RESOLUCIÓN RECTORAL No. 539
06 de julio de 2021

"Por medio del cual se adopta la Política de Administración de Riesgos en la Institución Universitaria Digital de Antioquia – IU. Digital, en el marco de la consolidación del Modelo Integrado de Planeación Gestión"

EL RECTOR DE LA INSTITUCIÓN UNIVERSITARIA DIGITAL DE ANTIOQUIA – IU. DIGITAL

En uso de sus atribuciones constitucionales, legales, reglamentarias y estatutarias, principalmente las establecidas en los artículos 209, 269 y 343 de la Constitución Política de 1991 y las fijadas por la Ley 87 de noviembre 29 de 1993 y el Decreto 111 de 1996; actuando en virtud de lo establecido en el literal e) del artículo 29 del Acuerdo Directivo No. 067 de 2019, amparado en las demás normas concordantes vigentes adscritas a nuestro ordenamiento jurídico, y,

CONSIDERANDO:

1. Que en la Constitución Política de 1991 dispuso en su artículo 342 que la ley orgánica reglamentará todo lo relacionado con los procedimientos de elaboración, aprobación y ejecución de los planes de desarrollo y dispondrá los mecanismos apropiados para su armonización y para la sujeción a ellos de los presupuestos oficiales.

2. Que el artículo 209 de la Constitución Política establece que la administración pública, en todos sus órdenes, tendrá un control interno que se ejercerá en los términos que señale la ley y que la función administrativa se debe desarrollar con fundamento en los principios de igualdad, moralidad, eficacia, economía, celeridad, imparcialidad y publicidad.

3. Que el artículo 269 de la Constitución Política dispuso que: *"En las entidades públicas, las autoridades correspondientes están obligadas a diseñar y aplicar, según la naturaleza de sus funciones, métodos y procedimientos de control interno, de conformidad con lo que disponga la ley"*

4. Que la Ley 87 de 1993 desarrolla los artículos 209 y 269 de la Constitución Política de Colombia. En su artículo 2 se definen los objetivos del Sistema de Control Interno y dentro de éste, los literales a) y f) que establecen: "*a) Proteger los recursos de la organización, buscando su adecuada administración ante posibles riesgos que los afecten y f) Definir y aplicar medidas para prevenir los riesgos, detectar y corregirlas desviaciones que se presenten en la organización y que puedan afectar el logro de sus objetivos*".

5. Que el artículo 2.2.21.5.3 del Decreto 1083 de 2015, Por medio del cual se expide el Decreto Único Reglamentario del Sector de Función Pública, Modificado Decreto 648 de 2017, artículo 17), estableció que: "*las Unidades u Oficinas de Control Interno o quien haga sus veces desarrollarán su labor a través de los siguientes roles: liderazgo estratégico; enfoque hacia la prevención, evaluación de la gestión del riesgo, evaluación y seguimiento, relación con entes externos de control*".

6. Que el artículo 2.2.21.5.4, del Decreto 1083 de 2015, Por medio del cual se expide el Decreto Único Reglamentario del Sector de Función Pública, "*Como parte integral del fortalecimiento de los sistemas de control interno en las entidades públicas las autoridades correspondientes establecerán y aplicarán políticas de administración del riesgo. Para tal efecto, la identificación y análisis del riesgo debe ser un proceso permanente e interactivo entre la administración y las oficinas de control interno o quien haga sus veces, evaluando los aspecto tanto internos como externos que pueden llegar a representar amenaza para la consecución de los objetivos organizaciones, con miras a establecer acciones efectivas, representadas en actividades de control, acordadas entre los responsables de las áreas o procesos y las oficinas de control interno e integradas de manera inherente a los procedimientos*".

7. Que en el artículo 73 de la Ley 1474 de 2011, quedó estipulado el Plan Anticorrupción y de Atención al Ciudadano, el cual contempla que: "*Cada entidad del orden nacional, departamental y municipal deberá elaborar anualmente una estrategia de lucha contra la corrupción y de atención al ciudadano. Dicha estrategia contemplará, entre otras cosas, el mapa de riesgos de corrupción en la respectiva entidad, las medidas concretas para mitigar esos riesgos, las estrategias antitrámites y los mecanismos para mejorar la atención al ciudadano*".

8. Que la Política de Gobierno Digital indica que las entidades requieren el establecimiento de sistemas de seguridad de la información que les permitan manejar adecuadamente los riesgos identificados, lo cual implica realizar el análisis de riesgo correspondiente.

9. Que mediante resolución Rectoral 115 de 2019, se adopta el Modelo Integrado de Planeación y Gestión-MIPG, en la Institución Universitaria Digital de Antioquia, como marco de referencia para dirigir, planear, ejecutar, hacer seguimiento, evaluar y controlar la gestión de la entidad, con el fin de generar resultados para el cumplimiento de la misión Institucional.

10. Que se hace necesario adoptar la Política de Administración de Riesgos en la Institución Universitaria Digital de Antioquia.

11. Que en sesión ordinaria No. 02 del Comité Institucional de Coordinación del Sistema de Control Interno, llevada a cabo el 02 de junio de 2021, conforme lo establece la Resolución 326 de 2020 en el artículo 4, numeral 7, se estudió y sometió a aprobación la Política de Administración de Riesgos, la cual fue debidamente aprobada.

12. Que en diciembre de 2020 el Departamento Administrativo de la Función Pública-DAFP, expidió la Guía para la Administración de Riesgos y el Diseño de Controles en la Administración Pública y sobre esta Guía se actualizarán los mapas de riesgos de la IU. Digital.

En mérito de lo anteriormente expuesto,

RESUELVE:

ARTÍCULO 1. Adoptar la Política de Administración del Riesgo de la Institución Universitaria Digital de Antioquia como un instrumento que soporta en forma técnica y objetiva el compromiso de la Institución Universitaria frente al cumplimiento de los objetivos Institucionales, además de la generación del valor público en la sociedad, en la garantía del goce del derecho fundamental, en particular de la educación superior.

ARTÍCULO 2: La Política de Administración de Riesgos, tiene su centro en el Modelo Integrado de Planeación y Gestión MIPG V2, en la Norma Técnica Colombiana NTC-ISO 31000:2018, el Decreto 2641 del 2012, compilado en el Decreto 1081 de 2015, , Estatuto Anticorrupción, y la “Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas” V4, expedida por la Presidencia de la República, Ministerio de Tecnologías de la Información y las Comunicaciones, y el Departamento Administrativo de la Función Pública.

ARTÍCULO 3: Los Objetivos de la Política de Administración de Riesgos:

a. Orientar la toma de decisiones respecto al tratamiento de los riesgos y sus efectos al interior de la Institución Universitaria.
b. Establecer los parámetros necesarios para una adecuada administración de los riesgos a través de los elementos: contexto estratégico; identificación de riesgos; análisis de riesgos; valoración de riesgos; políticas de administración del riesgo, su trazabilidad, registro y monitoreo.
c. Orientar la toma de decisiones para la prevención del riesgo.
d. Incentivar el pensamiento basado en riesgos dentro de la entidad.
e. Buscar la mejora continua en cada uno de los procesos.

