POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Bogotá,2020

ASAMBLEA GENERAL

Fr. Albeiro Arenas Molina

Presidente de la Asamblea General

Fr. Jorge Chaparro Caro

Secretario de la Asamblea General

CONSEJO SUPERIOR

Miembros Principales

Fr. Juan José Gómez Gómez. OAR

Fr. Antonio Abecia Valencia. OAR

Fr. Juan Camilo Torres Chisaba. OAR

Fr. Diego Montoya Naranjo. OAR

Fr. Jorge Chaparro Caro. OAR

Alfonso Mantilla Parra

Representante de los Docentes

Fabio Quimbaya Piña

Representante de los Docentes (suplente)

Luisa Bejarano Tumay

Representante de los Estudiantes

Alfonso Beltrán Orjuela

Representante de los Estudiantes (suplente)

Viviana Rojas Rodríguez

Representante de los Egresados

Oscar José Fernández Laches

Representante de los Egresados (suplente)

DIRECTIVAS INSTITUCIONALES

Fr. Enrique Arenas Molina

Rector

Ricardo Rojas López

Vicerrector Académico (E)

Julio César León Luquez

Vicerrector de Investigaciones

Alejandra Díaz Manzano

Vicerrectora de Extensión y Desarrollo Humano

Ángela Ovalle Posada

Vicerrectora Administrativa y Financiera

Araminta Clavijo Clavijo

Directora Oficina de Planeación y Gestión de la Calidad

Andrés Riveros Casas

Gerente de Transformación Digital

Ricardo Rojas López

Secretario General y

Asesor Jurídico

DECANOS

Carolina Berrío Hoyos

Decana Facultad de Ciencias Económicas y Administrativas

Directora Especialización Gerencia de Empresas

Directora Especialización Planeación Tributaria

Directora Especialización Gerencia Estratégica de Marketing

Directora Especialización Gestión Ambiental

Yenny Alexandra Martínez Ramos

Decana Facultad de Ingeniería

Directora Especialización Gerencia de la Calidad

Directora Especialización Seguridad Social Integral

Edward Lozano Martínez

Decano Facultad de Artes, Comunicación y Cultura

Fernando Sánchez Gélvez

Decano Facultad de Humanidades, Ciencias Sociales y Educación

Director Especialización en Pedagogía

Leonardo Santana Cortés

Decano Facultad de Educación Virtual y a Distancia

Director Especialización Gerencia del Talento Humano. Virtual

DIRECTORES ACADÉMICOS

Jaime Edgardo Valderrama Ochoa

Director Negocios Internacionales

Edgar Reyes Claro

Director Administración de Empresas

Omar Augusto Puerto Abella

Director Contaduría Pública

Gloria Duque Ayala

Directora de Hotelería y Turismo

Jairo Neira Guevara

Director de Mercadeo

Fabián Guillermo Oliveros Murillo

Director Cine y Televisión

Director Comunicación Social

Edward Lozano Martínez

Director Arquitectura

Jorge Wilson Motato Ramírez

Director Tecnología en Gastronomía

Ricardo Efrén Meza

Director Ingeniería Industrial

Director Ingeniería Mecatrónica

Nydia Stella García Roa

Directora Ingeniería en Telecomunicaciones

Directora Tecnología Desarrollo de Software

David Gerardo López Galvis

Director Teología

Director Licenciatura en Teología

Director Licenciatura en Filosofía

Carlos Alberto Castro Rendón

Director Administración Empresas. Virtual

Director Negocios Internacionales. Virtual

María José Arango de Manrique

Directora Ciencias Básicas

Ovidio Arlando Díaz González

Director Humanidades y Cátedra Agustiniana

Cristian Camilo Figueroa Ayala

Director Desarrollo Profesoral

Ernesto Iván Alfonso Acuña Ruiz

Director Permanencia Estudiantil

Adriana Yamile León

Directora Biblioteca

Carlos Alberto Castro Rendón

Director Calidad Académica y pedagógica. Virtual

Diego Fernando Cabrera Feo

Director Producción Medios Educativos Digitales. Virtual

Luis Alberto Penagos López

Director Centro Lenguas Extranjeras

Leonardo Santana Cortés

Director Centro Tecnología Agustiniana

DIRECTORES ADMINISTRATIVOS

Fr. Diego Montoya Naranjo. OAR

Director de Espiritualidad

Nathaly González Villegas

Directora Relaciones Internacionales e Interinstitucionales

Sandra Ujueta Rodríguez

Directora Aseguramiento de la Calidad

Diana Marcela Barón Vera

Directora Procesos de Calidad

Leydith Deyneth González Perilla

Directora Programación de Recursos

Cristián Camilo Botía Bociga

Director de Estadística

Héctor Mauricio Rincón Moreno

Director de Investigaciones

David Alejandro Guerrero Pirateque

Director de Emprendimiento

Edilberto Luis Lara Pupo

Director Proyección Social

Natalia Osorio Palacio

Directora de Bienestar Institucional

Lady Marian Cubides Cristancho

Directora Educación Continua

Pier Eduardo Gossen Echeverry

Director de Tecnología

María del Pilar Gómez Sánchez

Directora Comunicación e Imagen Corporativa

David Moncada Troncoso

Director de Marketing

Diana Rocío Granados Espinosa
Directora Capital Humano

María Clemencia Parra Gómez
Directora de Tesorería

Stella Ramos Páez
Directora de Contabilidad

Arnol Danilo Peña Valderrama
Director de Compras

Pedro Luis Vargas Cárdenas
Director de Seguridad y Logística

TABLA DE CONTENIDO

ÍNDICE DE FIGURAS

1. PRESENTACIÓN

La **UNIAGUSTINIANA** en el marco del desarrollo de las Políticas consagradas en los Estatutos, el Proyecto Educativo Institucional y el Plan de Desarrollo Institucional vigente, presenta el desarrollo de la Política de seguridad informática, bajo la cual se busca garantizar los procedimientos y aspectos a seguir referentes a la seguridad informática.

2. MARCO LEGAL

2.1. De la ley en general

- **Constitución política de Colombia (1991)**: En sus artículos 15, 20, 23 y 74.
- **Ley 599 de 2000**: Código Penal. Capitulo VII, artículos 192, 193, 196 y 197.
- **Ley 1341 de 2009**: Define principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones.
- **Ley 1273 de 2009**: La cual modifica el Código Penal, crea un nuevo bien tutelado denominado "de la protección de la información y los datos" y preserva integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.
- **Ley 1450 de 2011**: Plan nacional de desarrollo, artículos 28, 29 y 30
- **Decreto 2693 de 2012**: Lineamientos generales de la Estrategia de Gobierno en línea de la República de Colombia. En este se reglamentan parcialmente las Leyes 1341 de 2009 y 1450 de 2011, y se dictan otras disposiciones.

