DIAGNÓSTICO DE SEGURIDAD AL SISTEMA DE INFORMACIÓN ACADÉMICO DE LA UNIVERSIDAD CENTRAL

ING. JOHAN FELIPE MUÑOZ LESMES

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
FACULTAD DE INGENIERÍA Y CIENCIAS BÁSICAS
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
CEAD JOSÉ ACEVEDO Y GÓMEZ
BOGOTÁ
2018

DIAGNÓSTICO DE SEGURIDAD AL SISTEMA DE INFORMACIÓN ACADÉMICO DE LA UNIVERSIDAD CENTRAL

ING. JOHAN FELIPE MUÑOZ LESMES

Proyecto de grado aplicado para optar por el título de Especialista en Seguridad Informática

DIRECTOR:

ING. JUAN JOSE CRUZ GARZÓN

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
FACULTAD DE INGENIERÍA Y CIENCIAS BÁSICAS
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
CEAD JOSÉ ACEVEDO Y GÓMEZ
BOGOTÁ
2018

Nota de aceptación:

_____

_____

_____

_____

_____

Firma del presidente del jurado

_____

Firma del jurado

_____

Firma del jurado

Bogotá, 12 de septiembre de 2018

DEDICATORIA

Dedico este trabajo de grado a mis padres Luis Felipe Muñoz Prieto y Miriam Alcira Lesmes Torres, que en paz descansen, ya que su ejemplo de perseverancia, esfuerzo y dedicación, me han permitido ser la persona que soy actualmente; gracias a sus enseñanzas he logrado alcanzar grandes metas y cumplir muchos objetivos.

También dedico este trabajo de grado a mi esposa Jenny Andrea Pérez, y a mis hijos Juan Andrés y Daniel Jerónimo, quienes me han acompañado en este proceso y me han facilitado los espacios para culminar con éxito esta etapa de mi vida.

AGRADECIMIENTOS

Agradezco a la Universidad Nacional Abierta y a Distancia UNAD, por permitirme realizar este proceso de formación académica que culmina con gran satisfacción, de igual manera agradezco a todos los profesores que en el transcurso de la especialización compartieron conmigo su conocimiento y estuvieron prestos a resolver las inquietudes y dudas presentadas.

Agradezco al ingeniero Juan José Cruz, quien me acompaño como director del proyecto, su tiempo y dedicación me permitió culminar con éxito la etapa de sustentación del proyecto de grado.

Agradezco a la Universidad, al ingeniero Ocampo director del Departamento de Informática, y a los demás directivos y colaboradores, quienes me permitieron aplicar y desarrollar mi proyecto de grado y estuvieron atentos a colaborar frente a las necesidades presentadas.

CONTENIDO

pág.

LISTA DE TABLAS

pág.

LISTA DE FIGURAS

pág.

LISTA DE ANEXOS

pág.

GLOSARIO

ACTIVO: cualquier elemento que conlleva un valor para la organización.

AMENAZA: elemento externo que puede afectar un sistema.

ADMINISTRACIÓN DEL PLAN DE CONTINUIDAD DEL NEGOCIO: es la administración del plan de continuidad que abarca toda la organización con el cual se pueden integrar todos los aspectos relacionados al plan de continuidad como lo son políticas, procesos, procedimientos, estrategias inherentes a la continuidad de la actividad comercial de la organización.

ANÁLISIS DE IMPACTO DEL NEGOCIO (BIA): proceso que permite identificar mediante un impacto específico la urgencia de restablecer un servicio crítico en la organización.

ANÁLISIS DE RIESGO: proceso de comprender la naturaleza del riesgo y para determinar el nivel de riesgo.

CONFIDENCIALIDAD: la información solo puede ser vista por quienes tienen autorización.

CRITERIOS DE RIESGO: términos de referencia respecto al cual el significado de riesgo se evalúa.

CONTROL: medida que puede modificar el riesgo.

DISPONIBILIDAD: la información está disponible cuando se requiere.

DESASTRE: evento que genera una interrupción del servicio en tiempos prolongados de tiempo que generan pérdidas importantes a la organización.

EVALUACIÓN DE RIESGOS: proceso general de identificación de riesgo, análisis de riesgo y de evaluación de riesgos.

FRECUENCIA: es el número de veces que se presenta un incidente en un periodo de tiempo.

FUENTE DE RIESGO: elemento que por sí solo o en combinación tiene el potencial intrínseco para dar lugar a riesgo.

GESTIÓN DEL RIESGO: actividades coordinadas para dirigir y controlar una organización con respecto al riesgo.

IMPACTO: es la afectación a la cual se ve expuesta la organización cuando se presenta un incidente.

INFORMACIÓN: conjunto de datos organizados que conforman un mensaje.

INTEGRIDAD: se refiere a asegurar que la información no ha sido alterada.

INCIDENTE DE SEGURIDAD: factor que altera la seguridad del sistema.

INCIDENTE DE TRABAJO: son los eventos que pueden suceder en la organización el cual puede causar afectación a la prestación del servicio sin estar vinculado a la operación específica del servicio afectado.

IDENTIFICACIÓN DEL RIESGO: proceso de encontrar, reconocer y describir los riesgos.

METODOLOGÍA: conjunto de métodos para desarrollar determinado trabajo.

NORMA: elemento que debe ser respetado y enmarca un actuar.

NIVEL DE RIESGO: magnitud de un riesgo, expresada en términos de la combinación de las consecuencias y su probabilidad.

PROBLEMA DE CONTINUIDAD DEL NEGOCIO: puede ser cualquier tipo de eventualidad que afecte la prestación del servicio.

PLANES DE CONTINGENCIA: normativas y medidas para responder a los eventos que generen interrupciones en los servicios de la organización.

PLAN DE CONTINUIDAD DEL NEGOCIO (PNC): elementos que componen toda la estructura documental y procedimental que permite continuar con la operación en caso de un evento que genere una interrupción del servicio.

PLAN DE RECUPERACIÓN DE DESASTRES (DRP): son las tareas detalladas que determinan el actuar en caso de presentarse un incidente que afecte la prestación del servicio.

PROBABILIDAD: probabilidad de que algo suceda.

RIESGO: materialización de una amenaza frente a una vulnerabilidad.

RIESGO RESIDUAL: riesgo restante después del tratamiento del riesgo.

SALVAGUARDA: medida para contrarrestar una falla de seguridad.

SEGUIMIENTO: control continuo, la supervisión, observación o crítica para determinar el carácter con el fin de identificar el cambio del nivel de rendimiento requerido o esperado.

TRATAMIENTO DE RIESGO: proceso para modificar el riesgo.

VULNERABILIDAD: debilidad de un sistema.

RESUMEN

En este proyecto se analizaron algunas fuentes documentales que se consideraron propicias para realizar un análisis de seguridad a un sistema de información, con la finalidad de determinar cuál o cuáles de ellas son las más adecuadas buscando implementar la metodología descrita en dicha fuente documental para realizar el diagnóstico de seguridad del sistema de información académico propio de la Universidad, en donde se hizo primordial la verificación de toda la estructura que compone el sistema académico tanto en hardware, software y demás elementos involucrados en la gestión y prestación del mismo; por este motivo se hizo necesario destacar metodologías de identificación de activos, análisis de riesgos, análisis de vulnerabilidades y tratamiento de riesgos para efectuar un análisis efectivo que permitiera fortalecer la seguridad del sistema académico.

INTRODUCCIÓN

Las instituciones de educación superior como es el caso de la Universidad, enfocan su modelo de negocio a la prestación de servicios educativos buscando eficiencia y calidad en la educación brindada a la comunidad estudiantil. La Universidad en veras de optimizar sus procesos como parte fundamental al apoyo de la gestión educativa, ha sistematizado los procesos necesarios para la gestión de matrículas, manejo de notas y horarios, actualización de datos, solicitudes de diferente índole a nivel académico y gestión de grados; para un mejor entendimiento lo anterior ha sido denominado como el Sistema de Información Académico.

El Sistema de Información Académico, ha permitido optimizar múltiples tareas relacionadas con la gestión de los estudiantes mejorando los tiempos de respuesta y atención, de manera adicional se ha reducido en un porcentaje alto el tiempo invertido por los estudiantes en la realización de los diferentes trámites gracias a las diferentes aplicaciones Web que evitan el desplazamiento y la realización de solicitudes de manera presencial.