ARTÍCULO 4: El Alcance - La Administración del Riesgo en la Institución Universitaria Digital de Antioquia tendrá el siguiente alcance:

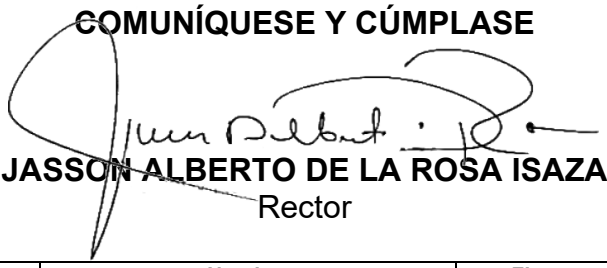
a. Los Riesgos de Gestión: los cuales cubren todos los procesos, los proyectos y los servicios que ofrece la Institución Universitaria y que representen una probabilidad de impacto sobre el cumplimiento de los objetivos institucionales.
b. Los Riesgos de Corrupción: contemplan cualquier posibilidad de que, por acción u omisión, se use el poder para desviar la gestión institucional hacia un beneficio privado.
c. Riesgos de Seguridad Digital: Al ser una institución de carácter digital, este tipo de riesgo puede debilitar el logro de los objetivos institucionales, por lo cual su alcance es extensible y aplicable a toda amenaza y vulnerabilidad en el entorno digital de los procesos que hacen parte de la Gestión de la Seguridad y Privacidad de la Información Institucional.

ARTÍCULO 5: De la presente Resolución Rectoral hace parte integra el documento técnico denominado: *"Política de Administración de Riesgos de la Institución Universitaria Digital de Antioquia",* el cual consta de 28 folios.

ARTÍCULO 6: La institución Universitaria Digital de Antioquia se compromete a gestionar en forma consciente, racional y planificada el Sistema de Administración de Riesgos a fin de garantizar el cumplimiento de los objetivos de cara a los grupos de valor.

ARTÍCULO 7. La presente Resolución Rectoral rige a partir de la fecha de su expedición y deroga las que le sean contrarias.

COMUNÍQUESE Y CÚMPLASE



JASSON ALBERTO DE LA ROSA ISAZA
Rector

Acción	Nombre	Firma	Fecha
Proyectó y elaboró	Guillermo Giraldo Díaz		29/06/2021
Revisó	Fabián Erley Escudero Salgado		29/06/2021
Revisó	Marleny García Ospina		29/06/2021
Revisó	Camilo alexander Hurtado Castaño		30/06/2021
Revisó	Gustavo Adolfo Londoño Cano		06/07/2021
Revisó y aprobó	Leonardo Fabio Marulanda Londoño		07/07/2021
Los arriba firmantes declaramos que hemos revisado el documento y lo encontramos ajustado a las normas y disposiciones legales y, por tanto, bajo nuestra responsabilidad lo presentamos para firma.			

POLÍTICA DE ADMINISTRACIÓN DE RIESGOS

IU Digital de Antioquia

INSTITUCIÓN UNIVERSITARIA DIGITAL DE ANTIOQUIA

Oficina Asesora de Planeación

2021

CONTENIDO

1. NATURALEZA JURÍDICA DE LA INSTITUCIÓN UNIVERSITARIA DIGITAL DE ANTIOQUIA

La Institución Universitaria Digital de Antioquia es una entidad descentralizada del orden departamental en la figura de Establecimiento Público de Educación Superior, creada mediante Ordenanza Nro. 074 de diciembre 27 de 2017, y cuenta con aprobación de factibilidad por parte del Ministerio de Educación Nacional mediante Resolución No. 28994 de 2017 y personería jurídica, autonomía académica, administrativa y financiera y patrimonio independiente, regido por las normas que regulan el sistema educativo, el sector educativo y el servicio público de educación superior, cuyo objeto es "ampliar el acceso a programas de formación a través de la consolidación de un ecosistema de educación virtual abierta, pertinente, de calidad y que contribuya al mejoramiento de las condiciones de vida de los ciudadanos, así como la implementación de programas de formación virtual pertinente al territorio antioqueño, que desarrollen habilidades para la vida y el trabajo en los habitantes del Departamento, articulados con la ciencia, tecnología e innovación"

En concordancia con el Acuerdo 067 del 12 de diciembre de 2019, emanado del Consejo Directivo, se tiene establecido el siguiente planteamiento estratégico:

1.1. Planteamiento Estratégico de la Institución Universitaria Digital de Antioquia

1.1.1. Visión.

La Institución Universitaria Digital de Antioquia- IU. Digital será la mejor alternativa de acceso a programas de educación formal e informal en modalidad virtual, pertinentes y de calidad, que permitan formar de manera integral a los bachilleres y a los trabajadores de entornos tanto urbanos como rurales deseosos de mejorar sus condiciones de vida y laborales, en el propósito de impulsar la competitividad sistémica en Antioquia.

1.1.2. Misión

La Institución Universitaria Digital de Antioquia, es una institución de educación superior que, mediante un ecosistema de educación virtual abierto, responde a las necesidades de formación integral, de cualificación del talento humano y de acceso al conocimiento de todas las personas en cualquier lugar del territorio; a través de una oferta educativa pertinente, de calidad, que posibilite igualdad de oportunidades, que elimine las barreras geográficas que tradicionalmente han sido un factor generador de inequidad en nuestro Departamento, el País y el mundo.

Somos una institución que, mediante la docencia, la investigación y la extensión, busca potenciar las capacidades de las personas y facilitar la adquisición de competencias para la vida y el trabajo, que les permitan elevar la calidad de vida y la competitividad sistémica en todos los entornos urbanos y rurales.

1.1.3. Objeto

La Institución de Educación Superior “Institución Universitaria Digital de Antioquia – IU. Digital” tiene como objeto principal la educación en la modalidad digital en ambientes virtuales de aprendizaje para la formación integral dentro del espíritu comunitario y solidario.

1.1.4. Objetivos

La Institución adopta como objetivos generales los contenidos en el capítulo II del Título Primero de la Ley 30 de 1992.

1.1.5. Objetivos Generales

A. Aportar a la formación integral de los colombianos y, en especial, a los de las distintas subregiones del Departamento de Antioquia, dentro de las modalidades y calidades de la educación superior, capacitándolos para cumplir las funciones profesionales, investigativas y de servicio social que requiera el país.
B. Trabajar por la creación, desarrollo y difusión del conocimiento en todas sus formas y expresiones y, promover su utilización en todos los campos para atender las necesidades del país.
C. Prestar a la comunidad un servicio con calidad, el cual hace referencia a los

resultados académicos, a los medios y procesos empleados, a la infraestructura institucional, a las dimensiones cualitativas y cuantitativas de mismo y a las condiciones en que se desarrolla la institución.

D. Propiciar el desarrollo científico, cultural, económico, político y ético a nivel nacional y regional.

E. Actuar armónicamente entre si y con las demás estructuras educativas y formativas del departamento del país.

F. Contribuir al desarrollo de los niveles educativos que le preceden, para facilitar el logro de sus correspondientes fines.

G. Promover la unidad nacional, la descentralización, la integración regional y la cooperación interinstitucional, con miras a que las diversas zonas dl país dispongan de los recursos humanos y de las tecnologías apropiadas que les permitan atender adecuadamente sus necesidades.

H. Promover la formación y consolidación de comunidades académicas o investigativas y la articulación con sus homólogas a nivel internacional.