  Ley Estatutaria 1581 de 2012: Por la cual se dictan disposiciones generales para la protección de datos personales. Reglamentada Parcialmente por el Decreto Nacional 1377 de 2013.

2.2. De los Derechos de Autor

- **Decisión 351 de la Comunidad Andina de Naciones**: Régimen común sobre derecho de autor y derechos conexos.
- **Ley 23 de 1982**: Ley sobre derechos de Autor que protege la imagen individual frente a varias formas de abuso.
- **Decreto 1360 de 1989**: Reglamenta la inscripción del soporte lógico (software) en el Registro Nacional del Derecho de Autor.
- **Ley 44 de 1993**: Modificación a la ley 23 de 1982 y ley 29 de 1944.
- **Decreto 460 de 1995**: Reglamenta el Registro Nacional del Derecho de Autor y regula el Depósito Legal.
- **Ley 565 de 2000**: La cual aprueba el "Tratado de la OMPI -Organización Mundial de la Propiedad Intelectual - sobre Derechos de Autor de 1996.
- **Ley 603 de 2000**: Modifica el artículo 47 de la ley 222 de 1995.

2.3. De la Propiedad Industrial

- **Decisión 486 de la Comunidad Andina de Naciones:** Régimen Común sobre propiedad industrial
- **Decreto 2591 de 2000**: Reglamenta parcialmente la Decisión 486 de la Comisión de la Comunidad Andina.

2.4. Del Comercio Electrónico y Firmas Digitales

- **Ley 527 de 1999**: La cual define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, establece las entidades de certificación y se dictan otras disposiciones.
- **Decreto 1747 de 2000**: El cual reglamenta parcialmente la Ley 527 de 1999, en lo relacionado con las entidades de certificación, los certificados y las firmas digitales
- **Resolución 26930 de 2000**: El cual fija los estándares para la autorización y funcionamiento de las entidades de certificación y sus auditores

2.5. De las normas internacionales

- **ISO/IEC 27001:2013**: Es la evolución certificable del código de buenas prácticas ISO 17799. Define cómo organizar la seguridad de la información en cualquier tipo de organización, con o sin fines de lucro, privada o pública, pequeña o grande. Es posible afirmar que esta norma constituye la base para la gestión de la seguridad de la información

3. FUNDAMENTACIÓN Y COMPROMISO INSTITUCIONAL

La UNIAGUSTINIANA se compromete a desarrollar la Política de seguridad de la información, haciendo cumplir los procesos de integridad, confidencialidad y disponibilidad de la información, garantizando el cumplimiento de la filosofía, los principios institucionales y los valores que nos identifican: interioridad, verdad, libertad, amistad, comunidad y justicia solidaria.

4. INTRODUCCIÓN

La política de seguridad de la información establece responsabilidades e identifica controles y responsabilidades no asignadas, así mismo instaura directrices y procedimientos para una protección integral de los servicios basados en los activos de la información.

En la actualidad la información de la UNIAGUTINIANA se ha gestionado y tratado como información crítica y confidencial, información que está fragmentada por diferentes áreas que componen un núcleo de información confidencial y disponible.

En la institución, los servicios de red y sistemas de información enfrentan amenazas de seguridad que incluyen, pero no se limitan, a: el fraude por medios computacionales como phishing, ataques directos por herramientas y programas de malware, espionaje, sabotaje, vandalismo, robo, fuego, inundación, indisponibilidad y alteración. Las posibilidades de daño, vulnerabilidad, pérdida y/o alteración de la información por diferentes causas (código malicioso, uso indebido por parte del usuario, por ataques de denegación de servicio, etc) son cada vez más reales.

La gestión de seguridad de la información para la UNIAGUSTINIANA, estará fundamentada en el nuevo estándar ISO/IEC 27001:2013, el cual es una mejora significativa desde su versión 2005. El siguiente gráfico muestra los dominios que abarca la nueva versión.

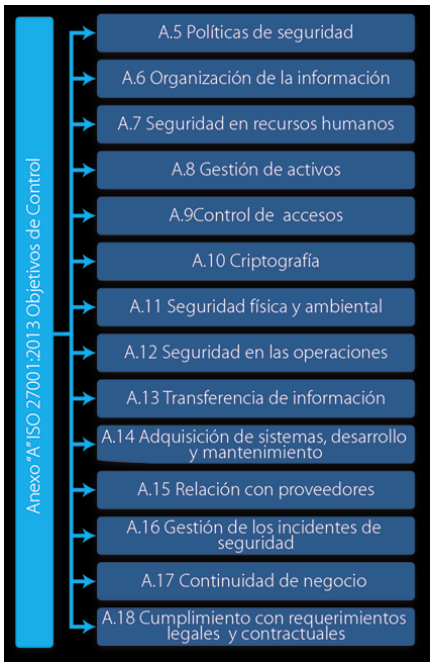

Figura 1. Dominios de la nueva ISO 27001:2013

Con la presente Política de Seguridad de la Información la UNIAGUSTINIANA establece en firme su compromiso institucional con un proceso de manejo de información responsable y seguro, teniendo como foco el cumplimiento de sus planes estratégicos institucionales.

5. CONCEPTOS Y DEFINICIONES

- **Seguridad de la información:** es un grupo de diversas medidas correctivas y preventivas de la institución y todos los sistemas tecnológicos que la componen, que permiten resguardar y proteger la información, buscando la confidencialidad, integridad y disponibilidad de los datos.

  El concepto de seguridad de la información es diferente al de seguridad informática, ya que este último se encarga de la seguridad en el medio informático de los equipos de cómputo y herramientas que participan en la infraestructura, pero la información puede encontrarse en varias formas y no solo en los medios informáticos.

  La seguridad de la información se fundamenta en tres pilares:

- **Confidencialidad**: Es el proceso mediante el cual se establece un mecanismo de control que impide que se realice la divulgación de la información de carácter netamente institucional con agentes externos o entidades que no estén autorizadas a conocer de dicha información.
- **Integridad**: Es el proceso que busca mantener los datos e información, libre de modificaciones no autorizadas o controladas. En términos generales, la integridad es mantener con exactitud la información tal cual fue generada, sin ser manipulada ni alterada por personas o procesos no autorizados.
- **Disponibilidad**: La disponibilidad es un principio y cualidad que busca garantizar que la información será accesible a las personas autorizadas cuando se le requiera.

Glosario de términos técnicos

- **Autenticidad o Autenticación**: Es la propiedad mediante la cual se puede establecer ciertamente el generador de la información.
- **Auditoría**: Es el proceso de conservar las evidencias y soportes de cada actividad que durante su desarrollo pueda afectar a los activos de información.
- **Protección a la duplicación**: Los activos de dicha información son procesos y registros que llevan copias ya generadas de aquellos artefactos que son catalogados como confidenciales.
- **No repudio**: Es la irrenunciabilidad, permite probar y verificar la participación de diferentes actores en un proceso de comunicación.
- **Legalidad**: Se refiere al cumplimiento de las normas legales aplicable a los activos de información.