Los beneficios de sistematizar los diferentes procesos mediante aplicaciones Web han sido evidentes, gracias a esto la imagen de la Universidad frente al servicio prestado ha mejorado considerablemente, de la misma manera se han reducido los errores humanos frente a la gestión de los datos de los estudiantes; por otro lado la Universidad ha pasado por alto múltiples detalles que han dejado en evidencia la seguridad de las aplicaciones Web implementadas en todo este proceso, lo cual ha sido evidente en los dos últimos semestres debido a suplantaciones de identidad que han generado problemáticas en los procesos de matrícula y cancelación de materias, por este motivo es primordial implementar una metodología que permita detectar y tratar los riesgos presentes de la manera más adecuada en la Universidad.

1. TÍTULO

DIAGNÓSTICO DE SEGURIDAD AL SISTEMA DE INFORMACIÓN ACADÉMICO DE LA UNIVERSIDAD CENTRAL

ÁREA DE CONOCIMIENTO: SEGURIDAD INFORMÁTICA

LÍNEA DE INVESTIGACIÓN: GESTIÓN DE SISTEMAS

2. DEFINICIÓN DEL PROBLEMA

2.1 ANTECEDENTES

Con el auge de las tecnologías de información, la gran mayoría de instituciones gubernamentales, empresas de servicios, instituciones educativas y del sector bancario han implementado soluciones informáticas para soportar los servicios prestados y de la misma manera soportar los procesos internos propios de la organización; con este tipo de implementaciones se obtienen grandes beneficios relacionados con la efectividad del servicio, tiempos eficientes de respuesta y agilidad en las operaciones, pero de la misma manera se expone la institución a un sinfín de riesgos latentes que a diario afectan a muchas organizaciones a nivel mundial.

En la actualidad la información es uno de los activos más importantes que tiene cualquier organización, por este motivo es indispensable enfocar grandes esfuerzos por asegurarla y preservarla; la información debe ser procesada, transmitida y almacenada, en todo este proceso intervienen muchos factores como lo son el factor tecnológico (equipos de cómputo, equipos de comunicaciones, software etc.), el factor humano (personal encargado del tratamiento de la información, personal encargado de la adecuación de los equipos computacionales etc.), y el factor gubernamental enfocado a las leyes sobre el tratamiento de la información, es por esto que debemos ver la información como un todo el cual debe ser protegido teniendo en cuenta diversos factores.

Los riesgos son muy variados y se pueden presentar en cualquier nivel, consiguiendo afectar la disponibilidad, la integridad y la confidencialidad de la información, por este motivo es de vital importancia establecer mecanismos y metodologías que permitan realizar un cuidadoso análisis en toda la organización, con lo cual se logrará identificar las áreas críticas y los sistemas de información que soportan dichas áreas a nivel organizacional, de esta manera evaluar todos los riegos que de alguna manera se logren materializar generando una afectación en los servicios prestados por dicha organización.

En el momento en que una organización tiene el conocimiento sobre sus activos o áreas sensibles además de los riesgos que se pueden presentar, puede comenzar a implementar controles o medidas que permitan minimizar o eliminar dichos riesgos, en el caso de no encontrar medidas de control o no poder aplicarlas por temas económicos o normativos, se entiende que se conoce el riesgo presente y lo asume de tal manera que ya no se presenta como un imprevisto, de esta forma no afecta la imagen de la organización frente a la confianza que debe existir con sus clientes o personal involucrado a la organización.

Teniendo en cuenta la innumerable cantidad de amenazas presentes, muchas organizaciones no han tomado el tema de seguridad informática con la seriedad que se merece, es por esto que en la actualidad se han dispuesto un número considerable de metodologías de análisis de riesgos y de normas certificables enfocadas a la gestión de la seguridad de la información, en donde se hace énfasis y se tiene como pilar fundamental el análisis y tratamiento de los riesgos informáticos, buscando de esta manera proteger a las organizaciones y a la información perteneciente a ellas.

Las aplicaciones Web son muy populares hoy en día, la proliferación de servicios en internet hace que este sea el escenario perfecto para que los piratas informáticos desplieguen su mejor arsenal en búsqueda de vulnerabilidades que les permitan comprometer la seguridad de los sitios web y de las aplicaciones que los componen.

La falta de formación en el desarrollo seguro por parte de los programadores Web, la falta de mantenimiento y actualización a los sistemas por parte de los administradores, la complejidad y tamaño de las aplicaciones Web hacen que estas sean menos seguras.

La problemática es tan fuerte que existen organizaciones dedicadas al tema de tratamiento de riesgos para aplicaciones web como es el caso del proyecto OWASP, que es un proyecto abierto de seguridad en aplicaciones Web, el cual busca crear conciencia en las organizaciones respecto a la seguridad de las aplicaciones y servicios web, ofreciendo al público herramientas para análisis de las aplicaciones web además de un listado de vulnerabilidades y medidas para contrarrestar buscar contrarrestarlas.

2.2 FORMULACIÓN

¿Cómo realizar el diagnóstico de seguridad al sistema de información académico de la Universidad?

2.3 DESCRIPCIÓN DEL PROBLEMA

La Universidad ha implementado diferentes aplicaciones Web exclusivas para la gestión académica las cuales se han denominado Sistema de Información Académico, estas aplicaciones han sido vulneradas a causa de suplantaciones de identidad que han afectado de manera directa la gestión académica de algunos

estudiantes, con lo cual la confianza de los estudiantes y del personal que opera dichas aplicaciones se ha reducido en menor cuantía, pero se estima que de seguir presentándose dichas situaciones la confianza se reduzca de manera considerable y la comunidad estudiantil opte por realizar los procesos de manera presencial y se reduzca el uso de los sistemas Web implementados.

Es necesario encontrar una metodología que se ajuste a la normatividad colombiana y que se pueda amoldar a las necesidades de la Universidad, con la cual se pueda realizar el diagnóstico de seguridad al sistema de información académico de la Universidad.

3. JUSTIFICACIÓN

La Universidad al ser una institución educativa, fundamenta su modelo de negocio en la prestación de servicios, buscando que estos sean eficientes y de calidad; esta búsqueda lleva a la implementación de diferentes tecnologías que por su naturaleza agilizan los diferentes procesos y minimizan los tiempos de atención. Entre las muchas tecnologías implementadas en la optimización de procesos están los servicios basados en aplicaciones Web, los cuales traen innumerables beneficios como pueden ser la realización de trámites en línea y la reducción del tiempo, pero la implementación de este tipo de tecnologías conlleva una variedad de riesgos que pueden atentar contra la disponibilidad del servicio prestado, la integridad de la información que se procesa en la aplicación y la confidencialidad de los datos almacenados; por lo anterior es primordial establecer mecanismos e implementar metodologías que permitan conocer las diferentes vulnerabilidades que están presentes en el sistema, identificar las amenazas que pueden sacar provecho de dichas vulnerabilidades y de esta manera detectar los riesgos que pueden comprometer la seguridad de las aplicaciones.

Las aplicaciones Web traen retos adicionales, ya que esta clase de aplicaciones están disponibles al público en Internet, por lo cual están expuestas a una variedad de ataques informáticos, además estas aplicaciones componen los portales Web, estos portales son la cara comercial de las empresas en Internet y al presentar fallas comprometen el nombre y la imagen comercial de las diferentes organizaciones.

4. OBJETIVOS DEL PROYECTO

4.1 OBJETIVO GENERAL

Realizar el diagnóstico de seguridad al sistema de información Académico, mediante metodologías de diagnóstico de seguridad informática, en la Universidad Central.

4.2 OBJETIVOS ESPECÍFICOS

1. Realizar el levantamiento de información de metodologías de diagnóstico de seguridad, análisis y gestión de riesgo informático, del estado actual del sistema de Información Académico de la Universidad.

2. Determinar y aplicar las metodologías de diagnóstico al sistema de Información Académica de la Universidad.

3. Realizar la propuesta del plan de tratamiento de riesgos.

4. Realizar el acompañamiento en la ejecución de la propuesta.

5. ALCANCE Y DELIMITACIÓN DEL PROYECTO

Este proyecto se realizará en la Universidad Central, específicamente para el Sistema de Información Académico el cual involucra las áreas de Registro Académico, Tesorería, Crédito y Cartera, Admisiones y Tecnología Informática.

El Sistema de Información Académico se compone de diferentes aplicaciones Web publicadas en el Portal Web Institucional, alojadas en un único servidor de aplicaciones, operadas desde diferentes estaciones de trabajo ubicadas en las áreas mencionadas anteriormente; estas aplicaciones Web están disponibles en internet para el servicio de los estudiantes de la Universidad.

