UNIVERSIDAD
NACIONAL
DE COLOMBIA

POLÍTICA DE SEGURIDAD INFORMÁTICA Y DE LA INFORMACIÓN

Documento Privado

11 DE OCTUBRE DE 2015

DIRECCIÓN NACIONAL DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES
Vicerrectoría General

SEGURIDAD DE LA INFORMACIÓN

POLÍTICA DE SEGURIDAD INFORMÁTICA Y DE LA INFORMACIÓN
DE LA UNIVERSIDAD NACIONAL DE COLOMBIA.

Bogotá, D.C., Versión 0.2
11 de octubre de 2015

INTRODUCCIÓN

La Dirección Nacional de Tecnologías de la Información y las Comunicaciones (DNTIC) acorde a lo dispuesto en el Artículo 6 de la Resolución 464 de 2014 de la Rectoría, diseña y elabora la propuesta de Políticas en materia de tecnologías de la información y de las comunicaciones y realiza el presente documento de Políticas de Seguridad Informática y de la Información, para que sea un instrumento no solo de concientización, sino de materialización para hacer efectivas las obligaciones de responsables y usuarios de infraestructura, controles, servicios, activos informáticos e información de carácter misional e institucional.

La sensibilidad de la información, infraestructura y servicios asociados exige la coordinación de toda la comunidad académica e institucional, a efectos de promover la superación de fallas y debilidades en protección y seguridad informática y de la información, que permitan a la Institución cumplir con su responsabilidad misional.

La Universidad Nacional de Colombia en atención a la exigencia de todos los requisitos legales, normativos y regulatorios, debe cumplir con estándares de Seguridad en sus sistemas misionales, servicios y protección de la información sensible, garantizando la confidencialidad de los datos, la disponibilidad de sistemas de información y la red y la integridad de la información, para lo cual adopta de manera voluntaria las disposiciones de la norma internacional de seguridad ISO27001.

En consecuencia, el documento de Políticas de Seguridad Informática y de la Información se encuentra disponible para toda la comunidad académica e institucional.

--- Blanco dejado intencionalmente ---

Tabla de Contenido

1. OBJETIVO GENERAL

Presentar los elementos que conforman la política de seguridad informática y de la información que debe conocer, acatar y cumplir toda la comunidad académica e institucional, incluyendo funcionarios contratistas y terceros que presten sus servicios o tengan algún tipo de relación con la Universidad.

Definir las directrices (*también llamadas políticas específicas*), para la correcta valoración, análisis y evaluación de los riesgos de seguridad asociados a la información y su impacto, identificando y evaluando diferentes opciones para su tratamiento, con el fin de garantizar la continuidad e integridad de los sistemas de información misionales de la Universidad (*véase el alcance del presente documento*).

--- Blanco dejado intencionalmente ---

2. MARCO DE REGULATORIO DE LA SEGURIDAD (MRS)

a. De conformidad con los lineamientos determinados por la Rectoría[1], la seguridad informática y de la información se constituirá en un mecanismo fundamental para que las dependencias de la Universidad garanticen la recolección oportuna y técnica, la trascripción, el análisis, la divulgación y el mantenimiento de los datos necesarios para la eficiente, eficaz y efectiva operación de los sistemas de información de la gestión académica y administrativa.
b. Propendiendo por el mejoramiento continuo, formará parte de nuestra cultura y ética[2] institucional, la seguridad informática y de la información con sujeción a los valores corporativos y a la gestión misional, orientada por valores como la transparencia, equidad, justicia, responsabilidad, rectitud e inclusión. La seguridad informática y de la información fortalecerá la gestión de tecnología informática y del riesgo y del uso eficiente y razonable de los recursos provistos, con miras a obtener un impacto positivo a nivel institucional.
c. La operacionalización de la Seguridad informática y de la información, incluirá y garantizará que las personas vinculadas[3] y aquellas que se vinculen a la institución en forma permanente o temporal (incluyendo contratistas), cumplan con los requisitos establecidos en la presente resolución para la ejecución idónea de las funciones y responsabilidades contratadas. De igual manera sus miembros ejercerán sus funciones procurando alcanzar los más altos estándares de desempeño con pleno acatamiento a las políticas de seguridad informática y de la información que aquí se establecen.
d. De conformidad con los principios de no duplicidad funcional y de eficiencia[4], el área responsable de desarrollar los mecanismos para la aplicación de las Políticas de Seguridad informática y de la información y sus Directrices o Políticas Específicas es la Dirección Nacional de Tecnologías de la Información y las Comunicaciones (DNTIC), en desarrollo de las disposiciones propias de aplicación institucional y en concordancia con el Artículo 6 de la Resolución 464 de 2014, expedido por la Rectoría.
e. De conformidad con el Acuerdo 035 de 2003 expedido por el Consejo Académico de la Universidad, los mecanismos y demás disposiciones de seguridad informática y de la información se aplicarán en todas aquellas actividades de carácter académico, laboral o contractual que tengan por objeto la creación intelectual en los campos

[1] Numeral 9, Artículo 4. Principios de la organización, Acuerdo Número 011 de 2005 "Estatuto general de la Universidad Nacional de Colombia", Publicado [http://www.unal.edu.co/estatutos/egeneral/egeca01.html].
[2] Ibídem Numeral 12. Ética.
[3] Ibídem Numeral 14. Idoneidad.
[4] Ibídem Numeral 1, Artículo 15. Régimen de autonomía.