- **Confiabilidad de la Información**: Se da por confiable un activo de información cuando es posible evidenciar en él el cumplimiento de los principios de integridad, confidencialidad, disponibilidad y autenticidad.
- **Activo de información**: Información representada en registros de tipo físico o digital que tienen valor para la Institución.
- **Amenaza**: Evento que compromete los principios de confidencialidad, integridad o disponibilidad de los activos de información.
- **Análisis de riesgo**: Proceso diagnóstico para identificar y analizar las posibles amenazas a las que se enfrenta un proceso, sistema o activo de información.
- **Continuidad**: Conjunto de actividades que permiten garantizar el proceso de negocio.
- **Control**: Medida que garantiza los 3 pilares de seguridad de la información.
- **Custodio de la información**: Cargo, persona o grupo de trabajo encargado de mantener las medidas de protección establecidas sobre los activos de información confiados.
- **Evaluación del riesgo**: Proceso mediante el cual se realiza la determinación del valor estratégico de los activos de información, se identifican las posibles amenazas aplicables y se evidencian las vulnerabilidades existentes o posibles, permitiendo generar los procesos de priorización y mitigación.
- **Gestión de activos**: Conjunto de actividades que clasifican la información de los activos, gestionando el riesgo y seguimiento que implican estos con su control, garantizando la confidencialidad, integridad y disponibilidad de la información.
- **Gestión de incidentes de seguridad**: Detectar y controlar recursos con los que se manejan los procesos y controles de incidentes asegurando la integridad y disponibilidad de la compañía.
- **Gestión de vulnerabilidades**: Conjunto de controles que consiste en detectar y controlar el riesgo producido por vulnerabilidades mediante estrictos controles.
- **Riesgo**: Es un conjunto de efectos que pueden surgir en el proceso de cualquier actividad con un evento no deseado para nuestra Institución, en donde podemos tomar acciones mitigando o minimizando el riesgo o simplemente el riesgo fue materializado y debemos realizar un plan de acción para futuros riesgos.
- **SGSI**: Sistema de Gestión de Seguridad de la Información
- **Sistema de información**: Mecanismo de software adquirido o desarrollado por UNIAGUSTINIANA en donde se requiere un proceso y control de activos de información para efectuar su función o actividad.
- **Vulnerabilidad**: Debilidades que se efectúan frente a una amenaza y que generalmente responde a una ausencia o déficit de controles que permiten que una amenaza se materialice.

6. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

La política de seguridad de información de la UNIAGUSTINIANA busca proveer las herramientas (procesos, políticas, personal y tecnología) necesarias para brindar apoyo y orientación a la alta dirección con respecto a la seguridad de los activos de información, alineadas con los requisitos del negocio, los reglamentos institucionales y las leyes aplicables.

La alta dirección debe establecer una dirección clara de la política según los objetivos del negocio, demostrar apoyo y compromiso con la seguridad de la información a través de la emisión y el mantenimiento de la presente política en toda la institución y garantizar su conocimiento y cumplimiento a través de los medios adecuados.

6.1. Alcance

La presente política de seguridad de la información busca dar cumplimiento a la normatividad legal vigente, con el objetivo de administrar y gestionar de forma adecuada la seguridad de la información, los sistemas informáticos y la infraestructura tecnológica de la UNIAGUSTINIANA.

Su aplicación es de obligatorio cumplimiento para cada persona, área, dependencia, tanto para personal interno como externo, sin ninguna diferencia en su vinculación contractual.

6.2. Objetivos

- Proteger, preservar, administrar todo el volumen de información generada al interior de la institución, así como toda aquella relativa a los terceros y que es recopilada a través de los diferentes procesos institucionales.

- Garantizar la presentación oportuna de la información a los diferentes actores que la requieran, teniendo en cuenta los principios enumerados en la norma ISO 27001

Establecer todos aquellos lineamientos que permitan a la institución medir de forma precisa el riesgo asociado a cada activo de información.

7. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

Con el objetivo de planear, diseñar, revisar y estructurar el proceso de gestión de la seguridad de la información y garantizar su efectiva comunicación y cumplimiento, se ha de constituir un grupo de trabajo que realice las tareas pertinentes. Dicho grupo, que se denominará **Grupo Técnico De Seguridad De La Información**, estará conformado por las siguientes personas de la institución:

- Gerente de transformación digital
- Director(a) de Tecnologías
- Director(a) de Comunicaciones
- Director(a) de Capital humano
- Director(a) de Procesos de Calidad
- Coordinador de Infraestructura
- Coordinador de Seguridad informática
- Coordinador de Gestión documental

Este grupo tendrá, entre sus funciones relativas a la gestión del SGSI, las siguientes:

- Revisar y aprobar la presente Política, así como aquellas responsabilidades generales relacionadas con el proceso de seguridad de la información.
- Monitorear cambios significativos en la exposición de activos de información frente a las amenazas más importantes.
- Revisar y monitorear cada uno de los incidentes relativos a la seguridad de la información.
- Revisar y aprobar todas las iniciativas generadas que propendan una mejora en la seguridad de la información.
- Acordar las funciones y responsabilidades de cada uno de los usuarios de la institución, de cara al cumplimiento de la presente política
- Establecer todas las metodologías y procesos específicos que se relacionen de manera directa al proceso de seguridad de la información.
- Establecer los canales, medios y recursos requeridos para la correcta difusión de la presente política, así como garantizar su cumplimiento.
- Garantizar que la seguridad haga parte de cada proceso individual relacionado con gestión de la información institucional.

- Evaluar la pertinencia y coordinar la implementación de controles específicos de seguridad de la información para nuevos sistemas o servicios.
- Promover la difusión y apoyo a la seguridad de la información dentro de la UNIAGUSTINIANA.

Adicional a las personas que conforman el **Grupo Técnico de Seguridad de la Información**, es responsabilidad de cada una de las coordinaciones, direcciones y vicerrectorías, la correcta identificación de sus activos de información, así como los riesgos asociados a los mismos y, por lo tanto, son parte activa de los responsables de seguridad de la información.

8. SEGURIDAD DEL RECURSO HUMANO

Cada individuo dentro de la institución hace parte integral del sistema de seguridad de la información, por lo tanto, se hace de vital importancia el actuar articuladamente entre cada uno de los actores que forman parte de la misma, así como extender este compromiso a todo el personal ajeno a la institución pero que requiere el acceso a la información institucional.