El proyecto tiene como alcance el análisis y gestión de riesgos el cual se realizará sobre todos los elementos (humanos, hardware, software, procesos e información), que componen el Sistema de Información Académico, esto mediante el desarrollo de la metodología seleccionada para el tratamiento de riesgos.

En este proyecto se proponen las salvaguardas para subsanar los riesgos encontrados, además se contempla el acompañamiento en la implementación de las salvaguardas hasta llegar al riesgo residual junto a las soluciones planteadas; lo anterior implica decisiones de la alta dirección frente a inversión económica, modificación en los contratos con los proveedores y el personal vinculado a la universidad lo cual conlleva tiempos de ejecución excesivamente largos, por este motivo en la documentación del proyecto se hará énfasis en los riesgos residuales que impacten de manera significativa el Sistema de Información Académico de la Universidad junto con las propuestas de solución.

6. MARCO REFERENCIAL

6.1 MARCO TEÓRICO

En la actualidad existen diferentes metodologías y estándares para la gestión y tratamiento de riesgos que sirven de apoyo, entre las cuales se destacan las siguientes:

MAGERIT

Magerit es un metodología para la gestión de riesgos informáticos ajustado a la norma ISO 27001, con la finalidad de implementar un Sistema de Gestión de Seguridad de la Información (SGSI); la metodología es estructurada y sigue unos pasos específicos iniciando con la identificación de los activos de la organización, luego se identifican las amenazas que pueden afectar a dichos activos y de esta manera realizar todo el proceso de identificación de los riesgos; los procesos anteriores facilitan el tema de gestión y tratamiento de riesgos permitiendo que la tarea de análisis de seguridad sobre la organización a nivel informático sea completa y eficaz.

Magerit se expone en 3 libros que facilitan su implementación, estos son el libro del Método, el libro del Catálogo de Elementos y el libro de las Guías Técnicas.

Libro 1: Método.

En este método se inicia con el tema específico de análisis de riesgos, en un paso a paso que lleva a identificar los activos de la organización, luego se revisan las amenazas que se pueden ver materializadas en cada activo; al identificar las amenazas se puede detectar el impacto potencial que puede repercutir en la materialización de la amenaza sobre el activo y de la misma manera el riesgo potencial que puede sufrir el activo frente al impacto de la amenaza sobre el mismo; al conocer lo anterior es posible identificar los posibles salvaguardas necesarios para minimizar, eliminar o asumir el riesgo; al aplicar los salvaguardas se pude identificar el impacto residual o impacto que queda presente una vez realizado un tratamiento específico y de la misma manera se obtendrá un nuevo riesgo residual. Es importante ver como el método establece unas tareas o actividades específicas que son la caracterización de los activos, la caracterización de las amenazas, la caracterización de las salvaguardas y la estimación del estado del riesgo.

El método también muestra el proceso de gestión de riesgo donde se encuentran algunos conceptos tales como la evaluación en donde se trata en específico el tema de impacto y riesgo residual que resulta de la aplicación de los salvaguardas, la

aceptación del riesgo que se presenta cuando las condiciones no son propicias para la aplicación de salvaguardas o los mismos no son suficientes, los tratamientos que se pueden aplicar a los riesgos, los diferentes estudios como pueden ser los cuantitativos, los cualitativos y los mixtos de la relación costo beneficio y las diferentes opciones de tratamiento de riegos que son la eliminación en el caso de erradicar el riesgo, la mitigación que es reducirlo hasta un nivel aceptable, la compartición que habla propiamente de ceder el riego a un tercero o mantener una parte en la organización y por último la financiación que asume la inversión económica frente al riesgo presente en el caso que se materialice. Se encuentra además la formalización de las actividades propias del tema de gestión de riesgos en donde se definen los roles del personal involucrado en el sistemas de gestión las funciones específicas de cada miembro, el contexto en el cual se mueve la organización, los criterios sobre los cuales se realizará el tratamiento, la evaluación de los riesgos, las diferentes opciones de aplicabilidad de las salvaguardas, el tema de comunicación y consulta de los tratamientos aplicados y los respectivos seguimientos y revisiones al sistema de gestión en general lo cual es plasmado en la documentación requerida y se aplica la mejora continua mediante la implementación de indicadores de gestión.

En el método se encuentra la implementación de un proyecto de análisis de riesgos en donde se destacan actividades puntuales como la definición de los roles y funciones, la actividades preliminares tales como el estudio de oportunidad del proyecto, la definición del alcance del proyecto, la planificación del proyecto y la ejecución del mismo; posterior a estas tareas se centra en el análisis de riesgos y la comunicación formal de los resultados obtenidos especificando los puntos de control específicos y la documentación propia de dicha actividad.

El método muestra un esquema del plan de seguridad que en últimas es la agrupación de los diferentes proyectos de seguridad en donde se destaca la identificación de los mismos, la planificación, la ejecución y las listas de control de cada uno de los proyectos de seguridad.

Se puede encontrar un espacio para el desarrollo de sistemas de información que llevan inmerso la temática de análisis de riesgos y de seguridad, arrancando con la inicialización de los procesos, la seguridad a los sistemas de información con lo que cabe destacar el ciclo de vida de las aplicaciones, su contexto, las fases de especificación y diseño, el soporte, la aceptación de sistema de información, la operación del sistema de información, las tareas de mantenimiento, la terminación definiendo la documentación específica.

Por último, el método expone unos consejos prácticos enfocados al alcance y la profundidad, para la identificación de activos, para modelar las dependencias entre los activos detectados, para el tema de valoración de los activos y la identificación de las amenazas, para la parte de valoración de las amenazas detectadas y la selección de las salvaguardas aplicadas al sistema.

Libro 2: Catálogo de Elementos.

En el catálogo de elementos se encuentran los tipos de activos con lo cual se facilita la tarea del método para todo el tema de identificación de activos, este catálogo expone una amplia gama de activos en donde se destacan los de personal, de instalaciones, de hardware, de software, de servicios, de datos, de redes, de claves y los de activos esenciales.

Se encuentran las dimensiones de valoración de las cuales se destacan la Disponibilidad, la confidencialidad, la integridad, autenticidad y trazabilidad; además se evidencian algunos criterios de valoración como las escalas estándar.

Se expone el listado de todas las amenazas que pueden llegar a afectar a los activos y por último el listado de las salvaguardas que se aplican a cada activo para mitigar las amenazas presentes.

Libro 3: Guía de Técnicas.

En este libro se hace énfasis en las diferentes técnicas que permiten hacer las diferentes valoraciones y estimaciones indicadas en el método, esto es aplicable tanto al análisis de riesgos, las valoraciones de activos, los análisis de costos y beneficios, los análisis de vulnerabilidades entre otros.

ISO 27001: Es una norma certificable enfocada en las tecnologías de la información, las técnicas de seguridad y los Sistemas de Gestión de Seguridad de la Información, esta norma referencia las normas adicionales que componen la familia de ISO 27000, en donde se encuentra la ISO 27002 que contiene el listado de controles de seguridad, ISO 27035 que se enfoca en los incidentes de seguridad de la información y como aspecto principal se tiene la norma ISO 27005 la cual se enfoca en la gestión de riesgos tecnológicos.

Es importante destacar que las normas ISO 27000 han sido adoptadas por la Norma Técnica Colombia NTC, por lo cual es aplicable para empresas de cualquier sector en Colombia.

ISO/IEC 27000

Agrupa el conjunto de series o normas ISO/IEC 27000, los cuales son estándares de seguridad publicados y avalados por la ISO/IEC. La norma ISO/IEC 27000 trata específicamente sobre el vocabulario estándar utilizado en los SGSI, además habla sobre los documentos adicionales que conforman la familia 27000 y en general es la introducción y base de soporte para el resto de documentos que componen esta familia.

ISO/IEC 27001

Norma que hace parte de la familia ISO/IEC 27000, la cual especifica los requisitos para la implementación de un SGSI, esta norma en específico es fundamental ya que ella es la norma certificable y sobre la cual las organizaciones pueden llegar a certificar sus SGSI. Esta norma se enfoca en la gestión de riesgos y en la mejora continua de todo el sistema de gestión.

ISO/IEC 27002

Norma que hace parte de la familia ISO/IEC 27000, la cual se compone de todos los controles de seguridad expuestos en la ISO 17799, y se puede definir como el código de buenas prácticas en donde se tienen los controles posibles aplicables a la organización frente a los temas de seguridad de la información.