del derecho de autor, derechos conexos, la propiedad industrial y las nuevas tecnologías, en la Universidad Nacional de Colombia.

f. En cumplimiento a lo dispuesto en la Ley estatutaria 1581 de 2012 y a su Decreto Reglamentario 1377 de 2013, la presente Política de Seguridad Informática y de la Información y los mecanismos para tales fines, son aplicables a la Institución para el tratamiento y protección de datos personales[5].
g. En cumplimiento al literal j) Artículo 2 del Acuerdo 016 de 2011 expedido por el Consejo Superior Universitario, se garantizarán los procesos de aprovechamiento responsable de los recursos naturales, fomentando actitudes de ahorro, reducción, recuperación, reutilización y reciclaje en lo referente a deterioro, desgaste, eliminación y retiro por daño y obsolescencia de tecnología informática como un principio básico de la seguridad informática y de la información.
h. En cumplimiento a las disposiciones descritas en la Resolución 1428 de 2006 expedida por la Rectoría; el esquema de organización y el conjunto de planes, programas, principios, normas, procedimientos y mecanismos de verificación y evaluación de la presente Política de Seguridad Informática y de la Información y los mecanismos para tales fines se incorporarán en su efecto al Sistema de Control Interno, para asegurar que todas las actividades y actuaciones así como los mecanismos de información, seguimiento y control, demás recursos y desarrollos aplicados, se realicen de acuerdo con las normas vigentes dentro de las políticas trazadas por la Rectoría y en atención a las metas u objetivos institucionales.
i. En desarrollo del marco de cooperación científica y tecnológica realizado por la Universidad Nacional de Colombia en convenio con otras universidades nacionales o internacionales o entidades públicas o privadas, se hace necesario aprovechar entre otros, los recursos tecnológicos de redes e infraestructura de tecnología informática, así como de aplicaciones y sistemas de información institucional; para lo cual será de estricta aplicación, la presente Política de Seguridad Informática y de la Información y los mecanismos para tales fines.

3. ALCANCE DEL SI

El ámbito de aplicación del Sistema de Seguridad de la Información (SI) para el cual se desarrolla la presente Política de Seguridad Informática y de la Información es:

a. Los Sistemas de Información tanto de misión crítica como de apoyo.
b. Los demás activos de información que la DNTIC estipule en sus directrices técnicas o políticas específicas de seguridad.

[5] POLÍTICA DE TRATAMIENTO PROTECCIÓN DE DATOS PERSONALES DE LOS TITUARES DE LA UNIVERSIDAD NACIONAL DE COLOMBIA, Publicado [http://www.unal.edu.co/contenido/habeas/POLITICA%20DE%20TRATAMIENTO%20DE%20DATOS.pdf]

El alcance para cada uno de los anteriores activos cubre:

3.1. **Activos de información**: sean estos: Datos, Aplicativos o Sistemas de Información, Personal, Servicios informáticos, Tecnología - Infraestructura de tecnología informática y de las comunicaciones TICs, Instalaciones y Equipamiento auxiliar.

3.2. **Procesos y subprocesos:** donde se gestione información de los Sistemas Misionales.

3.3. **Estructura organizacional**: propio de la gestión de tecnología informática de cada sede y a nivel nacional incluyendo aquella, bien sea en funciones o roles, relativa a competencias de administración y gestión de la seguridad informática.

--- Blanco dejado intencionalmente ---

4. POLITICA DE SEGURIDAD INFORMATICA Y DE LA INFORMACIÓN

4.1. POLITICA GENERAL

4.1.1. Objetivos

a. Definir las disposiciones de propósito general para asegurar una adecuada protección de la información de la Universidad.
b. Apoyar y orientar a las instancias directivas en materia de seguridad informática y de la información, de acuerdo con los requisitos del negocio y los reglamentos y las leyes aplicables.
c. Proteger, preservar y administrar objetivamente la información de la Universidad, junto con las tecnologías informáticas utilizadas para su procesamiento frente a amenazas internas o externas (*deliberadas o accidentales*), con el fin de asegurar el cumplimiento de las características de confidencialidad, integridad, disponibilidad, legalidad, confiabilidad y no repudio de la información.
d. Mantener la Política de Seguridad informática y de la Información actualizada, vigente, operativa y auditada dentro del marco determinado por los riesgos globales y específicos de la Universidad para asegurar su permanencia y nivel de eficacia.

4.1.2. Disposición

La información es un recurso vital para el desarrollo misional e institucional de la Universidad que, como el resto de los activos, tiene un valor relevante y por consiguiente debe ser debidamente protegida.

El establecimiento, implementación, seguimiento, mejora continua y aplicación de la Política de Seguridad de la Información garantiza y expresa un compromiso ineludible de toda la comunidad académica e institucional a realizar todos los esfuerzos de protección frente a una amplia gama de amenazas y peligros a la que hoy se encuentra expuesta la información.

Con esta política se contribuye a minimizar los riesgos asociados a pérdida, robo, daño, uso intencionado y no intencionado y se asegura el eficiente cumplimiento de las funciones y actividades misionales apoyadas en un correcto funcionamiento de la plataforma e infraestructura de tecnología informática y sistemas de información misionales asociados.