I. Promover la preservación de un medio ambiente sano y fomentar la educación y cultura ecológica.

J. Conservar y fomentar el patrimonio cultural del país.

1.1.6. Objetivos Específicos

a) Consolidar comunidades académicas, definiendo procesos de enseñanza y de aprendizaje, que se realicen en estrecho contacto con la gente y la calidad de la educación superior.

b) Determinar, dentro de su función académica y administrativa, la identificación y evaluación permanente de necesidades en competencias requeridas por el sector productivo y la sociedad en general, definiendo así metodologías que aseguren la pertinencia de los programas y el diseño de los currículos servidos en la institución.

c) Contribuir en la diseminación del saber dentro de la comunidad mediante articulación con los diferentes niveles de la educación, buscando el fortalecimiento de las áreas misionales institucionales.

d) Integrar la investigación, desarrollo e innovación a los currículos.

e) Hacer que las TIC's sean en la Institución una herramienta metodológica para mejorar los procesos enseñanza-aprendizaje.

f) Definir mecanismos que estimulen en el personal docente y discente una

actitud positiva y funcional hacia la investigación, el desarrollo y la innovación, en áreas de las ciencias o de la tecnología, o que le permitan profundizar teórica y conceptualmente, en el campo de la filosofía, las humanidades y las artes.

g) Vincular la investigación, el desarrollo y la innovación a la orientación de la función profesoral en los procesos de desarrollo de la región y de la sociedad en general.

h) Hacer que el educador utilice sistemas de evaluación donde el estudiante, haciendo uso de las habilidades y destrezas desarrolladas en el curso, aplique los conocimientos adquiridos a diferentes situaciones, por medio del desarrollo de los procesos de transferencia, integración, análisis, sistemas de interpretación, entre otros.

i) Disponer de un educador: -Preparado para el cambio, que investigue, planee, organice y aplique nuevos procesos de aprendizaje, - Generador de condiciones, por medio de la DINÁMICA DE LA INVESTIGACIÓN, que conduzcan a los estudiantes a desarrollar actitudes que le permitan diagnosticar nuevas situaciones, anticiparse a ellas y participar activamente en la solución de los problemas que éstas generen, - Que desarrolle un proceso de ENSEÑANZA APRENDIZAJE en el cual, la actividad central esté dirigida a darle la oportunidad al estudiante de: aprender a hacer, aprender a hacerse, aprender a aprender, aprender a autoevaluarse, aprender a ser y aprender a servir, - Cuyo papel sea de orientador, de estimulador, de retroalimentador y de enriquecedor de la personalidad de los educandos.

j) Proyectar una dimensión humanística integrada donde se practiquen las sanas costumbres, los valores de la existencia humana y el respeto a las normas que nos rigen.

k) La Institución Universitaria Digital de Antioquia -IU. Digital- se propone ser un instrumento para la consolidación de la paz a través del ejercicio de su responsabilidad misional, con criterios de inclusión, igualdad y calidad; educando y formando personas competentes y de bien.

1.1.7. De los Principios de la Institución Universitaria Digital de Antioquia

La Institución Universitaria Digital de Antioquia, en cumplimiento de sus objetivos adopta como principios los contenidos en la Ley 30 de 1992 y en aquellas que la

adicionen, modifiquen o sustituyan. Coherente con la filosofía y en desarrollo de su autonomía, basa su gestión en los siguientes principios:

a) Responsabilidad social. Instituye la responsabilidad social para el cumplimiento de su Misión y Visión, teniendo en cuenta que responde ante la sociedad mediante sus órganos de gobierno.
b) Excelencia académica. Encamina su labor hacia la consecución de niveles de excelencia, para lo cual no escatimará esfuerzos que lo conduzcan a obtener logros cada vez mayores en los procesos académicos.
c) Innovación. Dada su vocación técnica y tecnológica, la Institución apoya y fomenta actividades conducentes a la innovación, en los campos que tengan que ver con el ejercicio de la docencia, la investigación y la extensión, con el fin de contribuir de manera eficiente y constante al desarrollo local, regional y del país.
d) Equidad e inclusión. Se compromete a llevar a cabo sus actuaciones con justicia, buscando el beneficio educativo de todos.
e) Universalidad. Orienta sus procesos de docencia, extensión, proyección social e investigación, hacia la búsqueda de diversidad de campos del conocimiento y hacia el impulso del saber, mediante las relaciones entre campos especializados de la ciencia y la tecnología.
f) Solidaridad. Impulsa las relaciones interpersonales basadas en la dignidad humana, estrategias de crecimiento y de sensibilidad social, para el beneficio común.
g) Sentido de ciudadanía. Expresado mediante la creación de espacios de convivencia que faciliten la colaboración y el apoyo, mediante la consolidación en un ambiente de respeto y apertura en las relaciones interpersonales, que aporten al desarrollo de la ética y al compromiso ciudadano.
h) Convivencia. Al acoger la condición social del Hombre, la Institución establece como uno de sus principios básicos el de la convivencia de sus participantes, mediante el respeto mutuo y el tratamiento constructivo de la divergencia de ideas y el acatamiento a los principios de la dignidad humana.
i) Transparencia. Uno de los fundamentos de la acción Institucional es la transparencia, entendida como la rectitud y coherencia en el obrar y la disposición permanente de hacer públicos todos sus actos.
j) Participación. En su labor de formar ciudadanos, promueve actitudes críticas y fomenta la participación ciudadana, estimula el trabajo en equipo, la

cooperación y ofrece respuestas a los retos que impone la democracia.

2. LA POLÍTICA DE ADMINISTRACIÓN DE RIESGOS DE LA INSTITUCIÓN UNIVERSITARIA DIGITAL DE ANTIOQUIA.

La política de administración del riesgo de la Institución Universitaria Digital de Antioquia es un instrumento que soporta en forma técnica y objetiva el compromiso de la Institución Universitaria frente al cumplimiento de los objetivos Institucionales, además de la generación del valor público en la sociedad, en la garantía del goce del derecho fundamental, en particular de la educación.

La Política de administración de riesgos, tiene su centro en el Modelo Integrado de Planeación y Gestión MIPG, en la Norma Técnica Colombiana NTC-ISO 31000:2018, el Decreto 2641 del 2012, por el cual se reglamentan los artículos 73 y 76 de la Ley 1474 de 2011 y la “Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas” V5, expedida por el Departamento Administrativo de la Función Pública.

2.1. Objetivos

a) Orientar la toma de decisiones respecto al tratamiento de los riesgos y sus efectos al interior de la Institución Universitaria
b) Establecer los parámetros necesarios para una adecuada administración de los riesgos a través de los elementos: contexto estratégico; identificación de riesgos; análisis de riesgos; valoración de riesgos; políticas de administración del riesgo, su trazabilidad, registro y monitoreo.
c) Orientar la toma de decisiones para la prevención del riesgo.
d) Incentivar el pensamiento basado en riesgos dentro de la entidad.
e) Buscar la mejora continua en cada uno de los procesos.

2.2. Alcance

La Administración del Riesgo en la Institución Universitaria Digital de Antioquia tendrá el siguiente alcance:

a) ***Los Riesgos aplicados a los procesos:*** están dirigidos a gestionar los riesgos aplicados al Modelo de Operación por Procesos de la IU DIGITAL, los cuales cubren todos los procesos, los proyectos y los servicios que ofrece la Institución Universitaria y que representen una probabilidad de impacto sobre el cumplimiento de los objetivos institucionales.

b) ***Los Riesgos de Corrupción:*** contemplan cualquier posibilidad de que, por acción u omisión, se use el poder para desviar la gestión institucional hacia un beneficio privado.