ISO/IEC 27005

Norma que hace parte de la familia ISO/IEC 27000, la cual se enfoca en el tratamiento o gestión de los riesgos en la seguridad de la información, en ella es posible vislumbrar técnicas de evaluación de riesgos, recomendaciones y lineamientos enmarcados en la gestión de los riesgos informáticos. Es destacable el tema de valoración, análisis y evaluación del riesgo a términos generales como fundamento de esta norma además de los anexos entre los cuales el anexo B ayuda con el tema de identificación y valoración de loa activos junto con la valoración del impacto en todo el proceso de gestión de riesgos.

ISO/IEC 27035

Norma que hace parte de la familia ISO/IEC 27000, la cual se enfoca en la gestión de incidentes de seguridad de la información; su objetivo se precisa en la detección de los incidentes de seguridad, esto conlleva al reporte y evaluación del mismo y las vulnerabilidades detectadas.

ISO 22301

Estándar internacional enfocado en la Gestión de la Continuidad del Negocio (BCM), en donde se busca minimizar el impacto generado a raíz de un evento catastrófico que pueda llegar a afectar la operación de la organización, logrando minimizar el cese de las operaciones o interrupciones del servicio ante eventos inesperados.

NTC-ISO-IEC 27001

Norma Técnica Colombiana la cual corresponde a la adopción idéntica (IDT) por traducción de la norma ISO/IEC 27001:2013, la cual se ha mencionado con anterioridad.

NTC-ISO-IEC 27002

Norma Técnica Colombiana la cual corresponde a la adopción idéntica (IDT) por traducción de la norma ISO/IEC 27002:2013, la cual se ha mencionado con anterioridad.

NTC-ISO-IEC 27005

Norma Técnica Colombiana la cual corresponde a la adopción idéntica (IDT) por traducción de la norma ISO/IEC 27005:2008, la cual se ha mencionado con anterioridad.

NCT ISO 31000

Norma Técnica Colombiana para la gestión del riesgo, principios y directrices. Norma enfocada a la gestión de riesgos aplicables a toda la serie de normativas NTC ISO.

NIST 800-30

Metodología de Gestión de Riesgos desarrollada por el Instituto Nacional de Estándares y Tecnología del Departamento de Comercio de los Estados Unidos; esta metodología se enfoca en la evaluación y gestión de riesgos propios de la seguridad de la información, destacando las tareas de gestión y evaluación de riesgos en donde es posible hablar de la preparación de la evaluación, la realización de la evaluación, la comunicación de los resultados de la evaluación y el mantenimiento de la misma. La metodología ayuda en la identificación de los factores de riesgo y la manera más adecuada de monitorearlos, además permite observar si el nivel de los riesgos ha aumentado de acuerdo con lo establecido por la organización.

6.2 MARCO CONCEPTUAL

- **Activo**: Cualquier elemento que conlleva un valor para la organización.
- **Información**: Conjunto de datos organizados que conforman un mensaje.
- **Vulnerabilidad**: Debilidad de un sistema.
- **Amenaza**: Elemento externo que puede afectar un sistema.
- **Riesgo**: Materialización de una amenaza frente a una vulnerabilidad.
- **Integridad**: Se refiere a asegurar que la información no ha sido alterada.
- **Confidencialidad**: La información solo puede ser vista por quienes tienen autorización.
- **Disponibilidad**: La información está disponible cuando se requiere.
- **Incidente de seguridad**: Factor que altera la seguridad del sistema.
- **Salvaguarda**: Medida para contrarrestar una falla de seguridad.
- **Norma**: Elemento que debe ser respetado y enmarca un actuar.
- **Metodología**: Conjunto de métodos para desarrollar determinado trabajo.
- **Administración del plan de continuidad del negocio**: Es la administración del plan de continuidad que abarca toda la organización con el cual se pueden integrar todos los aspectos relacionados al plan de continuidad como lo son políticas, procesos, procedimientos, estrategias inherentes a la continuidad de la actividad comercial de la organización.
- **Incidente de trabajo**: Son los eventos que pueden suceder en la organización el cual puede causar afectación a la prestación del servicio sin estar vinculado a la operación específica del servicio afectado.
- **Problema de continuidad del negocio**: Puede ser cualquier tipo de eventualidad que afecte la prestación del servicio.
- **Desastre**: Evento que genera una interrupción del servicio en tiempos prolongados de tiempo que generan pérdidas importantes a la organización.
- **Planes de contingencia**: Normativas y medidas para responder a los eventos que generen interrupciones en los servicios de la organización.
- **Plan de Continuidad del Negocio (PNC)**: Elementos que componen toda la estructura documental y procedimental que permite continuar con la operación en caso de un evento que genere una interrupción del servicio.
- **Plan de recuperación de desastres (DRP)**: Son las tareas detalladas que determinan el actuar en caso de presentarse un incidente que afecte la prestación del servicio.
- **Análisis de impacto del negocio (BIA)**: Proceso que permite identificar mediante un impacto específico la urgencia de restablecer un servicio crítico en la organización.
- **Frecuencia**: Es el número de veces que se presenta un incidente en un periodo de tiempo.
- **Impacto**: Es la afectación a la cual se ve expuesta la organización cuando se presenta un incidente.

- **Riesgo residual**: Riesgo restante después del tratamiento del riesgo.
- **Identificación del riesgo**: Proceso de encontrar, reconocer y describir los riesgos.
- **Nivel de riesgo**: Magnitud de un riesgo, expresada en términos de la combinación de las consecuencias y su probabilidad.
- **Gestión del riesgo**: Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo.
- **Criterios de riesgo**: Términos de referencia respecto al cual el significado de riesgo se evalúa.
- **Tratamiento de riesgo**: Proceso para modificar el riesgo.
- **Análisis de riesgo**: Proceso de comprender la naturaleza del riesgo y para determinar el nivel de riesgo.
- **Evaluación de riesgos**: Proceso general de identificación de riesgo, análisis de riesgo y de evaluación de riesgos.
- **Fuente de riesgo**: Elemento que por sí solo o en combinación tiene el potencial intrínseco para dar lugar a riesgo.
- **Seguimiento**: Control continuo, la supervisión, observación o crítica para determinar el carácter con el fin de identificar el cambio del nivel de rendimiento requerido o esperado.
- **Control**: Medida que puede modificar el riesgo.
- **Probabilidad**: Probabilidad de que algo suceda.

6.3 ESTADO DEL ARTE

La Universidad se encuentra certificada por la norma de calidad ISO 9001:2015, por este motivo existen una serie de documentos que hacen referencia a los procesos y procedimientos de toda la gestión administrativa.

Existen procedimientos específicos a la operación del Sistema de Información Académico, el tratamiento de datos, aplicación de parches y manejo por parte de los usuarios.

Existe un procedimiento específico sobre la gestión y tratamiento de riesgos propio para la gestión de riesgos del sistema de gestión de calidad implementado bajo la norma ISO 9001:2015, del cual se desarrollará el modelo para la gestión de riesgos enfocado en el Sistema de Información Académico, adicional cabe destacar que nunca se ha realizado un análisis de riesgos sobre el Sistema de información Académico por lo cual es incierto el estado del mismo.

Se pueden destacar procesos y procedimientos específicos de la siguiente manera:

Tabla 1. Procesos y procedimientos de la Universidad

Proceso	Procedimiento
Respaldo a sistemas	Copia en frío. Copia en caliente. Clonación de bases de datos.
Soporte de hardware	Mantenimiento preventivo de equipos de cómputo. Atención de casos de hardware. Monitoreo de Plataforma tecnológica.
Desarrollo de software	Atención de casos de software. Soporte y mantenimiento de software. Actualización de Software Base Servidores. Desarrollo de Software
Administración de Servicios Informáticos	Administración de usuarios en aplicativos institucionales y servicios básicos de red. Asignación, cambio y custodia de claves de administración. Gestión de acceso remoto a la red privada institucional.
Planeación y control del Sistema de Gestión de Calidad Administrativa	Gestión de riesgos (Enfocado en el Sistema de Gestión de Calidad)

Fuente: El autor.

Como es evidente no se han formalizado procesos asociados a la seguridad informática y a la continuidad de la operación de manera puntual, pero los procesos y procedimientos establecidos dan un punto de partida para establecer los fundamentos sobre los cuales se puede iniciar todo el proceso de análisis de riesgos del sistema de información académico.

6.4 MARCO LEGAL

Norma ISO 27000: La Norma Técnica Colombiana NTC ha adoptado el conjunto de normas que componen la familia ISO 2700 para los Sistemas de Gestión de Seguridad de la Información, esta normatividad no es de obligatorio complimiento, pero es una norma certificable en Colombia.

Régimen General de Protección de Datos Personales, Ley 1518 de 2012. Protección de Datos Personales en Colombia. Es una ley de obligatorio

cumplimiento trata en términos generales de la reglamentación para el manejo y tratamiento de los datos personales.