La Universidad Nacional de Colombia, en consonancia a lo establecido en el Artículo 6 de la Resolución 464 de 2014 expedida por la Rectoría, delega en la Dirección Nacional de Tecnologías de Información y las Comunicaciones (DNTIC) las funciones de definir los estándares y lineamientos técnicos para la gestión de TIC, liderar y orientar la gestión de tecnologías de información y comunicaciones, evaluar y hacer seguimiento a la gestión de TICs a nivel nacional, de sedes y facultades; orientar, proponer y contratar la infraestructura de la plataforma tecnológica y desarrollar o contratar soluciones de TICs de carácter transversal e institucional, así como orientar, proponer y contratar los

sistemas de seguridad, de contingencia y de buen uso de los recursos informáticos y de comunicaciones, para mejorar el nivel de seguridad y confiabilidad de los sistemas de información de la Universidad.

Según se indica en el Articulo 4 del Acuerdo 046 de 2009 expedido por el Consejo Superior Universitario, se faculta a DNTIC para que de aplicación a las políticas de informática y comunicaciones mediante la emisión de directrices técnicas de acuerdo con la normatividad vigente de aplicación institucional. En materia de seguridad y respaldo de la información, el Articulo 8 del Acuerdo en comento, define a DNTIC con el apoyo y la activa participación de las Oficinas de Tecnología Informática y las Comunicaciones o centros de cómputo (*en adelante OTICs*), para que implemente mecanismos necesarios para garantizar la integridad, confiabilidad, oportunidad, disponibilidad y la seguridad en los sistemas informáticos y de comunicaciones de la Universidad. A tenor seguido, se resalta que las dependencias usuarias tendrán como responsabilidad velar por el manejo y mantenimiento adecuado de los datos, en cuanto a consulta, ingreso, modificación, eliminación o divulgación de los mismos referentes al sistema de información y que el responsable de la información contenida en sus equipos es el usuario final, sea este funcionario o contratista.

En honor a lo expuesto, la presente Política de Seguridad informática y de la información, cumple una función estratégica mediante la cual se reconoce que las tecnologías de la información y las comunicaciones son herramientas necesarias para el desarrollo Institucional, pero que conlleva riesgos inherentes que deben ser mitigados. Los delitos informáticos no detectados, no detenidos, no minimizados y sin capacidad de determinación de su fuente o pasos donde dejo rastro, tienen el potencial de erosionar la confianza y fe institucional perjudicando de este modo el desarrollo misional de la Universidad. Por consiguiente, la definición de estrategia de la seguridad ha sido considerada en el párrafo anterior y se desarrollará en torno a las siguientes áreas clave de manera transversal a procesos y servicios que requieran el uso de activos informáticos a nivel institucional: i) Medidas Técnicas; ii) recursos humanos y desarrollo de capacidades; iii) legal y regulatorio; y (iv) Educación y conciencia institucional y pública.

La presente Política de Seguridad Informática y de la información se convierte en un canal de comunicación entre todos los miembros de la comunidad institucional y universitaria, lo que incluye en su apreciación de unidad, la configuración de un conjunto de disposiciones, que sujeten a los usuarios a mantener una alta responsabilidad derivada de la manipulación o uso de diferentes Activos de Información, infraestructura y servicios tecnológicos informáticos a disposición de la misión institucional. Algunas de estas disposiciones en mención son: Directrices técnicas, específicas, normativas y procedimentales, estándares, instructivos u otras disposiciones que serán definidas por DNTIC para desarrollar los lineamientos de la seguridad informática.

Se incorpora como parte del Sistema de Gestión de Calidad, la regulación y puesta en operación de la Política de Seguridad Informática y de la Información, con miras que toda la comunidad académica e institucional sea responsable y mantenga habilitados y en correcto funcionamiento controles de protección contra perdida, daño, uso intencionado y no-intencionado y modificación de información o de su procesamiento en aras de hacer efectiva la correcta administración y prestación de las obligaciones y responsabilidades de los usuarios de los servicios de tecnologías informáticas de Universidad.

4.1.3. Aplicabilidad

Esta política es de aplicación a todas las dependencias que componen la comunidad académica e institucional, a sus recursos, a la totalidad de los procesos internos o externos vinculados a la universidad a través de contratos, convenios o acuerdos con terceros y a todo el personal de la Universidad Nacional de Colombia, cualquiera sea su vinculación, la dependencia a la cual se encuentre adscrito y el nivel de las tareas que desempeñe dentro de alcance definido para la Seguridad informática y de la información y en general a todos los usuarios de la información o aquellos que sean beneficiados con el uso de la infraestructura, servicios, sistemas misionales de la Universidad.