La gestión de los riesgos de corrupción serán un componente del Plan Anticorrupción y Atención al Ciudadano, en adherencia con Establecido en la Ley 1474 de 2011 (artículo 73) y el Decreto 124 de 2016 (artículo 2.1.4.1.)

c) **Riesgos de seguridad de la Información o ciberseguridad:** Como aquellos diferentes peligros que afectan el nivel informático y que pueden producir situaciones de amenaza a la IU DIGITAL. Cuando se habla de ciberseguridad, el análisis de riesgos informáticos es la evaluación de los diferentes peligros que afectan a nivel informático y que pueden producir situaciones de amenaza a la Institución Universitaria, como robos o intrusiones que comprometan los datos, la información, las redes o las plataformas, también se refiere a los ataques externos que impidan el funcionamiento de los sistemas propiciando periodos de inactividad en la organización.

El instrumento a utilizar será Modelo de Gestión de Riesgos de la Seguridad Digital, emanado del Ministerio del as TICs.

En conclusión, esta política de administración de los riesgos contribuye al desarrollo de la calidad de los controles internos en la Institución Universitaria en la vía de la generación del Valor Público en la comunidad.

2.3. Metodología para la Gestión de los Riesgos

El diseño y ejecución de la Administración del Riesgo en la Institución Universitaria están sujetos a las orientaciones que sobre la materia impartan el Departamento Administrativo de la Función Pública y las normas y estándares internacionales sobre el particular.

Se construirá el mapa de riesgos por cada uno de los procesos de la Institución Universitaria, es decir por cada uno de los líderes de procesos de la entidad, quienes trabajarán de la mano de la Oficina Asesora Planeación, el Mapa de riesgos institucional, el cual contendrá los riesgos con su respectiva valoración.

El mapa de riesgos de corrupción se elaborará por cada uno de los procesos, con el acompañamiento de la Oficina Asesora de Planeación y, según las directrices del Plan de Anticorrupción y Atención al Ciudadano, de conformidad con los lineamientos contenidos en el artículo 73 de la Ley 1474 de 2011, y la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas versión

Las responsabilidades que se deberán cumplir respecto a la gestión del riesgo de seguridad digital serán las siguientes:

a) Definir el procedimiento para la Identificación y valoración de Activos.
b) Adoptar o adecuar el procedimiento formal para la gestión de riesgos de seguridad digital (Identificación, Análisis, Evaluación y Tratamiento).
c) Asesorar y acompañar a la primera línea de defensa en la realización de la gestión de riesgos de seguridad digital y en la recomendación de controles para mitigar los riesgos.
d) Apoyar en el seguimiento a los planes de tratamiento de riesgo definidos.
e) Informar a la línea estratégica sobre cualquier variación importante en los niveles o valoraciones de los riesgos de seguridad digital.

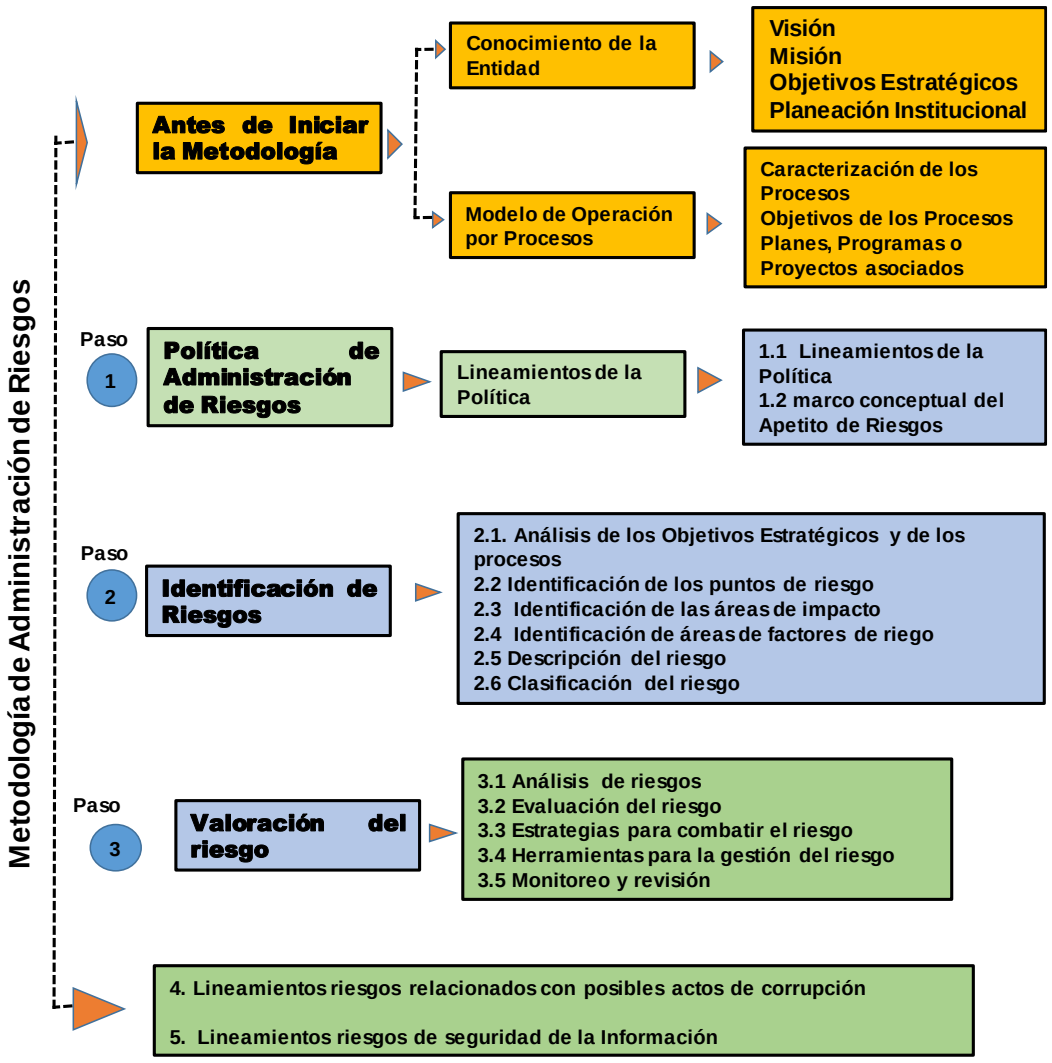
En el contexto de seguridad digital son activos, los elementos tales como aplicaciones de la entidad pública, servicios Web, redes, información física o digital, Tecnologías de la Información -TI- o Tecnologías de la Operación -TO-) que utiliza la organización para su funcionamiento.

La identificación y valoración de activos debe ser realizada por la primera línea de defensa – líderes de proceso, en cada proceso donde aplique la gestión del riesgo de seguridad digital, siendo debidamente orientados por el responsable de seguridad digital o de seguridad de la información de la Institución Universitaria.

2.4. La Estructura de la Administración de Riesgos

La Estructura de la Administración de Riesgos de la Institución Universitaria Digital de Antioquia guardará plena adherencia con la metodología adoptada por la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas – Versión 5, propuesta por el Departamento Administrativo de la Función Pública. En consecuencia, la estructura será la siguiente:

Metodología para la Administración del Riesgo[1]



1 Tomado de Guía para la administración del riesgo y el diseño de controles en las entidades públicas v5-2020 DAFP

2.5. Contexto para la Administración de los riesgos

El Contexto Interno y Externo para la Administración de Riesgos, permite identificar situaciones que afecten la operación de la Institución o el cumplimiento de sus objetivos, a fin de establecer el lineamiento estratégico que oriente las decisiones de la entidad pública frente a los riesgos que la puedan afectar.