Dentro de la perspectiva de responsabilidades, se han establecido diversos grupos de riesgo, los cuales, por su nivel de acceso e información solicitada, requieren diferentes manejos:

8.1. Personal directamente vinculado a la UNIAGUSTINIANA

Todo el personal con relación contractual con la UNIAGUSTINIANA, debe firmar el documento que establece los lineamientos de uso de TI, conocer las políticas que en materia de seguridad de la información se estipulan en este documento y aceptar las condiciones de ambos.

El Estatuto Orgánico General y el Estatuto Docente Profesoral deben contemplar procesos y sanciones disciplinarias y/o penales para todas aquellas situaciones en las cuales se presente un uso indebido de los recursos de TI, se violen las políticas de acceso a la información, se ponga en riesgo la imagen o credibilidad institucional o se causen daños punibles a terceros.

La dirección de capital humano junto con la coordinación de seguridad informática, se encargarán de estructurar, diseñar, difundir, actualizar, mantener, ejecutar y evaluar un plan de capacitación en seguridad de la información que propenda por el crecimiento continuo de la conciencia individual y colectiva en temas de seguridad de la información.

La coordinación de sistemas de información, en conjunto con las coordinaciones de infraestructura tecnológica y seguridad informática, tendrá a su cargo la creación y el mantenimiento de un repositorio documental con acceso a toda la comunidad, en la cual se podrán consultar todos los aspectos relacionados con la seguridad de la información.

8.1.1 Dirección de tecnologías

El **Grupo Técnico de Seguridad de la Información**, tendrá la responsabilidad del planteamiento estratégico de la política, sus revisiones y modificaciones, la socialización de la misma y el velar por su correcta aplicación y cumplimiento. El Coordinador de Seguridad Informática tendrá a su cargo la responsabilidad directa de la implementación y ejecución de la presente política.

Todas las coordinaciones del área de tecnologías deberán ajustarse a los lineamientos de la presente política en todos los aspectos de su labor, y será de obligatorio cumplimiento y ejecución por cada uno de los colaboradores del equipo de trabajo. Cada uno de los coordinadores deberá determinar de cuales recursos tecnológicos y sistemas de información son responsables de custodia.

8.1.2 Capital humano

La dirección de capital humano tendrá la responsabilidad de socializar estas políticas con todos aquellos que se vinculen contractualmente con la institución, independientemente de las condiciones de su contrato. De igual forma, deberá comunicar a todo el personal, de cualquier cambio o modificación que se realice a esta política y que tenga implicaciones en la relación contractual con la institución.

8.1.3 Comunicaciones

La dirección de comunicaciones, como miembro del **Grupo Técnico de Seguridad de la Información**, tendrá la responsabilidad de articular las estrategias de difusión de la presente política. Su trabajo será articulado con las direcciones de capital humano, tecnologías y calidad, de acuerdo con la política de comunicaciones de la UNIAGUSTINIANA

8.1.4 Direcciones, Coordinaciones y Vicerrectorías

Todos aquellos que se hayan designado como responsables de activos de información por la institución, tendrán la responsabilidad de la clasificación,

mantenimiento y actualización de dicha información. De igual forma, serán responsables de la definición del personal a su cargo que tendrá acceso a la información en sus respectivos niveles.

8.2. Estudiantes

Para acceder a los diversos recursos informáticos de la Institución, los estudiantes deben leer y aceptar, en cada proceso semestral de matrícula, el acuerdo con los términos y condiciones del uso de dichos recursos. La Dirección de Tecnologías asegurará los mecanismos para la difusión y aceptación de dichas condiciones por medio de registros o confirmaciones virtuales y aceptación de términos de tratamiento de la respectiva información.

El reglamento estudiantil contemplará los procesos y sanciones disciplinarias a que haya lugar, para los casos en que se presente el uso indebido de los sistemas de información y/o en los que violen los términos y condiciones.

8.3. Usuarios Externos

Todos los usuarios y personal de empresas, deben contar con la respectiva autorización por parte de un funcionario de la institución con la autoridad para otorgar dicho acceso, quien tendrá la responsabilidad del control y vigilancia del uso adecuado de la información y los recursos informáticos institucionales. Los procedimientos para el registro de tales usuarios deben ser creados y mantenidos por las direcciones de Tecnologías y de Capital Humano.

Los usuarios externos deben aceptar por escrito los términos y condiciones de uso de la información y recursos de TI institucionales. Las cuentas de usuarios externos deben ser de perfiles específicos y tener caducidad no superior a tres (3) meses, renovables de acuerdo a la naturaleza del usuario.

8.4. Usuarios invitados y servicios de acceso público

El acceso de usuarios no registrados solo debe ser permitido al sitio web de información institucional. El acceso y uso a cualquier otro tipo de recurso de información y TI no es permitido a usuarios invitados o no registrados.

Recae en el **Grupo Técnico de Seguridad de la Información** el diseño y desarrollo de los perfiles de acceso a la información, fundamentados en criterios establecidos de forma institucional y asociados a cada cargo a través

de la dirección de capital humano. Este grupo determinara que atributos particulares se correlacionan con cada perfil.

Para todo el personal que termina su vinculación contractual con la UNIAGUSTINIANA, se establece un proceso en el cual se cambia la propiedad o custodia de los activos en poder de dicho usuario, y será su jefe inmediato el responsable de dicha información. La entrega por parte del empleado deberá ser parte fundamental de la terminación contractual.

En el mismo sentido, todo cambio de cargo y/o responsabilidad deberá involucrar la entrega absoluta de toda la información al jefe inmediato o responsable de dicho activo, quien tomará la responsabilidad por dicha entrega.

9. GESTIÓN DE ACTIVOS DE INFORMACIÓN

Es responsabilidad de la UNIAGUSTINIANA el establecimiento de las prácticas y los procedimientos que sean requeridos para la correcta administración y gestión de los activos de información.

El **Grupo Técnico de Seguridad de la Información**, tendrá bajo su responsabilidad, estructurar, organizar, revisar y supervisar, la generación de los inventarios de activos de información de cada una de las áreas de la institución. Cada una de estas áreas será responsable del mantenimiento y la actualización de dicho inventario. La gestión de los activos de información y sus riesgos de seguridad asociados son de aplicación a cada uno de los procesos de la institución.

Sera responsabilidad de la dirección de tecnologías, poner a disposición de cada una de las distintas áreas de la institución las herramientas tecnológicas que permitan la eficiente generación, organización y administración de dicho inventario.

10. CONTROL DE ACCESO

Para restringir el acceso no autorizado a los sistemas de información se implementan una serie de controles que están estrechamente vinculados con los procedimientos formales para realizar la asignación de derechos de acceso a los sistemas de información, bases de datos y servicios de información, los cuales deberán estar correctamente documentados, comunicados y controlados en cuanto a su cumplimiento.

El acceso a los recursos de tecnologías de información institucionales debe estar restringido y solo se permitirá acceso a los mismos según los perfiles de usuario definidos por el **Grupo Técnico de Seguridad de la Información**.