4.1.4. Responsabilidad

a. La Dirección Nacional de Tecnologías de la Información y las Comunicaciones (DNTIC) con la participación de las Oficinas de Tecnologías de la información y de las Comunicaciones (OTICs), diseña y elabora la propuesta de Políticas de Seguridad informáticas y de las información que son presentadas al Comité Nacional de Informática y Comunicaciones (CNTIC), quien propone y presenta esta propuesta al Consejo Superior Universitario (CSU), para que recomiende aprobar el texto de la Política de Seguridad de la Información, las funciones generales en materia de seguridad de la información y la estructuración, seguimiento y mejora de la Seguridad Informática y de la Información de la Universidad.
b. Es responsabilidad del CNTIC definir las estrategias de capacitación en materia de seguridad de la información al interior de la Universidad.
c. El grupo responsable de Seguridad Informática se configura de la siguiente manera: Gobierno de seguridad y operaciones de Seguridad. El Gobierno de la Seguridad es responsabilidad de DNTIC y tiene como función principal velar por el gobierno corporativo de la seguridad, emitir disposiciones relativas a la materia y practicar evaluaciones, control, seguimiento y auditorías de seguridad que evidencien el nivel de maduración de la seguridad en la institución. La operación y gestión de la seguridad es responsabilidad de cada una de las OTIC y deberá cumplir funciones relativas a la seguridad de los sistemas de información misionales, su infraestructura, servicios y activos de información asociados. El nivel de supervisión que pueda realizar cada grupo responsable de seguridad está relacionado con el talento humano que lo conforma y en todo caso deberá ser aprobado por el CSU.

d. La Dirección Nacional de Personal Académico y Administrativo de la Vicerrectoría General, cumplirá la función de notificar a las sedes, para que éstas a través de la Secretaria de Sede notifiquen a todo el personal que se vincula contractualmente con la Universidad, de las obligaciones respecto del cumplimiento de la Política de Seguridad informática y de la Información y de todos las directrices, estándares, procesos, procedimientos, prácticas y guías que surjan de la Seguridad de la Información; adscrita al Sistema de Control Interno y al Sistema de Gestión de Calidad Institucional. De igual forma, será responsable de la notificación de la presente Política y de los cambios que en ella se produzcan a todo el personal, por medio de los canales establecidos a través de la suscripción de los Compromisos de Confidencialidad y de tareas de capacitación continua en materia de seguridad según lineamientos dictados por CNTIC.
e. El Director de la Dirección Jurídica Nacional verificará el cumplimiento de la presente Política en la gestión de convenios, acuerdos u otra documentación de la Institución con empleados y con terceros. Asimismo, asesorará en materia legal a la entidad en lo que se refiere a la seguridad de la información.
f. La Gerencia Nacional Financiera y Administrativa, a través de sus Divisiones de gestión de la contratación, verificará el cumplimiento de la presente Política en la gestión de todos los contratos firmados entre la Institución y terceros en lo que se refiere a la seguridad de la información.
g. Los usuarios de la información, infraestructura tecnológica, servicios utilizados para su procesamiento y sistemas misionales son responsables de conocer y cumplir la Política de Seguridad de la Información vigente.
h. La DNTIC es responsable de practicar auditorías periódicas sobre los sistemas y actividades vinculadas con la gestión de activos de información y la tecnología de información. Es su responsabilidad informar sobre el cumplimiento de las especificaciones y medidas de seguridad de la información establecidas por esta Política y por las normas, procedimientos y prácticas que de ella surjan.

4.1.5. Reglas

1. Establecer, implementar, hacer seguimiento, auditar y promover la mejora continua de la Política de Seguridad de la Información en toda la Comunidad Universitaria.
2. Desarrollar y mantener actualizado un inventario de activos de información y recursos tecnológicos y brindar esta información a DNTIC para mantener actualizado el repositorio de arquitectura de seguridad informática que compone el marco de arquitectura empresarial.
3. Establecer indicadores que determinen y aseguren el eficiente cumplimiento de las funciones y actividades misionales en las que se demuestre cómo se ha logrado minimizar los riesgos asociados de pérdida, robo, daño, uso intencionado y no-intencionado de información.
4. Definir los estándares y lineamientos técnicos para la gestión de seguridad informática y de la información de TICs en los niveles nacional, sedes y facultades.

5. Evaluar y hacer seguimiento a la gestión de Seguridad informática y de la Información de TICs a nivel nacional, de sedes y facultades.
6. Orientar, proponer y contratar los sistemas de seguridad y contingencia y de buen uso de los recursos informáticos y de comunicaciones, para mejorar el nivel de seguridad y confiabilidad de los sistemas de información de la universidad.
7. Implementar los mecanismos necesarios para garantizar la integridad, confiabilidad, oportunidad, disponibilidad y la seguridad en los sistemas informáticos y de comunicaciones de la Universidad.
8. Establecer y responder por el manejo y mantenimiento adecuado de los datos, en cuanto a consulta, ingreso, modificación, eliminación o divulgación de los datos de los Sistemas de Información Misionales y demás Activos de Información y verificar mediante auditorías internas su cumplimiento.
9. Verificar que los usuarios finales (sean funcionarios o contratistas), se hacen responsables de la información contenida en sus equipos.
10. Instaurar y verificar que procesos y servicios que requieran el uso de activos informáticos a nivel institucional cuentan con los componentes de seguridad informática y de la información: i) Medidas Técnicas; ii) recursos humanos y desarrollo de capacidades; iii) legal y regulatorio; y (iv) Educación y conciencia institucional y pública.
11. Emitir disposiciones en materia de seguridad (Directrices técnicas, específicas, normativas y procedimentales, estándares y lineamientos técnicos, instructivos u otras) de acuerdo con la normatividad vigente, que sujeten a los usuarios a mantener una alta responsabilidad respecto de la seguridad informática y de la información, derivada de la manipulación o uso de diferentes Activos de Información, infraestructura y servicios tecnológicos informáticos a disposición de la misión institucional.
12. Incorporar como parte del Sistema de Gestión de Calidad y del Control Interno la regulación y puesta en operación de la Política de Seguridad Informática y de la Información y verificar que toda la Comunidad Universitaria es responsable y mantiene habilitados y en correcto funcionamiento controles de protección contra perdida, daño, uso intencionado y no-intencionado y modificación de información o de su procesamiento para la prestación de las obligaciones y responsabilidades de los usuarios de los servicios de tecnologías informáticas de Universidad.
13. Establecer como requisito para la toma de decisiones en seguridad informática y de la información los resultados de la gestión del riesgo, con miras a obtener un impacto positivo a nivel institucional.
14. Validar la operacionalización de la seguridad informática y de la información en el ejercicio de funciones o roles, a bien de acatar las políticas y disposiciones aquí contenidas.
15. Incluir todas las disposiciones legales y reglamentarias en el ejercicio y demostración de la seguridad informática y de la información a todo nivel, aplicables a la institución en cumplimiento de la misión institucional.