El Contexto de la administración de riesgos, es producto de la observación, distinción y análisis del conjunto de factores internos y externos que pueden generar situaciones de riesgo. Un análisis más acertado requiere tener en cuenta la naturaleza jurídica y técnica de la entidad, sus objetivos, la misión y la visión, la estructura organizacional, los aspectos operativos, financieros y legales y la percepción de los diferentes grupos de interés.

El Contexto de riesgos se establece a partir de la identificación de circunstancias internas y externas a la entidad que pueden afectar el cumplimiento de sus objetivos.
Constituye la base para la identificación de los Riesgos en los Macroprocesos, Procesos y Procedimientos. Su análisis es realizado, a partir del conocimiento de las situaciones del entorno político, social, económico, cultural, tecnológico y ambiental. Se complementa con el estudio interno de la entidad, el diagnóstico del ambiente de control, la estructura organizacional, el modelo de operación y el cumplimiento de los planes y programas.

2.5.1. Requerimientos para la identificación del Contexto

a) Función constitucional y legal de la entidad
b) Normas que regulan la entidad
c) Los Objetivos contemplados en la Ordenanza 074 de 2017 sobre la creación de la Institución Universitaria Digital de Antioquia
d) El Autodiagnóstico del Modelo Integrado de Planeación-MIPG.
e) El Plan Nacional de Desarrollo vigente
f) El Plan del Departamento de Antioquia, vigente.
g) Estudios sectoriales realizados por entidades públicas o privadas.
h) Información sobre los avances tecnológicos de interés para la entidad.
i) La Estructura Organizacional
j) Los avances sobre la economía y educación digital

A continuación, se presenta un sugerido de los factores del contexto externo e interno que de alguna manera pueden afectar positiva o negativamente el cumplimiento de los objetivos de la Institución Universitaria Digital de Antioquia.

2.5.2. Contexto Externo

Conjunto de variables del ambiente externas que pueden afectar o beneficiar el cumplimiento de los objetivos de la Institución Universitaria Digital.

Factores Externos	Descripción de la amenaza
Económico:	Desaceleración del crecimiento económico. Aumento del desempleo con mayor impacto en los jóvenes y la mujer. Factores económicos por emergencia nacional. Creciente necesidad de creación de pequeñas y medianas empresas. Reducido gasto público en educación. Aumento de los niveles en la tasa de desempleo. Incremento de costo de vida. Insostenibilidad fiscal del país. Sobre oferta de profesionales para la empleabilidad. Incremento del dólar y caída del petróleo (divisas).
Medioambiental y de Salud:	Desastres naturales en algunas subregiones de Antioquia. Contaminación del aire por material particulado. Uso de tecnologías sostenibles con el medio ambiente. Pérdida de cobertura vegetal en el país . Incremento en un 50% en el mercado de productos ecológicos. Reactivación del mercado agrícola. Sistemas nacionales de innovación orientados al cumplimiento de objetivos de desarrollo sostenible. Reforma rural integral agraria. Pandemias: como la COVID-19 y otras
Político:	Cambio de Gobierno Departamental, cada cuatro años. Polarización por intereses políticos. Voluntad política volátil. Auge de movimientos sociales. Corrupción en el Estado. Imagen, marca y reputación del estado fragmentada. Reestructuración de Planes de Desarrollo. Aumento en la estructuración de la gobernanza. Tensiones geopolíticas.
	Deterioro del orden público en algunas subregiones de Antioquia. Dificultades de orden público en municipios del país.

Social:	Oferta educativa en las regiones no consecuente con las demandas sociales. Incumplimiento de la meta para superar el analfabetismo (5,8% a 3,8%). Aumento de la protesta social. Adaptación del modelo educativo actual. Inserción y uso de TICs en actividades sociales. Violencia politizada hacia líderes sociales Pérdida de rasgos culturales en el país.
Tecnológico:	Desactualización tecnológica. Saturación de redes de servicio por incremento en la demanda. Ausencia de infraestructura y redes en zonas rurales y urbanas. Limitación de cobertura y acceso a nuevas tecnologías. Analfebetización tecnológica. Gobernanza e implementación deficiente de la política de CTI. Favorecimiento de redes 5G en el desarrollo del internet. Debilidad para el Desarrollo de Tecnologías Emergentes.
Cultural digital	Bajas competencia digital
Conectividad	Baja cobertura de conectividad en internet en algunas subregiones del Departamento de Antioquia y del País, en especial en zonas rurales.
Legislación en materia de educación Superior	Obsolescencia de la legislación en educación superior frente a los entornos digitales. Directiva Ministerial No.4: Adopción de virtualidad por parte de IES.
Legislación laboral	Obsolescencia de la legislación laboral en relación con los entornos digitales. Ley de Crecimiento 2020 (Reforma tributaria). Agenda Mundial educación 2030, objetivos de Desarrollo Sostenible (4).
Contratación	La tramitología inmersa en la contratación para dar celeridad a los contratos para atender situaciones del entorno digital. Rigidez en políticas nacionales. Decreto legislativo 491 de 2020 Ministerio de Justicia y del Derecho.

2.5.3. Entorno Interno

Conjunto de variables del ambiente interno que pueden afectar o beneficiar el cumplimiento de los objetivos de la Institución Universitaria Digital.

Factores Internos	Descriptor de la Debilidad
Direccionamiento Estratégico y planeación Institucional.	Ausencia del Modelo de Universidad Digital, vinculado al Planteamiento Estratégico de la Institución Universitaria.

Factores Internos	Descriptor de la Debilidad
	Rigidez en el sistema de planeación frente al entorno cambiante de la economía digital y sus demandas. Carencia de un modelo de gestión del conocimiento e innovación.
Gestión presupuestal y eficiencia del gasto público	Presupuesto insuficiente para gastos de inversión y funcionamiento. Limitada generación de recursos propios.
Talento humano	Bajas competencias laborales frente a entornos digitales, como, por ejemplo: • Visión estratégica frente al ADN Digital • Liderazgo en red • Gestión de la Información • Trabajo en red • Comunicación Digital • Aprendizaje Continuo Conocimiento Digital • Orientación al usuario Comunicaciones internas fragmentadas.
Integridad	• Desconocimiento de los Principios de la Función Administrativa del Estado • Desconocimiento del Código de integridad • Inexistencia de los acuerdos, compromisos o protocolos éticos.
Transparencia, acceso a la información pública y lucha contra la corrupción	Altos niveles de opacidad en la gestión y los resultados Inexistencia de un Modelo de Comunicación Pública en la Institución Universitaria.
Fortalecimiento organizacional y simplificación de procesos	Rigidez de las operaciones de los procesos frente al entorno cambiante del entorno digital. Desarticulación en los procesos institucionales.
Participación ciudadana en la gestión pública	Débiles mecanismos de participación de la comunidad universitaria en la gestión
Servicio al ciudadano	Deficiencias en la atención a la comunidad universitaria y demás grupos de interés.
Racionalización de trámites	Rigidez de las operaciones de los procesos frente al entorno cambiante del entorno digital.
Gestión documental	Pérdida de información, obstáculos para la consulta de la información.
Gobierno Digital, antes Gobierno en Línea	Comunicaciones desestructuradas con grupos de valor.
Seguridad Digital	Fuga de Información, Pérdida de la confidencialidad, Pérdida de la integridad, Pérdida de la disponibilidad.
Defensa jurídica	Inexistencia de la estrategia de defensa administrativa o judicial, atendiendo las políticas de prevención del daño antijurídico establecidas por el Comité de Conciliación y

Factores Internos	Descriptor de la Debilidad
	Defensa Judicial de la Institución Universitaria Digital de Antioquia.
Gestión del conocimiento y la innovación	Falta de competencias laborales para la gestión del conocimiento y el diseño de programas de innovación. Investigación incipiente. Limitada oferta de programas académicos y cursos cortos. Baja apropiación de herramientas e instrumentos tecnológicos.
Control interno	Ineficacia de los controles internos.
Seguimiento y evaluación del desempeño Institucional	Ausencia de directrices e Instrumentos para la realización del monitoreo, seguimiento y evaluación a la gestión institucional.
Mejora Normativa	Desconocimiento de la normatividad aplicable a los procesos y a los servicios entregados a la comunidad. Ausencia de mecanismo para emprender acciones de evaluación para determinar el grado de cumplimiento de las normas aplicables a la entidad. (Evaluación a la autorregulación).