Los procedimientos comprenden todas las etapas del ciclo de vida de los accesos de los usuarios de todos los niveles, desde el registro inicial de nuevos usuarios hasta la privación final de derechos de los usuarios que ya no requieren el acceso.

La cooperación de los usuarios es esencial para la eficacia de la seguridad, por lo tanto, es necesario concientizar a los mismos acerca de sus responsabilidades por el mantenimiento de controles de acceso eficaces, en particular aquellos relacionados con el uso de contraseñas y la seguridad del equipamiento.

10.1. Perfiles de Acceso

El **Grupo Técnico de Seguridad de la Información** será el único responsable de establecer los perfiles sobre los cuales se otorgará el acceso a los usuarios.

10.2. Registro y anulación de registros de usuarios

Se deberán establecer procedimientos formales para controlar la asignación de los derechos de acceso a los sistemas y servicios de información.

Los procedimientos deberán comprender todas las fases del ciclo de vida del acceso del usuario, desde el proceso de su creación hasta la cancelación final del registro de aquellos que ya no requieren del acceso a los servicios y sistemas de información. Se debe tener especial cuidado con aquellos accesos que le permiten al usuario tener privilegios de administración y control sobre el funcionamiento del sistema. La Institución debe inclinarse por una metodología de autenticación única, garantizando que cada usuario tenga el mínimo de credenciales requeridas para el acceso a los sistemas.

El acceso a toda información restringida será estrictamente controlado. La UNIAGUSTINIANA implementará todas las automatizaciones dentro de sus sistemas de autenticación donde se manejen credenciales o firmas digitales.

Corresponde a la coordinación de sistemas de información, en articulación con las coordinaciones de infraestructura tecnológica y Seguridad Informatica, elaborar, mantener y publicar los documentos de servicios de red que ofrece la institución a su personal, estudiantes, docentes y terceros, así como los de administración de cuentas de usuarios para el uso de servicios de red.

El acceso a sistemas de cómputo y los datos que contienen es responsabilidad exclusiva del personal encargado de tales sistemas.

El control de las contraseñas de red y uso de equipos es responsabilidad de coordinación de Infraestructura Tecnológica. Dichas contraseñas deben ser codificadas y almacenadas de forma segura.

Las claves de administrador de los sistemas deben ser conservadas por la dirección de Tecnologías y deben ser cambiadas en intervalos regulares de tiempo y en todo caso cuando el personal adscrito al cargo cambie.

La coordinación de infraestructura en articulación con coordinación de seguridad informática, deben elaborar, mantener y actualizar el procedimiento y las guías para la correcta definición, uso y complejidad de claves de usuario.

10.3. Acceso Remoto

El acceso remoto a servicios de red ofrecidos por la UNIAGUSTINIANA debe estar sujeto a medidas de control definidas por coordinación de infraestructura tecnológica, las cuales deben incluir acuerdos escritos de seguridad de la información.

10.4. Auditoria y Seguimiento

Todo acceso y uso a los sistemas de información de la UNIAGUSTINIANA debe estar alineado con la reglamentación interna que se aprueba para cada uno de los actores de la institución y podrá ser auditado por la dirección de tecnologías.

11. CRIPTOGRAFÍA

La UNIAGUSTINIANA a través del área de tecnologías establecerá la óptima implementación de los sistemas y técnicas criptográficas para la protección de la información, herramientas que serán brindadas por el área de tecnologías y que se evaluara para verificar si dicha información necesita ser protegida o cifrada para que se conserve su confidencialidad e integridad de dicha información. (Herramientas de cifrado de disco duro o cifrado de dispositivos externos en donde se considere que dicha información contenida necesita protegerse)

El área de tecnologías debe brindar el apoyo necesario a administrativos, proveedores y docentes, en el uso de las herramientas tecnológicas para protección de la información sensible, también realizar programas de concientización para entrenar el activo más importante que son los empleados en la seguridad e integridad de la información.

El área de tecnologías, debe definir un procedimiento de gestión de claves, donde incluirán los métodos para la generación, longitud, eliminación y recuperación de claves en caso de pérdida, divulgación o daño.

12. SEGURIDAD FÍSICA

La UNIAGUSTINIANA cuenta con diferentes métodos para el control del acceso a las diferentes áreas de la institución, garantizando que solo el personal autorizado a tenga acceso a las mismas.

Toda persona que se encuentre dentro de la institución deberá poder ser identificado de manera fácil y oportuna por la comunidad y en especial por los miembros del personal de seguridad. Todo el personal con vinculación laboral deberá portar su carnet en un lugar visible, el cual deberá estar en un buen estado. La institución garantizara que todos sus empleados cuenten con el carnet de identificación vigente, de acuerdo al último diseño aprobado.

La UNIAGUSTINIANA deberá implementar los mecanismos necesarios para garantizar la seguridad de sus documentos de identificación, imposibilitando a posibles personas malintencionadas el acceso a los recursos de la institución.

12.1. Acceso físico

Todo visitante se debe registrar en la recepción de la institución para obtener la correcta autorización de ingreso. Durante su permanencia en las instalaciones deberá portar su carnet de visitante o sticker en lugar visible y el personal de seguridad deberá contar con mecanismos para identificación fácil y oportuna.

El centro de datos es un área restringida y sólo tendrán acceso a ella los colaboradores de la dirección de tecnologías definidos en la respectiva política de operación del centro de cómputo. Todo personal, ya sea administrativo, proveedores o técnicos, que requieran el ingreso a esta área, tendrán que diligenciar el formato de ingreso a DATACENTER y deberá contar con la aprobación y supervisión del director de tecnologías, coordinador de infraestructura o coordinador de seguridad informática.

12.2. Acceso lógico

Los usuarios de la Institución son los únicos responsables de velar por la seguridad que respecto a su cargo implique, así mismo el área de seguridad informática estará trabajando constantemente en controles y monitoreo de toda información que se clasifique como confidencial, que sea necesaria su integridad y que requiera disponibilidad.

El uso de contraseña tendrá que estar fundamentado por el uso de contraseñas con un nivel óptimo de seguridad, complementando signos, alfanuméricos, números y letras mayúsculas y minúsculas (Se recomienda tener una palabra clave para que esta contraseña sea más fácil de recodar, si llegase a olvidar el área de tecnologías podrá ayudarle a realizar el proceso de recuperación).

12.3. Seguridad en los equipos

Los servidores donde se procesen la información y los servicios institucionales deben ser mantenidos en un ambiente seguro y debidamente protegido por lo menos con:

- Controles de acceso y seguridad física.
- Detección y extinción de incendios
- Controles de humedad y temperatura.
- Alejados del flujo de agua.
- Sistema de respaldo de energía primario y secundario

Toda información de carácter institucional en formato digital debe ser almacenada de manera exclusiva en los servidores de la institución, los cuales han sido previamente certificados por la dirección de Tecnologías. Quedará expresamente prohibido el almacenamiento de información institucional en memorias USB personales, servicios en línea de almacenamiento o servidores fuera de la institución sin una aprobación directa por parte de la dirección de tecnologías.