Norma Técnica ICONTEC 5854, Accesibilidad a páginas Web.

Tabla 2. Legislación Nacional Colombiana

Delito Informático	Legislación Nacional Colombiana
Acceso no autorizado	Artículo 269A: ACCESO ABUSIVO A UN SISTEMA INFORMÁTICO. El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes
Denegación de servicio	Artículo 269B: OBSTACULIZACIÓN ILEGÍTIMA DE SISTEMA INFORMÁTICO O RED DE TELECOMUNICACIÓN. El que, sin estar facultado para ello, impida u obstaculice el funcionamiento o el acceso normal a un sistema informático, a los datos informáticos allí contenidos, o a una red de telecomunicaciones, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con una pena mayor.
Captura de datos	Artículo 269C: INTERCEPTACIÓN DE DATOS INFORMÁTICOS. El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los trasporte incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses.
Alteración de datos	Artículo 269D: DAÑO INFORMÁTICO. El que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.
Virus	Artículo 269E: USO DE SOFTWARE MALICIOSO. El que, sin estar facultado para ello, produzca, trafique, adquiera, distribuya, venda, envíe, introduzca o extraiga del territorio

Delito Informático	Legislación Nacional Colombiana
	nacional software malicioso u otros programas de computación de efectos dañinos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.
Manipulación de datos personales.	Artículo 269F: VIOLACIÓN DE DATOS PERSONALES. El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.
Sitios Web fraudulentos.	Artículo 269G: SUPLANTACIÓN DE SITIOS WEB PARA CAPTURAR DATOS PERSONALES. El que con objeto ilícito y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con pena más grave.
Fraude informático	Artículo 269I: HURTO POR MEDIOS INFORMÁTICOS Y SEMEJANTES. El que, superando medidas de seguridad informáticas, realice la conducta señalada en el artículo 239[3] manipulando un sistema informático, una red de sistema electrónico, telemático u otro medio semejante, o suplantando a un usuario ante los sistemas de autenticación y de autorización establecidos, incurrirá en las penas señaladas en el artículo 240 del Código Penal [4], es decir, penas de prisión de tres (3) a ocho (8) años.
Traslado de activos	Artículo 269J: TRANSFERENCIA NO CONSENTIDA DE ACTIVOS. El que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consiga la transferencia no consentida de cualquier activo en perjuicio de un tercero, siempre que la conducta no constituya delito sancionado con pena más grave, incurrirá en pena de prisión de cuarenta y ocho (48) a ciento veinte (120) meses y en multa de 200 a 1500 salarios mínimos legales mensuales vigentes.
Piratería informática	La Ley 44 de 1993 especifica penas entre dos y cinco años de cárcel, así como el pago de indemnizaciones por daños

Delito Informático	Legislación Nacional Colombiana
	y perjuicios, a quienes comentan el delito de piratería de software. Se considera delito el uso o reproducción de un programa de computador de manera diferente a como está estipulado en la licencia. Los programas que no tengan licencia son ilegales. Es necesaria una licencia por cada copia instalada.

Fuente: Ley de Delitos Informático en Colombia, disponible en: http://www.deltaasesores.com/articulos/autores-invitados/otros/3576-ley-de-delitos-informaticos-en-colombia

7. DISEÑO METODOLÓGICO

7.1 TIPO DE INVESTIGACIÓN

Proyecto aplicado.

En este proyecto se seleccionará una metodología para análisis de riesgos, con la cual se realizará el análisis de riesgos al sistema de información académico de la Universidad.

7.2 METODOLOGÍA DE DESARROLLO

Se utilizó la norma ISO 27001, como metodología de gestión documental.

- Sistema de gestión de seguridad de la información.
- Ciclo PHVA
- Requisitos generales.
- Establecimiento y gestión del SGSI (Alcance, Enfoque organizacional, Metodología para evaluación riesgos, Identificación de Riesgos, Evaluación de riesgos, Opciones de tratamiento de riesgos, Controles, Declaración de Aplicabilidad)
- Anexo A. Objetivos de Control y Controles

Se utilizó la norma ISO 27005, como metodología para la gestión de riesgos.

- Alcance y límites.
- Gestión del riesgo en la seguridad de la información.
- Valoración, análisis y evaluación del riesgo.
- Tratamiento del riesgo.
- Reducción, retención, evitación, transferencia o aceptación del riesgo.
- Comunicación de los riesgos.
- Monitoreo bajo la mirada del ciclo PHVA.
- Anexo B. Identificación y valoración de activos y valoración de impacto.

7.3 HIPÓTESIS

HI: Existe una metodología para realizar el diagnóstico de seguridad al sistema de información académico de la Universidad.

HO: No existe una metodología para realizar el diagnóstico de seguridad al sistema de información académico de la Universidad.

VARIABLES: Grado de nivel de seguridad actual del sistema de información académico de la Universidad.

Medidas: Optima, buena, regular, deficiente.

DIMENSIONES:

- Identificación de todos los activos que hacen parte del sistema de información académico de la Universidad.
- Auditorías al sistema de información académico de la Universidad.
- Monitoreo al hardware y software que compone el sistema de información académico de la Universidad.
- Personal capacitado en la operación del sistema de información académico de la Universidad.
- Documentación de la implementación y operación del sistema de información académico de la Universidad.

7.4 UNIVERSO O POBLACIÓN

- Áreas que hacen parte del Sistema de Información Académico de la Universidad: Mercadeo y Admisiones, Registro Académico, Secretaria General y Unidades Académicas.
- Áreas que soportan el Sistema de Información Académico de la Universidad: Tecnología Informática y Control Interno.
- Funcionarios académico administrativos que hacen parte del sistema de información académico de la Universidad.

7.5 MUESTRA O RECOLECCIÓN DE LA INFORMACIÓN

- Entrevistas directas a los directores de departamento que hacen parte del sistema de información académico de la Universidad.

- Entrevistas directas a los funcionarios académico administrativos que hacen parte del sistema de información académico de la Universidad.
- Procesos y procedimientos existentes que hacen parte del sistema de información académico de la Universidad.

8. ESQUEMA TEMÁTICO

En el presente numeral se encuentra todo el proceso elaborado para dar cumplimiento al primer objetivo de este trabajo de proyecto aplicado, en donde se realiza el levantamiento de información referente a las distintas metodologías de diagnóstico de seguridad, análisis y gestión de riesgo informático el cual está plasmado en el Marco Teórico de este documento, obteniendo los fundamentos que permiten determinar cuál es la metodología que mejor se ajusta para realizar el diagnóstico de seguridad al Sistema de Información Académico de la Universidad.

Debido a la fuente de información se realizará una investigación documental, esto debido a que en un primer momento se deben analizar las diferentes metodologías de análisis de riesgos para determinar cuál se ajusta a las necesidades del caso en específico.

Según el nivel de medición y análisis de información se realizará una investigación cualitativa ya que veremos una metodología de análisis de riesgos aplicada a un sistema de información académico.

La población se compone de los estándares y normas sobre SGSI, Análisis de Riesgos y Gestión de Riesgos.

La muestra está compuesta por: Magerit, Familia de Normas ISO 27000, Norma ISO 22301, Norma NIST 800-30, Norma ISO 31000.

Se utilizará la Técnica Documental en donde el objetivo principal es referirse a las fuentes de información que para este caso son las metodologías de análisis y gestión de riesgos y mantenerlos como instrumentos o insumos para el desarrollo de la investigación.

Se utilizará la Técnica de Campo ya que para la implementación de la metodología es necesario obtener información del sistema de información académico, lo cual se logra con la observación, el levantamiento de información mediante registros, diagramas, entrevistas, inventarios y registros.

8.1 COMPARATIVO DE LAS PRINCIPALES METODOLOGÍAS

Una vez definidos y analizados los distintos estándares se define el cuadro comparativo de las principales metodologías analizadas para la gestión de riesgos.

El cuadro se realiza teniendo como objetivo la aplicabilidad de la metodología en el diagnóstico de seguridad al Sistema de Información Académica de la Universidad.