16. Coordinar e integrar la seguridad informática y de la información a los diferentes sistemas de gestión de la Universidad sin que ello implique duplicidad o realización de esfuerzos aislados. Ej. Integración al Sistema de Control interno, al Sistema de Gestión de Calidad, al Sistema de Gestión Ambiental; entre otros.
17. Fortalecer el marco de cooperación científica y tecnológica realizado por la Universidad, facilitando mecanismos y recursos necesarios que garanticen el cumplimiento de la presente disposición de seguridad informática y de la información.
18. Implementar, revisar y actualizar las Políticas de seguridad informática y de la información a través de los mecanismos establecidos en el Sistema de Gestión de Calidad.
19. Diseñar, programar y realizar los programas de Auditoría a la Seguridad informática y de la información, los cuales estarán a cargo de los entes que ejercen el control interno y DNTIC.
20. El Rector, los Vicerrectores, Directores, gerentes, jefes de área o dependencia deben asegurar que todos los procedimientos de seguridad de la información dentro de su área de responsabilidad, se realizan correctamente para lograr el cumplimiento de las políticas y estándares de seguridad de la información de UNAL.

--- Blanco dejado intencionalmente ---

5. TERMINOS Y DEFINICIONES

- **Aceptación del Riesgo**: Decisión de aceptar un riesgo.
- **Activo:** (También tratado como **Activo(s) de información**) Según [ISO/lEC 13335-1:2004]: Cualquier cosa que tiene valor para la organización. También se entiende por 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 Nacional de Colombia. Se pueden clasificar de la siguiente manera:
    - **Datos**: Son todos aquellos elementos básicos de la información (en cualquier formato) que se generan, recogen, gestionan, transmiten y destruyen en UNAL. Ejemplo: archivo de Word "listado de personal.docx", entre otros o más formatos.
    - **Aplicaciones o Sistemas Misionales**: Es todo el software que se utiliza para la gestión de la información. Ejemplo: SIA. Sistema de Información Académico.
    - **Personal**: Es todo el personal de UNAL (funcionarios), el personal subcontratado (Contratista), los usuarios y en general, todos aquellos que tengan acceso de una manera u otra a los activos de información de UNAL.
    - **Servicios informáticos**: Son los servicios de tecnologías informáticas y de la Información, prestada por parte de las oficinas de tecnologías informáticas y de las comunicaciones (OTICs) entre las cuales se distinguen:
        - **Servicios de cliente**: Mesa de ayuda, video conferencia, soporte a computadores personales.
        - **Servicios de Seguridad informática y de la Información**: Manejo y administración de incidentes de seguridad, recuperación ante desastres, continuidad del negocio, investigaciones, operación de seguridad, monitoreo, auditoria de seguridad.
        - **Servicios a sistemas de información**
        - **Servicios intermedios**
        - **Servicios básicos**
        - **Servicios a servidores**: Hardware y equipo, almacenamiento, virtualización, sistemas operativos, bases de datos.
        - **Servicios de red**: Internet, WAN, LAN, Inalámbrica, telefonía
        - **Servicios Físicos**: Cableado, ductería, UPS, Aire acondicionado, Planta eléctrica, tableros
    - **Tecnología** (También denominado **Infraestructura de tecnología informática y de las comunicaciones TICs**): Son todos los equipos utilizados para gestionar la información y las comunicaciones Ejemplo: equipo de cómputo, teléfonos, impresoras.