La institución seguirá estrictos planes de mantenimiento y tendrá contratos de soporte con los proveedores, que garanticen la correcta operación de la infraestructura en todo momento. Las estaciones de trabajo deberán estar correctamente instaladas y el personal a cargo será capacitado acerca de su uso y del contenido de esta política.

13. SEGURIDAD EN OPERACIONES

La UNIAGUSTINIANA promoverá la aplicación de las mejores prácticas para asegurar que las operaciones en la institución se cumplen bajo parámetros seguros, considerando aspectos para la gestión de cambios, la protección contra malware, el respaldo de la información y la gestión de vulnerabilidades técnicas.

La Dirección de tecnologías y los dueños de los procesos son los responsables de la aplicación de los controles de Seguridad de la Información que soportan los aspectos mencionados.

13.1. Documentación

La dirección de tecnologías tendrá bajo su responsabilidad la correcta documentación de todos los procesos que involucren operaciones de TI, así como poner estos a disposición de los usuarios que los requieran.

13.2. Control de cambios

Todo cambio que se realice sobre la infraestructura tecnológica debe ser controlado, gestionado, sometido a una evaluación que permita identificar riesgos asociados que pueden afectar la operación del negocio y autorizado por los niveles correspondientes según la infraestructura afectada.

Los cambios que puedan afectar los controles de Seguridad de la Información en ambiente de producción pueden ser revisados por el Grupo Técnico de Seguridad de la Información, cuando esta instancia considere pertinente su análisis para evaluar impactos adversos en las operaciones del negocio.

Entre los aspectos que debe considerar el control de cambios están:

- La planeación y pruebas de los cambios
- El análisis del impacto por el cambio, incluyendo el impacto en la Seguridad de la Información
- Las actividades de rollback y las actividades de recuperación considerando imprevistos en los cambios.

En todos los casos se deben seguir el procedimiento de Gestión de cambios y configuración disponible en el sistema de información de gestión

13.3. Gestión de Capacidad

La dirección de tecnologías será responsable por el continuo monitoreo, análisis y evaluación de las capacidades de los recursos de TI y de tomar las medidas tendientes a garantizar el óptimo funcionamiento de las mismas.

En conformidad con la ley, la Institución podrá realizar seguimiento a las actividades de los sistemas tecnológicos a través de diferentes mecanismos, cuando se detecte actividad inusual en los mismos y con el objetivo de

garantizar la estabilidad de los propios sistemas afectados. No obstante, lo anterior, se requerirá de previa autorización de la Dirección de Tecnologías, y en todo caso notificando previamente a los afectados por esta decisión.

13.4. Protección contra Malware

La UNIAGUSTINIANA considera como prioridad la protección de equipos de cómputo y servidores con software de seguridad (antivirus, firewall, antispyware, anti-bootnet) y otras aplicaciones que brinden efectiva protección contra cualquier código malicioso o intrusión. Cualquiera que sea la herramienta usada, deberá contar con un mecanismo que permita su actualización de manera automática, así como la generación de informes y alertas en una consola unificada. Todos los sistemas deben ser protegidos teniendo en cuenta un enfoque que involucre tanto al factor humano como aspectos tecnológicos.

El **Grupo Técnico de Seguridad de la Información** será responsable de estructurar, diseñar, mantener y evaluar las políticas, normas, estándares, procedimientos y guías que garanticen la mitigación de riesgos asociados a amenazas de software malicioso, hacking o ransomware.

La UNIAGUSTINIANA, en cumplimiento con las leyes vigentes, no permitirá ningún proceso de extorsión por técnicas de encriptación de la información realizada por terceros.

La dirección de Tecnologías, previa autorización de la alta dirección, está facultada para intervenir el tráfico de red cuando se sospeche de actividad inusual. Dicha intervención será comunicada a la comunidad Agustiniana a través de los medios establecidos para ello.

13.5. Separación de ambientes

Con el objetivo de mantener la seguridad y estabilidad de todas las plataformas de software de la institución, los nuevos desarrollos y/o mejoras deberán realizarse en entornos separados a los productivos. La dirección de tecnologías tendrá la responsabilidad de estructurar, diseñar y mantener los diferentes entornos de desarrollo y pruebas que sean requeridos.

13.6. Respaldo de información

La información contenida en los distintos medios de almacenamiento es vulnerable distintas situaciones como robo, incendios, inundaciones, fallos

eléctricos, fallo del dispositivo, virus, hacking, borrado accidental, etc, las cuales, en caso de presentarse, imposibilitaría tener disponibilidad de la información, afectando la continuidad del negocio. Por esta razón, es imprescindible el uso de una estrategia de copia de seguridad (backup) que le permita a la institución garantizar el retorno a la operación habitual en el mínimo periodo de tiempo.

Para garantizar la correcta realización del respaldo de información, es necesario realizar un inventario detallado de los activos de información y su respectiva clasificación de acuerdo al impacto en el proceso de negocio.

La coordinación de seguridad informática, será responsable por la estructuración, diseño, implementación y verificación de los planes de respaldo y restauración, entre los cuales se debe contemplar:

- El Origen de la información a respaldar
- Tipo de respaldo
- La recurrencia del respaldo y su ubicación
- La vigencia de la copia
- El soporte de la realización del respaldo
- Las pruebas de restauración

El **Grupo Técnico de Seguridad de la Información** determinara las ubicaciones donde los usuarios deberán guardar todos los documentos y/o archivos que hacen parte de la información institucional. Es responsabilidad de cada uno el cumplimiento de estas directrices con el objetivo de salvaguardar dichos activos de información en los respectivos procesos de respaldo.

Las coordinaciones de seguridad informática y Sistemas de información deberán realizar de forma periódica los procesos de validación de las copias de seguridad, con el fin de garantizar que se podrán utilizar en el momento en que se requiera.

13.7. Gestión de las Configuraciones de Red

Estará prohibido para cualquier usuario, sin relevancia de su cargo y/o responsabilidades, la instalación de equipos de red, comunicaciones o computo sin la debida autorización por parte de la dirección de tecnologías. Cualquier dispositivo que sea encontrado haciendo parte de la red de manera irregular, será desconectado y reportado como incidente de seguridad con las consecuencias que se establezcan para esta conducta.

La coordinación de infraestructura tecnológica será responsable de mantener una copia de seguridad de la configuración de todos los elementos de la red (Switchs, firewalls, enrutadores, UTM, Gateway GSM IP, etc), así como la documentación relativa a cada uno de estos dispositivos.