Tabla 3. Cuadro comparativo de las principales metodologías

Nombre	Enfoque	Certificable	Material Disponible	Cumple con el Objetivo
MAGERIT	Gestión de Riesgos	NO	SI (Gratuito)	Si, ya que permite la identificación de activos y el tratamiento de riesgos de los mismos.
ISO/IEC 27000 (27001, 27002, 27005, 27035)	SGSI	SI (ISO 27001)	SI (Pago)	Si, ya que permite la identificación de activos y el tratamiento de riesgos de los mismos. Además es posible implementar un SGSI y certificar a la organización.
ISO 22301	Continuidad del negocio	SI	SI (Pago)	Sí, pero enfocado a la continuidad del negocio.
NTC-ISO-IEC (27001, 27002, 27005)	SGSI	SI	SI (Pago)	Si, ya que permite la identificación de activos y el tratamiento de riesgos de los mismos. Además, es posible implementar un SGSI y certificar a la organización. Estas normas son homologadas por la norma técnica colombiana.
NTC-ISO 31000	Gestión del riesgo, principio y directrices	SI (Nivel de auditor)	SI (Pago)	Sí, pero se enfoca exclusivamente en la gestión del riesgo.

Fuente: El autor.

Es evidente que las distintas metodologías y normas se estructuran adecuadamente, cumplen con el objetivo primordial que es determinar las vulnerabilidades y realizar el tratamiento de riesgos en la organización; para el caso puntual de la Universidad este análisis se realizará sobre el Sistema de Información Académico.

8.2 APLICACIÓN DE LAS NORMAS SELECCIONADAS

En el presente numeral se encuentra todo el proceso elaborado para dar cumplimiento al segundo objetivo de este trabajo de proyecto aplicado, en donde se determinan y aplican las metodologías de diagnóstico al Sistema de Información Académico de la Universidad.

Se utilizarán como fundamento las normas NTC-ISO-IEC (27001, 27002, 27005 y 31000), para el diagnóstico de seguridad, análisis y gestión del riesgo informático de la Universidad, esto debido a los siguientes factores que son determinantes en el momento de realizar la elección:

- La Universidad cuenta con la certificación de la norma del Sistema de Gestión de la Calidad ISO 9001:2015.
- La experiencia adquirida con la certificación ISO 9001:2015, facilita la implementación de las normas ISO ya que se cuenta con software que permite la gestión de las mismas.
- Las normas ISO-IEC (27001, 27002, 27005, 31000), son homologadas por la NTC (Norma Técnica Colombia), lo cual facilita la obtención de certificaciones en caso que la Universidad así lo decidiera.
- La documentación necesaria en cuanto a las normas NTC están disponibles para ser consultadas en las bases de datos de la Universidad, esto gracias a acuerdos preestablecidos que conllevan a la disponibilidad del material sin incurrir en gastos adicionales al proyecto.
- Las normas NTC-ISO-IEC (27001, 27002, 27005 y 31000), permiten desarrollar de manera adecuada el Diagnóstico de Seguridad al Sistema de Información Académico de la Universidad.

ISO/IEC 27001 reúne los distintos enfoques de seguridad y los presenta como estándares y buenas prácticas, en donde se pueden encontrar soluciones técnicas, físicas, administrativas e incluso legales. Este estándar define todos los requisitos para operar un SGSI (Sistema de Gestión de Seguridad de la Información), además de establecer el conjunto de controles de seguridad; con lo anterior es evidente que ISO/IEC 27001 está enfocado en los SGSI los cuales abarcan toda la organización; para el objeto de estudio de este proyecto solo se aplicara al Sistema de Información Académico de la Universidad, lo anterior no afecta la aplicabilidad de la norma ya que el sistema en cuestión, por si solo es lo suficientemente complejo como para ser objeto de análisis bajo esta norma.

Es fundamental aclarar que las normas mencionadas con anterioridad serán el fundamento para el desarrollo de este trabajo, pero no se aplicarán al pie de la letra, esto debido a que se debe buscar la articulación entre la documentación existente elaborada para el Sistema de Gestión de la Calidad implementado en la Universidad.

8.3 PROPUESTA PLAN DE TRATAMIENTO DE RIESGOS

En el presente numeral se encuentra todo el proceso elaborado para dar cumplimiento al tercer objetivo de este trabajo de proyecto aplicado, en donde se realiza el plan de trabajo a manera general para implementar las distintas metodologías seleccionadas de diagnóstico de seguridad, análisis y gestión de riesgo informático, al Sistema de Información Académico de la Universidad.

Para el Diagnóstico de Seguridad al Sistema de Información Académico de la Universidad, se tomará como base el siguiente plan de trabajo:

Tabla 4. Plan de Trabajo

Actividad	Propósito	Producto Esperado
Levantamiento de Información Inicial • Razón Social	El levantamiento de información inicial permite conocer un poco la	Documentación clara y concisa que dé respuesta y claridad

Actividad	Propósito	Producto Esperado
• Tipo de Negocio • Sector Comercial • Antecedentes de la Universidad • Organigrama de la Universidad • Organigrama del Área de Tecnología • Áreas Sensibles • Control Interno	organización de estudio, identificando el tipo de negocio y el sector comercial en el cual se desempeña, esto ayuda a enfocar el análisis de seguridad especifico priorizando los aspectos fundamentales de la organización; además facilita determinar el nivel de madurez de la organización en cuanto a la parte administrativa de la misma.	frente a la información solicitada. Esta información será parte de este proyecto y se identificará propiamente como el Levantamiento de la Información Inicial.
Identificación de Activos (Criterios de Valoración y valoración de Activos)	Identificar todos los activos que componen el Sistema de Información Académico de la Universidad	Cuadro de identificación de activos clasificado y organizado.
Identificación de Amenazas (Identificación de vulnerabilidades, criterios y valoración)	Identificar todas las amenazas y vulnerabilidades presentes en cada uno de los activos que componen el Sistema de información.	Cuadro de identificación de amenazas y vulnerabilidades por activo clasificado y organizado.
Análisis de Riesgos (Impactos, Definiciones y Valoración)	Identificar los riesgos a los que están expuestos los activos del Sistema de Información.	Cuadro de identificación de riesgos con la respectiva categorización. Análisis de impacto y probabilidad.
Identificación de Controles existentes en la organización – Riesgo residual	Identificar los controles que se han implementado o existen en la organización para obtener el estado actual de la seguridad en el Sistema de Información.	Cuadro de identificación de controles existentes por riesgo y amenaza presente.
Declaración de Aplicabilidad	Identificar los controles de la norma ISO/IEC 27002	Cuadro de controles que aplican y no aplican para el caso de estudio.

Actividad	Propósito	Producto Esperado
	que aplican para el análisis en cuestión.	
Plan de tratamiento de riesgos	Identificar los riesgos con impacto alto y establecer su tratamiento según lo establecido en la norma ISO/IEC 27005	Cuadro de declaración de tratamiento de riesgos con la aplicabilidad de controles específicos.

Fuente: El autor.

8.4 EJECUCIÓN DE LA PROPUESTA

En el presente numeral se encuentra todo el proceso elaborado para dar cumplimiento al cuarto objetivo de este trabajo de proyecto aplicado, en donde se realiza el acompañamiento en la ejecución de la propuesta del plan de trabajo enfocado al análisis de riesgos informático, al Sistema de Información Académico de la Universidad.

8.4.1 Levantamiento De Información Inicial

Razón Social: Universidad Central

Tipo de Negocio: Institución de Educación Superior

Sector Comercial: Sector Educativo

Antecedentes de la Universidad:

Reseña Histórica tomada de la página de la empresa:

UC: 49 años al servicio de la educación superior en Colombia

En una oficina del edificio Los Cerros, ubicado en el centro de Bogotá (calle 19 con carrera 4), el 30 de junio de 1966, nació la Universidad Central.

En ese lugar se reunieron ocho personajes, vinculados a la educación, el deporte y la vida cultural y política del país, con el fin de firmar el Acta de constitución de la Fundación Universidad Central. Ellos eran Alberto Gómez Moreno, Elberto Téllez Camacho, Carlos Medellín Forero, Raúl Vásquez Vélez, Eduardo Mendoza Varela, Darío Samper, Jorge Enrique Molina Mariño y Rubén Amaya Reyes, el anfitrión.

En aquel documento esbozaron los primeros derroteros de la naciente universidad. "Cuyos fines esenciales serán el servicio de la educación superior en Colombia, a nivel universitario (sic), de orientación tecnológica, de naturaleza estrictamente cultural y, por consiguiente, sin ánimo de lucro".