2.5.4. Contexto del Proceso

Conjunto de variables relacionadas con el Modelo de Operación por Procesos que pueden afectar o beneficiar el cumplimiento de los objetivos de la Institución Universitaria Digital.

Diseño del Proceso	Reciente apropiación de los procesos en la fase de implementación por parte de los responsables y demás servidores.
Las Interacciones con los otros Procesos	Debilidades en el establecimiento de las interacciones de los procesos normalizados en la Institución Universitaria. Opacidad en las interacciones de los procesos
La Transversalidad	Falta de concientización de la relevancia de la caracterización de los procesos y los procedimientos.
Procedimientos Asociados	Reciente aplicación de los procedimientos por medio de los registros y formatos.
Responsables del Proceso	Autoridad y responsabilidad difusa para el ejercicio de las operaciones y los controles. Por cuento existen dependencias que aún no tienen su planta de empleos requerida para el desempeño de sus funciones
La Comunicación entre los Procesos	Debilidades en la difusión del plan de medios de comunicación entre los responsables de los procesos,
Los activos de seguridad digital del Proceso	No identificación apropiada los activos digitales

2.5.5. Esquema de responsabilidades para la administración de los riesgos

Seguidamente se presentan los roles y responsabilidades por las líneas de defensa, para asumir las acciones que se deben emprender a fin de garantizar la eficacia de los resultados para la gestión de los riesgos en la Institución Universitaria Digital de Antioquia. En todo caso, la responsabilidad de la gestión del riesgo está asignada a todas las dependencias de la Institución Universitaria, así como a los empleados públicos en todos los niveles, a los docentes, e igualmente a los contratistas.

ROL	FUNCION
Alta Dirección: – Comité Institucional de Coordinación de Control Interno (Línea Estrategica)	• Analizar los cambios en el entorno (contexto interno y externo) que puedan tener un impacto significativo en la operación de la entidad y que puedan generar cambios en la estructura de riesgos y controles. • Evaluar el estado del sistema de control interno y aprobar las modificaciones, actualizaciones y acciones de fortalecimiento del mismo • Establecer la Política de Administración de Riesgos. • Realizar seguimiento y análisis periódico a los riesgos • Formular las recomendaciones como producto del seguimiento periódico a los riesgos. • Verificar la aplicación efectiva de las recomendaciones formuladas.
Líderes de procesos y sus equipos de trabajo (primera línea de defensa)	• Identificar los riesgos y controles de procesos y proyectos a cargo en cada vigencia. • Aplicar los controles para atenuar los riesgos • Realizar seguimiento y análisis a los controles de los riesgos, para determinar la eficacia de los controles • Actualizar el mapa de riesgos cuando la administración de los mismos lo requiera
Oficina Asesora de Planeación (Segunda línea de defensa)	• Asesorar a la primera línea estratégica en el análisis del contexto interno y externo, para la definición de la política de riesgo, el establecimiento de los niveles de impacto y el nivel de aceptación del riesgo. • Consolidar el Mapa de riesgos institucional (riesgos de mayor criticidad frente al logro de los objetivos) y presentarlo para análisis y seguimiento ante el Comité de Gestión y Desempeño Institucional • Acompañar y orientar sobre la metodología para la identificación, análisis, calificación y valoración del riesgo. • Monitorear cambio de entorno y nuevas amenazas.

	• Presentar al CICCI los resultados el seguimiento a la eficacia de los controles en las áreas identificadas en los diferentes niveles de operación de la entidad
Oficina Asesora de Auditoría Interna (Tercera línea de defensa)	• Asesorar a la Institución en metodologías, herramientas y técnicas para la identificación y administración de los riesgos y controles en coordinación con la segunda línea de defensa. • Identificar y evaluar a través de la auditoria interna y las evaluaciones periódicas de riesgos; la efectividad de la gestión del riesgo en la entidad así como la adecuada aplicación de controles, planes de contingencia y actividades de monitoreo vinculados a riesgos clave en la entidad. • Establecer en el programa anual de auditorías basado en riesgos, aquellos procesos o unidades auditables que tienen mayor nivel de exposición del riesgo. • Comunicar al Comité Institucional de Coordinación del Sistema de Control Interno los cambios e impactos en la ealuación del riesgo que resulten de la evaluación independiente. • Alertar sobre la propabilidad de riesgo de fraude o corrupción significativo en las áreas auditadas.

2.5.6. Responsabilidad y autoridad con el acto de delegación frente a la Administración de los riesgos.

Cuando el Rector o algún miembro autorizado del equipo directivo deleguen determinadas funciones, dicha delegación debe ser consecuente con las obligaciones que asumió al ser parte del sector público, de modo que debe fijar claramente los derechos y obligaciones del delegado, obligándose a mantenerse informado del desarrollo de los actos delegados, impartir orientaciones generales sobre el ejercicio de las funciones entregadas, y establecer sistemas de control y evaluación periódica de los mismos para asumir los riesgos.

Por su parte, los funcionarios que ejerzan las funciones delegadas deben cumplir como mínimo los requisitos de solvencia moral probada, idoneidad profesional y experiencia para la representación que les es asignada

2.6. Actualización y Monitoreo de los Riesgos

La actualización del Mapa de riesgos se deberá hacer cada año al inicio de la vigencia y el monitoreo de los riesgos se deberá realizar trimestralmente y generar

el informe de autoevaluación, el cual deberá ser socializado por el líder del proceso a la totalidad de los servidores públicos de su dependencia y remitido a la Oficina Asesora de Auditoría Interna, junto con las actas de la socialización, en cumplimiento del procedimiento establecido.

Nota: cuando se identifique un nuevo riesgo o se determine la valoración del riesgo en zona de riesgo extrema, producto de un proceso de autocontrol o de auditoría interna, se implementarán de manera inmediata las acciones pertinentes, y se comunicará al Comité de Coordinación de Control Interno, para el respectivo aval de actualización del mapa de riesgos por procesos e institucional.

2.7. Evaluación y Seguimiento

La evaluación y seguimiento al levantamiento de los mapas de riesgo será responsabilidad de la Oficina de Control Interno (Tercera Línea), quien deberá realizar el examen sistemático e independiente para determinar si las actividades y los resultados, relacionados con la administración de riesgos, cumplen las disposiciones de las políticas, planes y acciones preestablecidos y si se aplican en forma efectiva y son aptas para alcanzar los objetivos.

La Oficina de Control Interno actuará como eje central de coordinación del monitoreo y reporte de riesgos y posibles desviaciones, sin comprometer su independencia y objetividad, así mismo y por lo menos una vez al año, comunicará al Comité Institucional de Coordinación de Control Interno, los resultados del seguimiento y evaluación a las políticas y al procedimiento de administración del riesgo, junto con las propuestas de mejoramiento y tratamiento a las situaciones detectadas.