13.8. Instalación de Software

Todo programa, software o pieza de código que sea de uso institucional deberá estar respaldado por la respectiva licencia de uso. Para el caso de aquellos aplicativos de uso libre, se debe contar con el documento que expresa los términos de uso de dicho software y las restricciones en caso de ser aplicables, adicional a la autorización para su uso. Sera responsabilidad de la dirección de tecnologías garantizar el cumplimiento de esta directiva.

La Dirección de Tecnologías, a través de la coordinación de sistemas de información, deberá implementar y mantener el inventario de software y sistemas de información autorizado y en uso en la institución, así como validar su uso en cada una de las estaciones de los usuarios y/o en los servidores.

Todas las instalaciones de software que se realicen sobre sistemas de la Institución deben ser aprobadas por la coordinación de infraestructura tecnológica o la coordinación de seguridad informática, de acuerdo a los procedimientos elaborados para tal fin por dichas dependencias. La dirección de Tecnologías podrá, a su criterio, definir el ámbito en el cual actuará cada dependencia.

No se permite la instalación de software que viole las leyes de propiedad intelectual y derechos de autor. El equipo de soporte técnico, en articulación con las coordinaciones de infraestructura y seguridad informática, están en la obligación de realizar la desinstalación de cualquier software ilegal y notificar este evento como un incidente de seguridad.

13.9. Internet y Correo Electrónico

Las normas que delimiten el uso de los servicios de Internet y correo electrónico serán estructuradas, mantenidas y actualizadas por el **Grupo Técnico de Seguridad de la Información.** Dicho grupo tendrá, además, la responsabilidad de garantizar el cumplimiento del código de ética institucional, así como del manejo responsable de los recursos informáticos de la institución.

14. TRANSFERENCIA DE INFORMACIÓN

Las solicitudes de información realizadas por los entes de control del estado o por cualquier entidad con la respectiva autorización, serán aprobadas por la Rectoría, y serán de carácter exclusivo al ente o entidad solicitante, quien será responsable de su custodia.

El área de seguridad informática está en total control y monitoreo de la transferencia de información confidencial y que su integridad no se vea afectada en procesos de comunicación no permitidos dentro de la institución, para ello se estará brindando buenas prácticas, capacitaciones y charlas para enviar información confidencial por medios electrónicos con procedimientos de cifrado y firmas criptográficas.

Los mensajes enviados a través de cualquier medio electrónico que contengan información privada, controlada o reservada, deben ir correctamente enviados para que sólo sean conocidos por el emisor y por el receptor(es), del mensaje, es obligatorio enviar este archivo con una llave criptográfica para que si su proceso de envió llegase a ser inequívoco o erróneo solo pueda ser visualizado por el receptor que contiene la llave de desencriptado.

Los correos electrónicos solo deben ser para uso institucional, por lo tanto, no será permitido su registro para cualquier actividad distinta a las establecidas en su cargo.

15. GESTIÓN DE VULNERABILIDADES E INCIDENTES DE SEGURIDAD

La coordinación de seguridad informática tendrá como responsabilidad la identificación de las posibles vulnerabilidades técnicas de los sistemas informáticos, a través de la elaboración de planes de análisis de vulnerabilidades, suscripción a entidades y/o organizaciones de identificación de riesgos informáticos, boletines de seguridad y asociaciones de información compartida.

Esta matriz que permite identificar el impacto de los incidentes de seguridad:

Impacto del Incidente			
MENOR (1)	***MODERADO (2)***	***MAYOR (3)***	***CATASTROFICO(4)***
Aquellos recursos o activos de información que al ser afectados, no poseen ningún grado de afectación en la operación de las funciones básicas de la entidad o los colaboradores de la misma.	Aquellos recursos o activos de información que al ser afectados, interfieren en las operaciones básicas de la entidad y de los colaboradores, pero que no detienen la operación de los mismos.	Aquellos recursos o activos de información que al ser afectados interfieren en las operaciones de soporte de la entidad o los colaboradores, como la Operación del correo electrónico. Servicios de Internet Servicios de telefonía IP. Sistema de control de acceso físico. Es importante tener presente que en esta categoría solo debe presentarse uno de los eventos anteriormente mencionados	Aquellos recursos o activos de información que al ser afectados interfieren en las operaciones misionales y de soporte de la entidad o de los colaboradores, que afectan de manera parcial o total la prestación de los servicios de la entidad.

Figura 2. Matriz de impacto de incidentes

Es responsabilidad de todos los usuarios de los sistemas informáticos el informar de cualquier actividad sospechosa o violación de seguridad a su jefe inmediato o a través de los canales que establezca el **Grupo Técnico de Seguridad de la Información**.

La Dirección de tecnologías, a través de la Coordinación de seguridad informática, es responsable de diseñar, implementar y evaluar los planes de acción que requieran ser aplicados tras la identificación de vulnerabilidades críticas en los sistemas.

El **Grupo Técnico de Seguridad de la Información** debe estructurar, mantener y socializar las normas, procesos y guías para el reporte e investigación de incidentes de seguridad.

Para todos aquellos sistemas considerados críticos para la operación institucional, se deberá contar con un procedimiento escrito, al cual se le debe realizar seguimiento de forma periódica para evaluar la confiabilidad del servicio.

16. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS

Con el fin de lograr sus objetivos institucionales, la UNIAGUSTINIANA requiere de la constante adquisición de aplicativos y sistemas de software, tanto de uso comercial como hecho a medida. Todo proyecto de desarrollo o adquisición de software debe contar con un documento de Identificación y Valoración de Riesgos, el cual será la base para el conocimiento, administración y mitigación del riesgo asociado. Sin este documento, la Institución no podrá desarrollar ninguno de estos procesos de Software.

La coordinación de desarrollo debe aplicar los lineamientos de esta política y de todos aquellos documentos complementarios durante los procesos de adquisición o desarrollo de sistemas de software.

Los sistemas software adquiridos a través de terceras partes deben certificar el cumplimiento de estándares de calidad en el proceso de desarrollo.

Las solicitudes de nuevos desarrollos o la modificación de las aplicaciones instaladas y almacenadas actualmente en los servidores de la institución que se encuentran en producción, deberán ser analizadas previamente, verificado que cumplan con los estándares de desarrollo seguro, con integraciones seguras y validaciones estrictas. Estos desarrollos nuevos serán puestos en marcha previamente en servidores de pruebas para su validación y finalmente aprobación por Checklist.

Todo desarrollo será puesto en pruebas y se verificará si cumple con los requerimientos mencionados en el proceso de contratación. También se observará el proceso de recolección de datos si así lo dispone la funcionalidad y que si cumple con los procesos de protección de datos y captura de datos al momento de ingresar. Con el fin de garantizar la seguridad, estabilidad y usabilidad de las soluciones, todos los desarrollos nuevos o modificaciones a desarrollos existentes, se deben cumplir con estándares de publicación como certificados SSL, formularios con CAPTCHA y envíos de parámetros por POST.