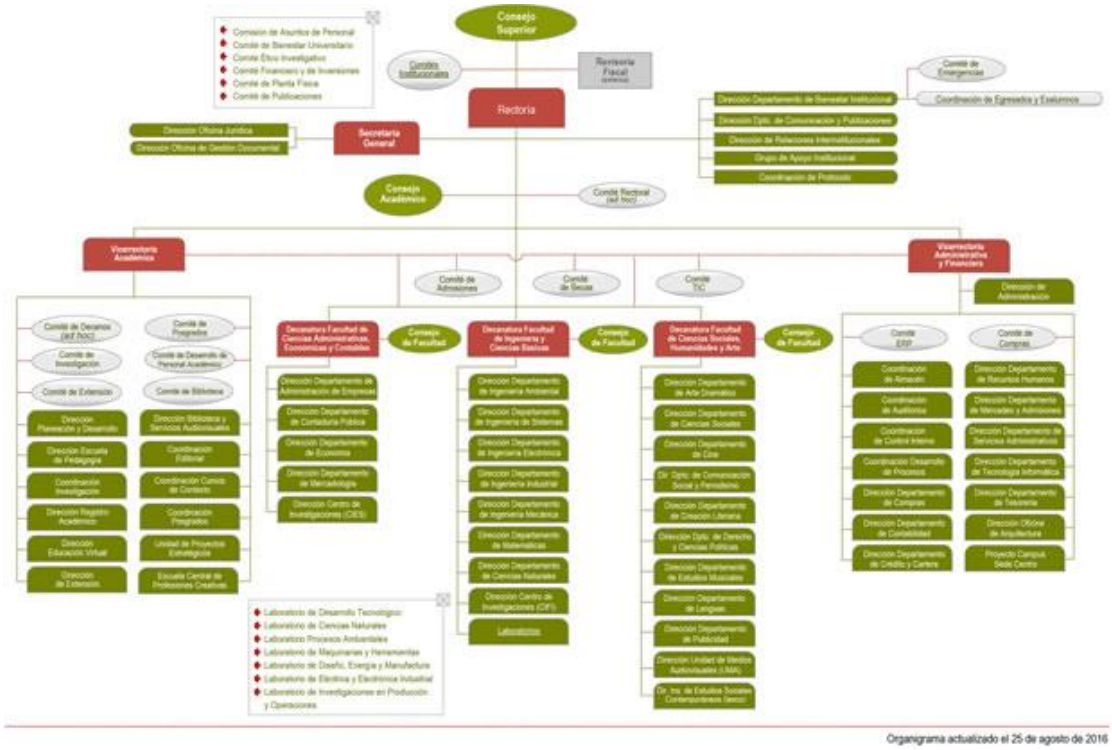
Esta nueva institución de educación superior reemplazó a la antigua Universidad Central Grancolombiano y también prolongó las actividades que esta última había desarrollado durante el primer quinquenio de la década de 1960. Como un hito importante de la recién creada institución está el grado que le fue conferido al primer egresado, el 9 de septiembre siguiente. En consecuencia, Efraín Mastrodoménico Galvis ha quedado inscrito en la historia de la Universidad Central y de la contaduría nacional; en primer lugar, por ser la primera persona graduada en el claustro unicentralista y por ser el primer contador titulado por una universidad privada en el país.

En cuanto al gobierno de la Fundación Universidad Central, quienes suscribieron el acta acordaron que la máxima autoridad académica y administrativa sería un Consejo Superior. En principio, este fue integrado por los mismos fundadores, los cuales, en la misma sesión, decidieron nombrar a Raúl Vásquez Vélez, como su presidente, y a Rubén Amaya Reyes, como vicepresidente. También designaron el rector, cargo para el cual fue escogido Carlos Medellín, y, el secretario general, cuyo nombramiento recayó en Jorge Enrique Molina Mariño. Los designados aceptaron y tomaron posesión de sus cargos ese mismo día.

El 8 de agosto siguiente, el claustro comenzó clases con tres unidades académicas: Facultad de Contaduría, con 24 alumnos matriculados; Facultad de Estudios Básicos para Ingeniería, con 12 estudiantes inscritos, y la Escuela de Publicidad y Ventas, con 22 alumnos.

Organigrama de la Universidad:

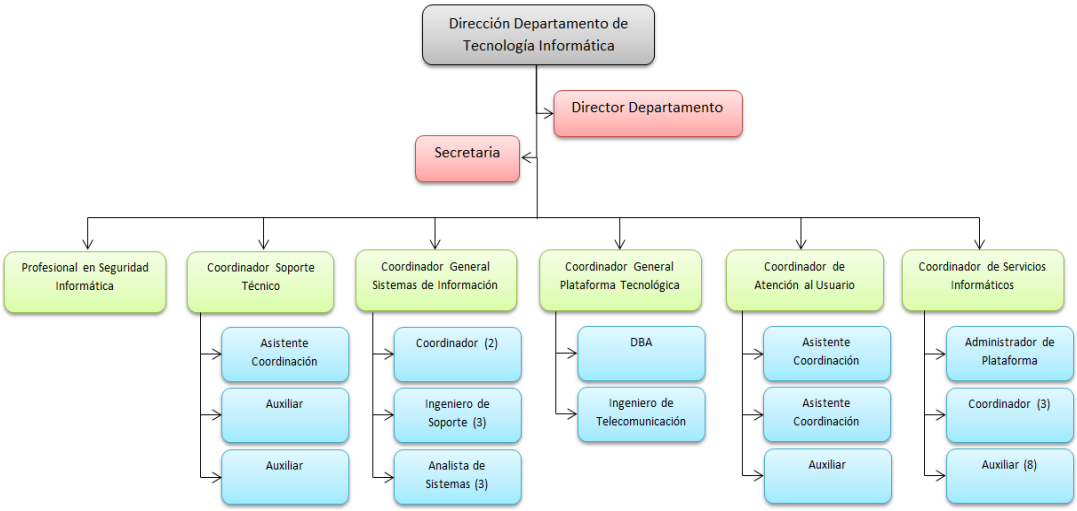
Figura 1. Organigrama Universidad



Disponible en: http://www.ucentral.edu.co/la-universidad/sobre-nosotros/organigrama

Organigrama del Área de Tecnología:

Figura 2. Organigrama DTI Universidad



Fuente: El autor

Áreas Sensibles:

Las áreas de riesgo están definidas en:

- Áreas académicas
- Áreas administrativas

Las áreas anteriores son las propietarias de los sistemas de información sensibles para la organización, ya que en ellos se maneja el modelo de negocio de la organización.

Las áreas académicas se componen de los departamentos de Crédito y Cartera, Registro Académico, Tesorería, Admisiones y Unidades Académicas. El Sistema de Información Académico de la Universidad soporta las áreas académicas.

Las áreas administrativas se componen de los departamentos de Crédito y Cartera, Tesorería, Contabilidad. El Sistema financiero ERP de la Universidad soporta las áreas administrativas.

Existen otros sistemas de información que soportan las labores de contratación y recurso humano que no son objeto de este trabajo de investigación y aplicación.

Tecnología Informática interviene como proveedor de servicio, soporte y mantenimiento de cada sistema de información.

Control Interno:

Por su naturaleza, la labor de la Coordinación de Control Interno abarca las siguientes áreas de acción generales:

- Control de la gestión global de la Universidad.
- Control de gestión del sistema académico.
- Control de gestión del sistema financiero y de la planta física.
- Control de gestión de los recursos humanos.

Misión:

La Coordinación de Control Interno es una unidad que presta asesoría en la implementación, el mantenimiento y el mejoramiento de procesos que aseguren un ambiente adecuado de control, para garantizar un mayor nivel de confianza y valor agregado a la Universidad.

http://www.ucentral.edu.co/la-universidad/vicerrectoria-administrativa-y-financiera/control-interno

Visión:

La Coordinación de Control Interno fomentará la cultura de autocontrol y se habrá consolidado, como una unidad de apoyo de la Vicerrectoría Administrativa y Financiera, en procura de un mejoramiento continuo que contribuya al logro de los objetivos institucionales.

http://www.ucentral.edu.co/la-universidad/vicerrectoria-administrativa-y-financiera/control-interno

Funciones:

- Contribuir al cumplimiento de la misión de la Universidad, informando sobre el desarrollo y mejoramiento de la gestión.
- Promover y difundir la cultura de autocontrol y calidad en la Universidad.

- Ayudar a proteger los recursos de la Universidad, buscando su adecuada administración ante posibles riesgos.
- Adelantar las coordinaciones necesarias para que todas las actividades y los recursos de la Universidad estén dirigidos al cumplimiento de sus objetivos.
- Asesorar en el diseño, la aplicación y la evaluación de los procedimientos, conjuntamente con las diferentes dependencias de la Universidad, y proponer recomendaciones para optimizar la calidad y eficacia de ellos.
- Evaluar el logro de los objetivos y metas que se hayan fijado en los planes y programas trazados por la Universidad.
- Garantizar que el sistema de control interno disponga de sus propios mecanismos de verificación y evaluación.