2.8. Divulgación

A fin de establecer e implementar la cultura y el compromiso necesario que aseguren que la administración del riesgo se convierta en parte integral de la planeación de los procesos, se desarrollarán planes de capacitación, los cuales serán incorporados en el Plan Institucional de Capacitación de la Institución Universitaria y realizará las publicaciones que sean necesarias para lograr la sensibilización e interiorización de los funcionarios hacia el tema de la administración del riesgo.

2.9. Tratamiento de los conflictos de intereses

La Institución Universitaria Digital de Antioquia, condena y prohíbe que el Consejo Directivo, el Rector con su equipo directivo, los miembros de comités, los servidores públicos y todos aquellos vinculados con la Institución incurran, entre otras, en cualquiera de las siguientes prácticas:

a) Solicitar o recibir dádivas o cualquier otra clase de lucro proveniente directa o indirectamente del usuario del servicio, del funcionario, empleado de su dependencia que tenga interés en el resultado de su gestión.
b) Tener a su servicio en forma estable o transitoria para labores propias de su despacho personas ajenas a la Institución Universitaria.
c) Solicitar o aceptar comisiones en dinero o en especie por concepto de adquisición de bienes o servicios.
d) Utilizar indebidamente información privilegiada o confidencial para obtener provecho o salvaguardar intereses individuales propios o de terceros.
e) Ejecutar actos de violencia, malos tratos, injurias o calumnias contra superiores, subalternos o compañeros de trabajo.
f) Coartar la libertad para trabajar o no trabajar, para asociarse o permanecer en ella o retirarse.
g) Desempeñar simultáneamente más de un empleo público o recibir más de una asignación que provenga del tesoro público, o de empresas industriales y comerciales del Estado, salvo los casos expresamente determinados por la Ley.
h) Nombrar para el desempeño de cargos públicos a personas que no reúnan los requisitos legales o reglamentarios o darles posesión.

Tratamiento de los riesgos: se guardará adherencia sobre la base de los resultados obtenidos en la evaluación y valoración de los riesgos de cada proceso, en donde se determinaran los niveles de aceptación de riesgos, Para ello, y de acuerdo con la Guía de Administración de Riesgos y el Diseño de Controles para las Entidades Públicas,V5, emanada del DAFP, se tendrán en consideración las estrategias para combatir los riesgos, con base en los siguientes criterios: Reducir, Mitigar, Transferir, Aceptar o Evitar el riesgo.

Vale anotar, que cuando se trate de los riesgos de corrupción, la estrategia estará centrada única y exclusivamente en evitar el riesgo de corrupción.

2.10. Clasificación de los riesgos.

De acuerdo con los objetivos de la Institución Universitaria Digital de Antioquia, la misión, la visión, los servicios, los grupos de interés, la administración de los riesgos presenta la siguiente clasificación: Riesgos de Gestión aplicados a los procesos, Riesgos de Corrupción, Riesgos de Seguridad de la información o ciberseguridad.

Riesgos Aplicados a los Procesos: Es la gestión de los riesgos aplicados al Modelo de Operación por Procesos de la Institución Universitaria Digital de Antioquia el cual le da soporte al Modelo Integrado de Planificación y Gestión.

2.11. Tipología de los riesgos aplicados a los procesos

Estratégicos: Posibilidad de ocurrencia de eventos que afecten los objetivos estratégicos de la organización y por tanto impacten toda entidad.
Riesgos Gerenciales: Posibilidad de ocurrencia de eventos que afecten los procesos gerenciales y/o alta dirección.

Operativos: riesgos derivados de la operación y funcionamiento de los procesos para la generación de los servicios a los diferentes grupos de interés en la vía de la solución de los problemas y expectativas y en la garantía del goce del derecho fundamental de la educación.

Cumplimiento y conformidad: relacionados con la eficacia en la prestación de los servicios, en relación con el cumplimiento de la normatividad aplicable, (Principio de legalidad sobre las actuaciones), los objetivos, las metas, los indicadores de producto y los indicadores de resultado, así como de las características y atributos de los servicios entregados a la comunidad universitaria.

Operativos: riesgos derivados de la operación y funcionamiento de los procesos para la generación de los servicios a los diferentes grupos de interés en la vía de la solución de los problemas y expectativas y en la garantía del goce del derecho fundamental de la educación.

Financiero: establecidos a través del manejo de los recursos que incluyen la gestión presupuestal, contabilidad, tesorería y manejo sobre los bienes.
De imagen: en asocio con la percepción, credibilidad y confianza que generada por los grupos de valor hacia la entidad.

2.12. Riesgos de Corrupción

La posibilidad de ocurrencia de una conducta o comportamiento que puede derivar en una actuación corrupta, entendiéndose por tal el mal uso público del poder, para conseguir una ventaja ilegítima, generalmente secreta y privada que conlleva inmersos los siguientes elementos en conjunto:

- Es un tipo de comportamiento activo o pasivo de un servidor público.
- Es emanada del ejercicio de la función pública en cuanto configura un abuso de esta o de la legitimidad que inspira el Estado.

2.13. Tipologías de riesgos de corrupción

Peculado: apropiación para sí o para otros, uso indebido o aplicación diferente de los bienes, fondos o dineros de la IU. Digital, por parte de los funcionarios públicos encargados de su administración o custodia.

Celebración Indebida de Contratos: El servidor público que, por razón del ejercicio de sus funciones, y con el fin de obtener beneficio ilícito para él, para el contratista, o para un tercero, celebre o liquide contratos sin los requisitos legales.
Cohecho: recibir o solicitar una dádiva, utilidad o aceptar promesa remuneratoria, de forma directa o indirecta a cambio de realizar u omitir un acto relacionado al cargo.

Utilización inapropiada de información de la entidad para favorecer intereses particulares.

Falsedad Ideológica en Documento Público: Cuando un servidor público en ocasión del cumplimiento de sus funciones manipule un documento que puede servir de prueba allegando falsedades, ocultando parte de la verdad o toda la verdad.

Concusión: abusar del cargo constriñendo o induciendo a alguien a dar o prometer al mismo servidor o a un tercero, dinero o cualquiera otra utilidad indebida con el fin de cumplir sus funciones.

Tráfico de influencias: Utilizar influencias personales para recibir, dar o prometer, para sí mismo o para un tercero, beneficios, favores o tratamiento preferencial. Desaparición intencional de expedientes, debido a intereses particulares.

Riesgos de seguridad de la Información o ciberseguridad: los diferentes peligros que afectan a nivel informático y que pueden producir situaciones de amenaza a la Institución Universitaria, como robos o intrusiones que comprometan los datos, la información, las redes o las plataformas, también se refiere a los ataques externos que impidan el funcionamiento de los sistemas propiciando periodos de inactividad en la organización.

2.14. Tipología de los riesgos de la Seguridad de la información o ciberseguridad

De Información: relacionada con la calidad, seguridad, oportunidad, pertinencia y confiabilidad de la información manejada por la Institución Universitaria.

Tecnológicos: Posibilidad de ocurrencia de eventos que afecten la totalidad o parte de la infraestructura tecnológica (hardware, software, redes, etc.) de una entidad.

Confidencialidad: es la propiedad que impide que la información sea divulgada a personas, entidades o sistemas no autorizados, de manera que sólo puede acceder a ella aquellas personas que cuenten con la debida autorización y de forma controlada.

Integridad: Es la propiedad que busca proteger la exactitud de la información, y evitar que sufra modificaciones no autorizadas.