  - **Instalaciones**: Son todos los lugares en los que se alojan los sistemas de información. Ejemplo: Oficina Pagaduría.
  - **Equipamiento auxiliar**: Son todos aquellos activos que dan soporte a los sistemas de información y que no se hallan en ninguno de los tipos anteriormente definidos. Ejemplo: Aire acondicionado, destructora de papel.
- **Administración de riesgos**: Gestión de riesgos, es un enfoque estructurado para manejar la incertidumbre relativa a una amenaza, a través de una secuencia de actividades humanas que incluyen evaluación de riesgo, estrategias de desarrollo para manejarlo y mitigación del riesgo utilizando recursos gerenciales. Las estrategias incluyen transferir el riesgo a otra parte, evadir el riesgo, reducir los efectos negativos del riesgo y aceptar algunas o todas las consecuencias de un riesgo particular.
- **Alcance:** Ámbito de la organización que queda sometido al SGSI (Siglas de Sistema de Gestión de Seguridad de la información. En delante SI – Seguridad informática y de la información). Debe incluir la identificación clara de las dependencias, interfaces y límites con el entorno, sobre todo si sólo incluye una parte de la organización.
- **Alerta**: Una notificación formal de que se ha producido un incidente relacionado con la seguridad de la información que puede evolucionar hasta convertirse en desastre.
- **Amenaza**: Según [ISO/lEC 13335-1:2004): causa potencial de un incidente no deseado, el cual puede causar el daño a un sistema o la organización.
- **Análisis de riesgos**: Según [ISO/lEC Guía 73:2002): Uso sistemático de la información para identificar fuentes y estimar el riesgo.
- **Auditabilidad:** Los activos de información deben tener controles que permitan su revisión. Auditabilidad es permitir la reconstrucción, revisión y análisis de la secuencia de eventos.
- **Auditor:** Persona encargada de verificar, de manera independiente, la calidad e integridad del trabajo que se ha realizado en un área particular.
- **Auditoria**: Proceso planificado y sistemático en el cual un auditor obtiene evidencias objetivas que le permitan emitir un juicio informado sobre el estado y efectividad del SI de una organización.
- **Autenticación:** Proceso que tiene por objetivo asegurar la identificación de una persona o sistema.
- **Autenticidad**: Los activos de información solo pueden estar disponibles verificando la identidad de un sujeto o recurso, Propiedad que garantiza que la identidad de un sujeto o recurso es la que declara, Se aplica a entidades tales como usuarios, procesos, sistemas de información.
- **Características de la Información**: las principales características son la confidencialidad, la disponibilidad y la integridad.

- **Checklist**: Lista de apoyo para el auditor con los puntos a auditar, que ayuda a mantener claros los objetivos de la auditoría, sirve de evidencia del plan de auditoría, asegura su continuidad y profundidad y reduce los prejuicios del auditor y su carga de trabajo, Este tipo de listas también se pueden utilizar durante la implantación del SI para facilitar su desarrollo.
- **CobiT - Control Objectives for Information and related Technology**: Publicados y mantenidos por ISACA. Su misión es investigar, desarrollar, publicar y promover un conjunto de objetivos de control de Tecnología de Información rectores, actualizados, internacionales y generalmente aceptados para ser empleados por gerentes de empresas y auditores.
- **Compromiso de la Dirección**: Alineamiento firme de la Dirección de la organización con el establecimiento, implementación, operación, monitorización, revisión, mantenimiento y mejora del SI.
- **Computo forense**: El cómputo forense, también llamado informática forense, computación forense, análisis forense digital o examinación forense digital es la aplicación de técnicas científicas y analíticas especializadas a infraestructura tecnológica que permiten identificar, preservar, analizar y presentar datos que sean válidos dentro de un proceso legal.
- **Confiabilidad**: Se puede definir como la capacidad de un producto de realizar su función de la manera prevista, De otra forma, la confiabilidad se puede definir también como la probabilidad en que un producto realizará su función prevista sin incidentes por un período de tiempo especificado y bajo condiciones indicadas.
- **Confidencialidad**: Acceso a la información por parte únicamente de quienes estén autorizados, Según [ISO/lEC 13335-1:2004]: "característica/propiedad por la que la información no está disponible o revelada a individuos, entidades, o procesos no autorizados".
- **Control**: Las políticas, los procedimientos, los mecanismos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido, (Nota: Control es también utilizado como sinónimo de salvaguarda).
- **Control correctivo**: Control que corrige un riesgo, error, omisión o acto deliberado antes de que produzca pérdidas. Supone que la amenaza ya se ha materializado pero que se corrige.
- **Control detectivo**: Control que detecta la aparición de un riesgo, error, omisión o acto deliberado. Supone que la amenaza ya se ha materializado, pero por sí mismo no la corrige.
- **Control disuasorio**: Control que reduce la posibilidad de materialización de una amenaza, p.ej., por medio de avisos disuasorios.
- **Control preventivo**: Control que evita que se produzca un riesgo, error, omisión o acto deliberado. Impide que una amenaza llegue siquiera a materializarse.

