida y efectiva.

Para contar con una buena estrategia tengamos en cuenta estos agentes:

- Daño potencial de recursos a causa del incidente

- Necesidad de preservación de evidencia

- Tiempo y recursos necesarios para poner en práctica la estrategia

- Efectividad de la estrategia total o parcialmente

- Duración de las medidas a tomar

- Criticidad de los sistemas afectados

- Características de los posibles atacantes

- Si el incidente es de conocimiento público

- Pérdida económica

- Posibles implicancias legales

- Relación costo-beneficio de la estrategia

- Experiencias anteriores

- El oficial de Seguridad de la Información, una vez neutralizado el incidente, procederá a investigar las causas de dicho incidente. Las causas se registrarán en el formato de reporte de incidentes.

La recolección de información cuando se investigan las causas debe respetar los siguientes puntos:

- **AUTENTICIDAD**: Quien haya recolectado la evidencia debe poder probar que es auténtica.

- **CADENA DE CUSTODIA**: Registro detallado del tratamiento de la evidencia, incluyendo quiénes, cómo y cuándo la transportaron, almacenaron y analizaron, a fin de evitar alteraciones o modificaciones que comprometan la misma.

- **VALIDACION**: Garantizar que la evidencia recolectada es la misma que la presentada ante las autoridades.

- **CUMPLIMIENTO** Todo uso y seguimiento de la seguridad de la información en la Universidad debe estar de acuerdo a las normas así como a la legislación nacional en la materia, incluido, pero no restringido a:

**Constitución Política de Colombia:**

**Artículo. 61**.- El Estado protegerá la propiedad intelectual por el tiempo y mediante las formalidades que establezca la ley.

**Ley 23 de 1982** Establece los derechos de autor.

**Ley 1266 de 2008** (Habeas Data)

**Ley 1273** Delitos Informáticos

**Ley 1581** Protección de datos personales

**Ley 488 de 1998** Se elimina el ajuste integral por inflación fiscal para los inventarios, ingresos, costos y gastos. Por expresa disposición del artículo 14 de la mencionada ley, estos cambios tienen efectos contables.

Plan único de cuentas

Decreto 2193 aplicativo SIHO

Normas de auditoría generalmente aceptadas NAGA

Decreto 2193 del MDPS

**ISO 27002:** Guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información. No es certificable.

# 9. REFERENCIAS


Gobierno en Linea, M. d. (2011). *Lineamientos para la implementación del modelo de seguridad de las información.* Bogotá.

**ISO 27001:2013.** Sistemas de gestión de Seguridad en la Información– Requerimientos.

**ISO 27001:2005.** Sistemas de gestión de Seguridad en la Información– Requerimientos.

**ISO/IEC 133351: 2004.** Tecnología de la información – Técnicas de seguridad – Gestión de seguridad en tecnología de información y comunicaciones – Parte 1: Conceptos y modelos para la gestión de seguridad en la tecnología de la información y comunicaciones

**ISO/IEC TR 133353: 1998**. Lineamientos para la Gestión de Seguridad TI – Parte 3: Técnicas para la gestión de la seguridad TI .

**ISO/IEC 133354: 2000.** Lineamientos para la Gestión de la Seguridad TI – Parte 4: Selección de salvaguardas.

**ISO 14001:2004.** Sistemas de gestión ambiental – Requerimientos con lineamiento para su uso.

**ISO/IEC TR 18044:2004**.Tecnología de la información – Técnicas de seguridad – Gestión de incidentes en la seguridad de la información.