Disponibilidad de la información: Es garantizar que la información sea accesible y usable bajo demanda de un usuario autorizado, que esté disponible en todo momento, evitando interrupciones del servicio por cortes de electricidad, fallos de hardware, etc.

3. GLOSARIO

Riesgo: Efecto que se causa sobre los objetivos de las entidades, debido a eventos potenciales.

Nota: Los eventos potenciales hacen referencia a la posibilidad de incurrir en pérdidas por deficiencias, fallas o inadecuaciones, en el recurso humano, los procesos, la tecnología, la infraestructura o por la ocurrencia de acontecimientos externos.

Acciones de mejora: Las actividades determinadas e implantadas por los titulares y demás servidores públicos de las instituciones para fortalecer el Sistema de Control Interno Institucional, así como prevenir, disminuir, administrar y/o eliminar los riesgos que pudieran obstaculizar el cumplimiento de objetivos y metas.

Administración de Riesgos: El proceso sistemático que deben de realizar las instituciones para evaluar y dar seguimiento al comportamiento de los riesgos a que están expuestas en el desarrollo de sus actividades, mediante el análisis de los distintos factores que pueden provocarlos, con la finalidad de definir las estrategias y acciones que permitan controlarlos y asegurar el logro de los objetivos y metas de una manera razonable.

Autocontrol: La implantación que realizan los titulares de las instituciones, de los mecanismos, acciones y prácticas de supervisión o evaluación de cada sistema, actividad o proceso; ejecutado de manera automática por los sistemas informáticos, o de manera manual por los servidores públicos; y que permite identificar, evitar y, en su caso, corregir con oportunidad los riesgos o condiciones que limiten, impidan o hagan ineficiente el logro de objetivos.

Activo: En el contexto de seguridad digital son elementos tales como aplicaciones de la organización, servicios web, redes, hardware, información física o digital, recurso humano, entre otros, que utiliza la organización para funcionar en el entorno digital.

Control: Medida que permite reducir o mitigar un riesgo.
Causa: todos aquellos factores internos y externos que solos o en combinación con otros, pueden producir la materialización de un riesgo.
Causa Raíz: Causa principal o básica, corresponde a las razones por la cuales se puede presentar el riesgo.

Causa Inmediata: Circunstancias bajo las cuales se presenta el riesgo, pero no constituyen la causa principal o base para que se presente el riesgo.

Consecuencia: los efectos o situaciones resultantes de la materialización del riesgo que impactan en el proceso, la entidad, sus grupos de valor y demás partes interesadas.

Impacto: las consecuencias que puede ocasionar a la organización la materialización del riesgo.

Debilidad de Control Interno: La insuficiencia, deficiencia o inexistencia identificada en el Sistema de Control Interno Institucional mediante la supervisión, verificación y evaluación interna y/o de los órganos de fiscalización, que pueden evitar que se aprovechen las oportunidades y/u ocasionar que los riesgos se materialicen.

Evaluación de Riesgos: Determinar el impacto y la probabilidad del riesgo. Dependiendo de la información disponible pueden emplearse desde modelos de simulación, hasta técnicas colaborativas.

Factores de Riesgo: Son las fuentes generadoras de riesgos.

Factores de Oportunidad: La situación favorable en el entorno institucional, bajo la forma de hechos, tendencias, cambios o nuevas necesidades que se pueden aprovechar.

Gestión del riesgo: Proceso efectuado por la alta dirección de la entidad y por todo el personal para proporcionar a la administración un aseguramiento razonable con respecto al logro de los objetivos.

Impacto o efecto: Se entiende como las consecuencias que pueden ocasionar a la organización la materialización del riesgo.

Mapa de Administración de Riesgos: El tablero de control que refleja el diagnóstico general de los riesgos para contar con un panorama de los mismos e identificar áreas de oportunidad en la Institución.

Nivel del Riesgo: (Determinación del) Es el resultado de correlacionar el impacto y la posibilidad, con los controles internos existentes.

Probabilidad: se entiende la posibilidad de ocurrencia del riesgo. Estará asociada a la exposición al riesgo del proceso o actividad que se esté analizando. La

probabilidad inherente será el número de veces que se pasa por el punto de riesgo en el periodo de 1 año.

Riesgo Inherente: Nivel de riesgo propio de la actividad. El resultado de combinar la probabilidad con el impacto, nos permite determinar el nivel del riesgo inherente, dentro de unas escalas de severidad.

Riesgo Residual: El resultado de aplicar la efectividad de los controles al riesgo inherente.

Riesgo de gestión: Posibilidad de que suceda algún evento que tendrá un impacto sobre el cumplimiento de los objetivos. Se expresa en términos de probabilidad y consecuencias.

Apetito de riesgo: Es el nivel de riesgo que la entidad puede aceptar, relacionado con sus Objetivos, el marco legal y las disposiciones de la Alta Dirección y del Órgano de Gobierno. El apetito de riesgo puede ser diferente para los distintos tipos de riesgos que la entidad debe o desea gestionar.

Riesgo de Seguridad Digital: Combinación de amenazas y vulnerabilidades en el entorno digital puede debilitar el logro de objetivos económicos y sociales, así como afectar la soberanía nacional, la integridad territorial, el orden constitucional y los intereses nacionales. Incluye aspectos relacionados con el ambiente físico, digital y las personas.

Riesgo de corrupción: Posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado.

Plan Anticorrupción y de Atención al Ciudadano: Plan que contempla la estrategia de lucha contra la corrupción que debe ser implementada por todas las entidades del orden nacional, departamental y municipal.

Riesgo de Seguridad de la Información: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información.

Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).

Capacidad de riesgo: Es el máximo valor del nivel de riesgo que una Entidad puede soportar y a partir del cual se considera por la Alta Dirección y el Órgano de Gobierno que no sería posible el logro de los objetivos de la Entidad.

Confidencialidad: Propiedad de la información que la hace no disponible o sea divulgada a individuos, entidades o procesos no autorizados.

Disponibilidad: Propiedad de ser accesible y utilizable a demanda por una entidad. Integridad: Propiedad de exactitud y completitud.

Vulnerabilidad: Representan la debilidad de un activo o de un control que puede ser explotada por una o más amenazas.

Tolerancia del riesgo: Es el valor de la máxima desviación admisible del nivel de riesgo con respecto al valor del Apetito de riesgo determinado por la entidad.

Capacidad de riesgo: Es el máximo valor del nivel de riesgo que una Entidad puede soportar y a partir del cual se considera por la Alta Dirección y el Órgano de Gobierno que no sería posible el logro de los objetivos de la Entidad.

Nivel de riesgo: Es el valor que se determina a partir de combinar la probabilidad de ocurrencia de un evento potencialmente dañino y la magnitud del impacto que este evento traería sobre la capacidad institucional de alcanzar los objetivos. En general la fórmula del Nivel del Riesgo poder ser Probabilidad *Impacto, sin embargo, pueden relacionarse las variables a través de otras maneras diferentes a la multiplicación, por ejemplo, mediante una matriz de Probabilidad – Impacto.

4. ANEXOS

- Anexo 1. Ley 1474 de 2011.
- Anexo 2. Decreto 1082 de 2015.
- Anexo 3. Decreto 124 de 2016.
- Anexo 4. Estrategias construcción del PAAC V2 – 2015.
- Anexo 5. Guía para la gestión de riesgos de corrupción 2015.
- Anexo 6. Guía para la administración del riesgo y el diseño de controles en entidades públicas V5 - 2020