- **Declaración de aplicabilidad** (*En inglés SOA – Statement Of Applicability*): Documento que enumera los controles aplicados por el SI de la organización - tras el resultado de los procesos de evaluación y tratamiento de riesgos- además de la justificación tanto de su selección como de la exclusión de controles incluidos en la norma.
- **Desastre**: Cualquier evento accidental, natural o malintencionado que interrumpe las operaciones o servicios habituales de una organización durante el tiempo suficiente como para verse la misma afectada de manera significativa.
- **Directiva**: Según [ISO/lEC 13335-1: 2004): una descripción que clarifica qué debería ser hecho y cómo, con el propósito de alcanzar los objetivos establecidos en las políticas.
- **Disponibilidad**: Según [ISO/lEC 13335-1: 2004): característica o propiedad de permanecer accesible y disponible para su uso cuando lo requiera una entidad autorizada.
- **Evaluación de riesgos:** Según [ISO/lEC Guía 73:2002]: proceso de comparar el riesgo estimado contra un criterio de riesgo dado con el objeto de determinar la importancia del riesgo.
- **Evento**: Según [ISO/lEC TR 18044:2004]: Suceso identificado en un sistema, servicio o estado de la red que indica una posible brecha en la política de seguridad de la información o fallo de las salvaguardas, o una situación anterior desconocida que podría ser relevante para la seguridad.
- **Evidencia objetiva:** Información, registro o declaración de hechos, cualitativa o cuantitativa, verificable y basada en observación, medida o test, sobre aspectos relacionados con la confidencialidad, integridad o disponibilidad de un proceso o servicio o con la existencia e implementación de un elemento del sistema de seguridad de la información.
- **Gestión de claves**: Controles referidos a la gestión de claves criptográficas.
- **Gestión de riesgos:** Proceso de identificación, control y minimización o eliminación, a un costo aceptable, de los riesgos que afecten a la información de la organización. Incluye la valoración de riesgos y el tratamiento de riesgos. Según [ISO/lEC Guía 73:2002]: actividades coordinadas para dirigir y controlar una organización con respecto al riesgo.
- **Gusanos**: Es un programa de computador que tiene la capacidad de duplicarse a sí mismo. A diferencia del virus, no precisa alterar los archivos de programas, sino que reside en la memoria y se duplica a sí mismo. Siempre dañan la red (aunque sea simplemente consumiendo ancho de banda).
- **Identidad Digital**: Es un identificador asignado dentro del Directorio de Identidades Digitales, que permite acceso a los diferentes servicios que ofrece la Universidad.
- **Identidad Temporal**: Rol de Identidades Digitales asociadas a personas o entidades no adscritas a la comunidad universitaria ni a la estructura administrativa institucional.

- **Interventor/Supervisor**: Se denomina Interventor la persona natural o jurídica que en razón a su conocimiento especializado o experiencia en el área del objeto contractual es contratada por la Universidad para que ejerza el seguimiento técnico, administrativo, jurídico, financiero y contable sobre el cumplimiento de la orden Contractual o Contrato, cuando la complejidad o la extensión del mismo lo justifiquen. Se denomina supervisor el servidor público de la Universidad designado para ejercer el seguimiento técnico, administrativo, jurídico, financiero y contable que garantice el cumplimiento del objeto de una orden contractual o contrato[6].
- **Impacto**: Resultado de un incidente de seguridad de la información.
- **Incidente:** Según [ISO/lEC TR 18044:2004]: 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.
- **Información:** La información constituye un importante activo, esencial para las actividades de una organización y, en consecuencia, necesita una protección adecuada. La información puede existir de muchas maneras. Puede estar impresa o escrita en papel, puede estar almacenada electrónicamente, ser transmitida por correo o por medios electrónicos, se la puede mostrar en videos, o exponer oralmente en conversaciones.
- **Ingeniería Social**: En el campo de la seguridad informática, es la práctica de obtener información confidencial a través de la manipulación de usuarios legítimos ganando su confianza muchas veces. Es una técnica que pueden utilizar investigadores privados, criminales, delincuentes computacionales (conocidos como cracker) para obtener información, acceso o privilegios en sistemas de información que les permiten realizar algún acto que perjudique o exponga a la persona o entidad a riesgos o abusos.
- **Integridad:** Mantenimiento de la exactitud y completitud de la información y sus métodos de proceso. Según [ISOIIEC 13335-1: 2004]: propiedad/característica de salvaguardar la exactitud y completitud de los activos.
- **Inventario de activos**: Lista de todos aquellos recursos (físicos, de información, software, documentos, servicios, personas, reputación de la organización, etc.) dentro del alcance del SI, que tengan valor para la organización y necesiten por tanto ser protegidos de potenciales riesgos.
- **IPS**: Sistema de prevención de intrusos. Es un dispositivo que ejerce el control de acceso en una red informática para proteger a los sistemas computacionales de ataques y abusos.

[6] Manual de Convenios y Contratos Resolución 1551 de 2014. Artículo 93. Parte III. Literal g. Informar al área técnica competente sobre el retiro del contratista, para eliminar claves y accesos autorizados sobre información de carácter confidencial de la Universidad.