Las áreas solicitantes de desarrollos nuevos o modificaciones a desarrollos ya existentes, deben asignar a funcionarios idóneos para colaborar en la realización y aprobación de los resultados de las pruebas.

Dentro del sistema de gestión de calidad se pueden encontrar otros documentos que soportan o amplían los alcances de esta política.

17. RELACIÓN CON PROVEEDORES

La UNIAGUSTINIANA, en su entendimiento de una relación sólida con sus partners, proveedores y contratistas, con quienes, por razones propias de la relación, debe compartir información, ha fijado una seria de controles para la seguridad de la misma. En esta relación, ambas partes se comprometen a resguardar la información obtenida de la contraparte y garantizar que su uso será exclusivamente para los fines determinados por la relación.

Los acuerdos de confidencialidad entre proveedores siempre tendrán que estar firmados y cumpliendo con las normas de integridad de información, así mismo en cualquier situación en donde el proveedor recolecte información privada o masiva de los usuarios de la UNIAGUSTINIANA (Recolección en eventos, talleres, congresos).

Las terceras partes involucradas se verán obligadas a firmar los formatos de confidencialidad aplicables. El área de seguridad informática se los brindara, según corresponda para Proveedores y/o Terceros, o administrativos, contratistas y docentes.

18. ADMINISTRACIÓN DE CONTINUIDAD DEL NEGOCIO

La UNIAGUSTINIANA tomara las decisiones estratégicas, económicas y logísticas a que haya lugar con el objetivo de garantizar la continuidad de la operación bajo cualquier circunstancia o factor, bien sean estos de carácter físico, lógico, humano o ambiental.

Como parte de continuar operando ante un evento adverso que interrumpa las operaciones, se establecen los requerimientos de continuidad para el proceso de Gestión de Seguridad de la Información de la institución, con el fin de mantener los niveles mínimos de seguridad para el negocio ante un evento de interrupción.

19. RECURSOS

Para la el cumplimiento de la política de seguridad de la información la UNIAGUSTINIANA destinará anualmente los recursos necesarios para su desarrollo a través de los proyectos y actividades que se presenten para este fin, además propenderá por la construcción de procesos y procedimiento requeridos para su mejora continua.

A continuación de describen los compromisos y recursos que la UNIAGUSTINIANA dispone a través de la alta dirección:

- La autorización para que la implementación del presente SGSI en la UNIAGUSTINIANA.
- El establecimiento y aprobación de esta política.
- Establecer los objetivos del SGSI
- Las revisiones periódicas del SGSI
- La asignación de roles y responsabilidades en seguridad de la información.
- La gestión de las comunicaciones requeridas para la socialización efectiva de la política, permitiendo que la comunidad se apropie de la importancia de lograr los objetivos aquí presentados en materia de seguridad.
- Proporcionar todos los recursos técnicos, económicos, tecnológicos, y humanos requeridos para una adecuada implementación del SGSI.
- Asegurar que todo el personal a quien se asignó las responsabilidades definidas en el SGSI sea competente para realizar las tareas requeridas

La responsabilidad final con respecto a la seguridad de la información de la implementación del SGSI recae sobre la Gerencia de transformación digital e innovación tecnológica, soportado por los responsables de cada área.

20. ARTICULACIÒN CON LA CALIDAD INTEGRAL UNIAGUSTINIANA

Las políticas institucionales deben estar articuladas con la Calidad Integral, concepto sobre el cual se soporta el Sistema Integrado de la Calidad Uniagustiniana (SICU).

Esta articulación de la política en cuestión tiene como primer ingrediente los resultados del seguimiento y evaluación de la misma. Dependiendo de las características de la Política podría escalar hasta la autoevaluación, los resultados de los distintos ejercicios de evaluación aplicado en la Institución y desde luego los derivados del enfoque por procesos.

Será responsabilidad del área de calidad la realización de auditorías de forma regular al sistema de seguridad de la información y las actividades asociadas con la gestión de activos de información.

Los procedimientos, reglamentos, manuales, instructivos o formatos vigentes se encuentran en el Sistema Integrado de Calidad Uniagustiniana (SICU).

21. CUMPLIMIENTO

La UNIAGUSTINIANA cumple con la reglamentación de propiedad intelectual, privacidad y protección de datos personales vigente en el país asegurando la protección de sus signos distintivos, validando que ante requerimientos de cambios en estos o el requerimiento de nuevos signos distintivos se estén respetando los derechos de propiedad intelectual de terceros, e implementando los controles de protección requeridos sobre datos personales.

La presente Política de Seguridad de la Información entra en vigencia una vez oficializada por la alta dirección de la institución. Los vicerrectores, directores y coordinadores de las distintas áreas serán responsables de ponerlas en conocimiento del personal a su cargo. Todos los colaboradores se acogen al cumplimiento de la ley y normas aplicables en materia de Seguridad de la Información, derechos de propiedad intelectual y privacidad y protección de datos personales.

Todo personal que sea contratado con posterioridad a la publicación y oficialización del presente documento deberá ser informado por los canales adecuados de la existencia de esta política, allegar una copia de la misma y firmar una declaración de toma de conocimiento y aceptación de la misma.

La presente política está gestionada a las leyes establecidas en una constitución política de la república de Colombia. Cualquier conflicto o inconveniente de estas debe ser informado al encargado de este documento inmediatamente.

22. BIBLIOGRAFIA

Camelo, L. (7 de Mayo de 2010). *Seguridad de la informacion en Colombia*. Obtenido de Seguridad de la informacion en Colombia: Dominio 5: http://seguridadinformacioncolombia.blogspot.com/search/label/Dominio 15

Isaza, Z. M. (2016). *ISO/IEC 27001:2013 – SISTEMAS DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN.* Obtenido de http://polux.unipiloto.edu.co:8080/00003427.pdf

ISO 27001 - Seguridad de la información: norma ISO IEC 27001/27002. (s.f.). Obtenido de Normas ISO: https://www.normas-iso.com/iso-27001/

ISO 27001 - Certificado ISO 27001 punto por punto. (s.f.). Obtenido de Normas ISO 27001: https://normaiso27001.es/

ISO 27001:2013 ¿Qué hay de nuevo? - Magazcitum. (s.f.). Obtenido de Magazcitum: https://www.magazcitum.com.mx/?p=2397

Norma 27001 2013 - PMI SGSI - ISO 27001. (s.f.). Obtenido de PMI - SGSI - ISO 27001 - Chile: https://www.pmg-ssi.com/norma-27001/

Seguridad de la información. (15 de Julio de 2020). Obtenido de Wikipedia, la enciclopedia libre: https://es.wikipedia.org/wiki/Seguridad_de_la_información