- **ISO:** Organización Internacional de Normalización, con sede en Ginebra (Suiza). Es una agrupación de organizaciones nacionales de normalización cuyo objetivo es establecer, promocionar y gestionar estándares.
- **ISO 17799**: Código de buenas prácticas en gestión de la seguridad de la información adoptado por ISO transcribiendo la primera parte de BS7799. A su vez, da lugar a ISO 27002 por cambio de nomenclatura el 1 de Julio de 2007. No es certificable.
- **ISO 19011:** "Guidelines for quality and/or environmental management systems auditing". Guía de utilidad para el desarrollo de las funciones de auditor interno para un SGSI.
- **ISO 27001:** Estándar para sistemas de gestión de la seguridad de la información adoptado por ISO transcribiendo la segunda parte de BS 7799. Es certificable. Primera publicación en 2005. Actualmente está en vigencia ISO27001:2013
- **ISO 27002:** Código de buenas prácticas en gestión de la seguridad de la información (transcripción de ISO 17799). No es certificable. Cambio oficial de nomenclatura de ISO 17799:2005 a ISO 27002:2005 el 1 de Julio de 2007.
- **ISO 9000**: Normas de gestión y garantía de calidad definidas por la ISO.
- **ISO/IEC TR 13335-3**: "Information technology. Guidelines for the management of IT Security .Techniques for the management of IT Security." Guía de utilidad en la aplicación de metodologías de evaluación del riesgo.
- **ISO/IEC TR 18044**: "Information technology. Security techniques. Information security incident management". Guía de utilidad para la gestión de incidentes de seguridad de la información.
- **ITIL IT Infrastructure Library**: Un marco de gestión de los servicios de tecnologías de la información.
- **Legalidad:** El principio de legalidad o Primacía de la ley es un principio fundamental del Derecho público conforme al cual todo ejercicio del poder público debería estar sometido a la voluntad de la ley de su jurisdicción y no a la voluntad de las personas (ej. el Estado sometido a la constitución o al Imperio de la ley). Por esta razón se dice que el principio de legalidad establece la seguridad jurídica, Seguridad de Información, Seguridad informática y garantía de la información.
- **No conformidad**: Situación aislada que, basada en evidencias objetivas, demuestra el incumplimiento de algún aspecto de un requerimiento de control que permita dudar de la adecuación de las medidas para preservar la confidencialidad, integridad o disponibilidad de información sensible, o representa un riesgo menor.
- **No conformidad grave:** Ausencia o fallo de uno o varios requerimientos de la ISO 27001 que, basada en evidencias objetivas, permita dudar seriamente de la adecuación de las medidas para preservar la confidencialidad, integridad o disponibilidad de información sensible, o representa un riesgo inaceptable.

- **No repudio**: Los activos de información deben tener la capacidad para probar que una acción o un evento han tenido lugar, de modo que tal evento o acción no pueda ser negado posteriormente.
- **Plan de continuidad del negocio** (Bussines Continuity Plan): Plan orientado a permitir la continuación de las principales funciones de la Entidad en el caso de un evento imprevisto que las ponga en peligro.
- **Plan de tratamiento de riesgos** (Risk treatment plan): Documento de gestión que define las acciones para reducir, prevenir, transferir o asumir los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma.
- **Política de seguridad:** Documento que establece el compromiso de la Dirección y el enfoque de la organización en la gestión de la seguridad de la información. Según [ISO/lEC 27002:20005): intención y dirección general expresada formalmente por la Dirección.
- **Protección a la duplicidad:** La protección de copia, también conocida como prevención de copia, es una medida técnica diseñada para prevenir la duplicación de información. La protección de copia es a menudo tema de discusión y se piensa que en ocasiones puede violar los derechos de copia de los usuarios, por ejemplo, el derecho a hacer copias de seguridad de una videocinta que el usuario ha comprado de manera legal, el instalar un software de computadora en varias computadoras, o el subir la música a reproductores de audio digital para facilitar el acceso y escucharla.
- **Riesgo:** Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Según [ISO Guía 73:2002]: combinación de la probabilidad de un evento y sus consecuencias.
- **Riesgo Residual:** Según [ISOIIEC Guía 73:2002] El riesgo que permanece tras el tratamiento del riesgo.
- **Rol:** Carácter que se le atribuye a una Entidad Digital, de acuerdo al tipo de vinculación del usuario dentro de la Universidad. Los roles actuales son: Estudiante, Docente, Administrativo, Institucional, Contratista, Dependencia, Pensionado, Egresado, Temporal.
- **Salvaguarda:** Véase: Control.
- **Segregación de tareas**: Separar tareas sensibles entre distintos funcionarios o contratistas para reducir el riesgo de un mal uso de los sistemas e informaciones deliberado o por negligencia.
- **Seguridad de la información**: Según [ISO/lEC 27002:20005]: Preservación de la confidencialidad, integridad y disponibilidad de la información; además, otras propiedades como autenticidad, responsabilidad, no repudio, trazabilidad y fiabilidad pueden ser también consideradas.
- **Selección de controles**: Proceso de elección de los controles que aseguren la reducción de los riesgos a un nivel aceptable.

- **SGSI o SI Sistema de Gestión de la Seguridad de la Información**: Según [ISO/lEC 27001: 20005]: la parte de un sistema global de gestión que, basado en el análisis de riesgos, establece, implementa, opera, monitoriza, revisa, mantiene y mejora la seguridad de la información. (Nota: el sistema de gestión incluye una estructura de organización, políticas, planificación de actividades, responsabilidades, procedimientos, procesos y recursos.)
- **Tratamiento de riesgos:** Según [ISO/IEC Guía 73:2002]: Proceso de selección e implementación de medidas para modificar el riesgo.
- **Trazabilidad:** Propiedad que garantiza que las acciones de una entidad se puede rastrear únicamente hasta dicha entidad.
- **Usuario:** en el presente documento se emplea para referirse a directivos, funcionarios, contratistas, terceros y otros colaboradores de UNAL, debidamente autorizados para usar equipos, sistemas o aplicativos informáticos disponibles en la red de UNAL y a quienes se les otorga un nombre de usuario y una clave de acceso.
- **Valoración de riesgos:** Según [ISO/lEC Guía 73:2002]: Proceso completo de análisis y evaluación de riesgos.
- **Vulnerabilidad**: Debilidad en la seguridad de la información de una organización que potencialmente permite que una amenaza afecte a un activo. Según [ISO/lEC 13335-1:2004]: debilidad de un activo o conjunto de activos que puede ser explotado por una amenaza.