Objetivos:

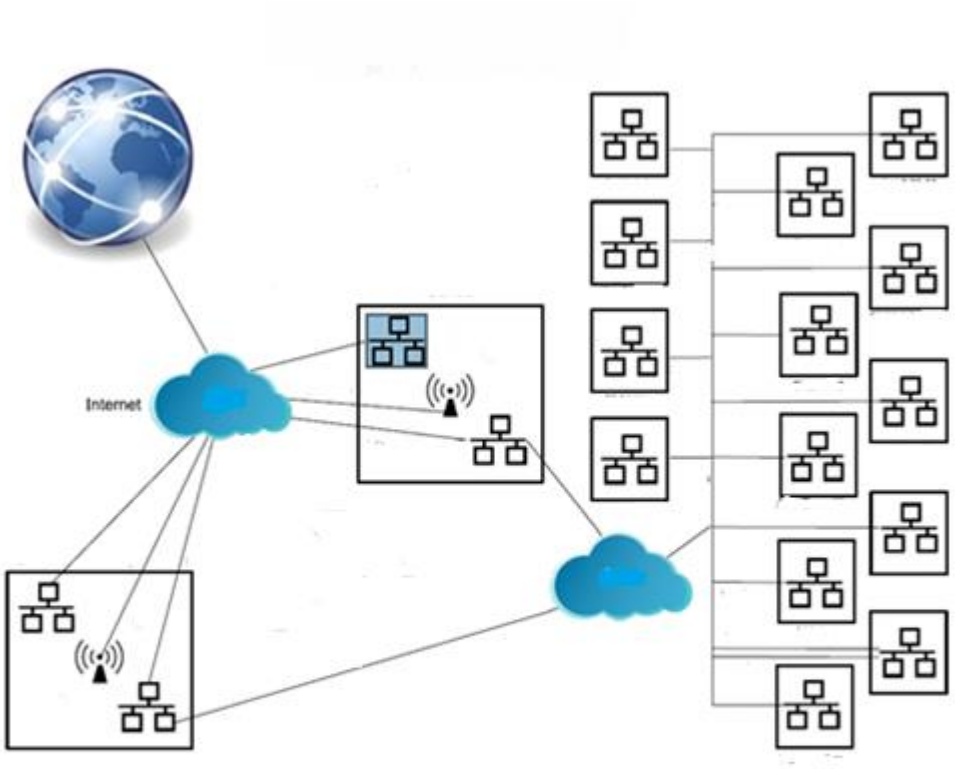
- Participar de manera proactiva en el mejoramiento de los procesos y procedimientos, con el fin de probar la efectividad de dichos controles en forma selectiva.
- Lograr una mayor participación de cada uno de los funcionarios en los procesos de mejora, inculcando una cultura del autocontrol.
- Agilizar los procesos en un entorno cambiante, maximizando la eficiencia y eficacia de la información y concentrándose en el manejo institucional, las normas éticas y el control interno continuo.
- Comunicar oportunamente las recomendaciones de control interno pertinentes cuando se detecten riesgos que puedan impedir el logro de los objetivos estratégicos.

8.4.2 Identificación De Activos

Para realizar el proceso de identificación de activos es importante dar claridad a temas esenciales como el Esquema de la Red WAN de la Universidad y la

arquitectura del Sistema de Información Académico respecto al Hardware, Software y Factor Humano que interviene en él.

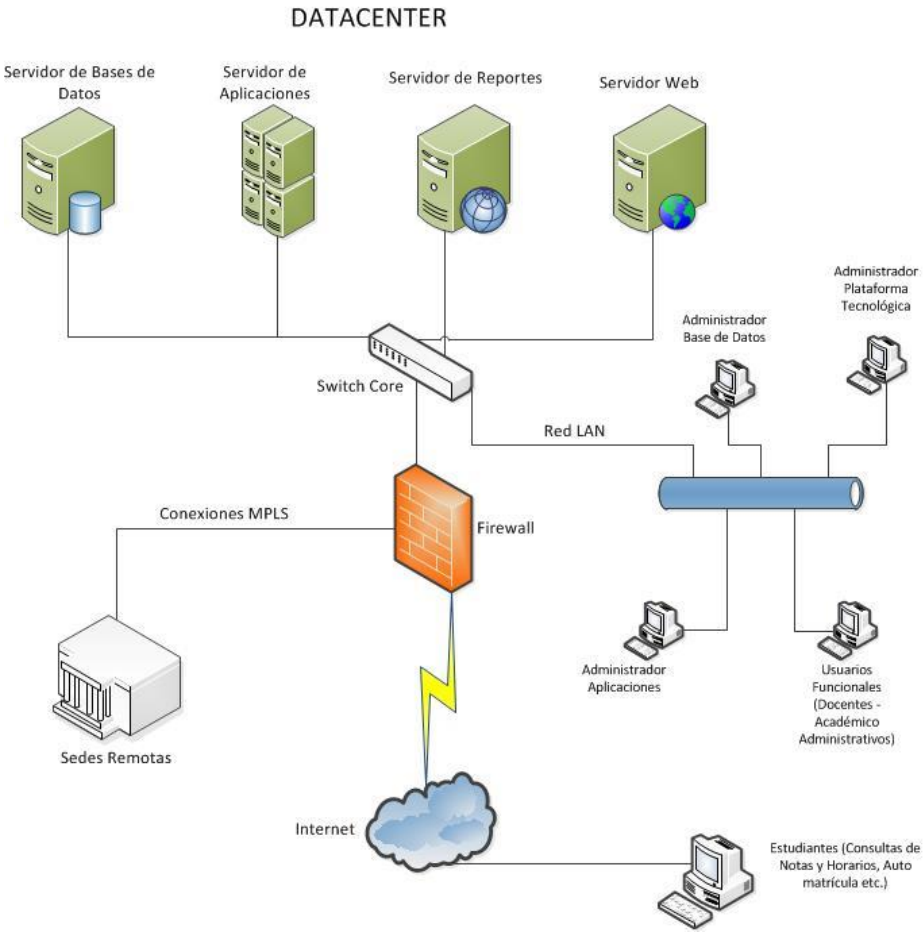
Figura 3. Esquema WAN Universidad



Fuente: El autor

En la figura anterior es evidente la interconexión que se realiza mediante MPLS de las sedes remotas con la sede principal denominada, la sede principal es primordial para este caso de estudio ya que en ella se encuentra ubicado físicamente el Centro de Datos que contiene los elementos Hardware y Software que soportan el funcionamiento del Sistema de Información Académico.

Figura 4. Arquitectura del Sistema de Información Académico



Fuente: El autor

En la figura anterior se puede evidenciar la relación de equipos servidores que soportan el sistema de información académico, la forma en que el sistema de información presta los servicios a los usuarios internos de la organización y a la comunidad estudiantil en general.

Con el Esquema de la red WAN y la Arquitectura del Sistema de Información Académica es factible realizar el proceso de identificación de activos.

Para el proceso de identificación de activos se toma como base el Anexo B (Informativo) Identificación y Valoración de los activos y valoración del Impacto – NTC-ISO/IEC 27005.

La valoración del activo se establece bajo los enfoques:

- Incapacidad de prestar el servicio
- Pérdida de credibilidad en el Sistema de Información Académico

Tabla 5. Escala de valoración de activos

Valoración de Activos (Nivel de Importancia para el Sistema)	
Alto	A (2)
Medio	M (1)
Bajo	B (0)

Fuente: El autor

Tabla 6. Identificación y Valoración de Activos

ACTIVOS			
ACTIVOS PRIMARIOS			
Tipo	**Nombre**	**Descripción**	**Valoración**
Actividades y Procesos del Negocio	Matrícula	Proceso de matrículas de estudiantes	A
	Gestión de Estudiantes	Proceso de actualización de datos, horarios y notas	A
	Gestión de Materias	Proceso de asignación de materias, intensidad horaria y docentes	M
	Gestión Docente	Proceso de Cargue de notas	A
	Gestión de Aulas	Proceso de selección de espacios físicos y laboratorios para desarrollo de asignaturas	M
	Cierre Académico	Proceso de periodo de cierre académico	A
Información	DB Académico	Base de Datos de Historias Académicas	A
	DB Estudiantes	Base de Datos de Estudiantes	A
	DB Docentes	Base de Datos de Docentes	M
	Planes de Estudio	Archivos de información de planes de estudio Académicos	M
ACTIVOS DE SOPORTE			
Hardware	Servidor DB	Servidor de Base de Datos que soporta las bases de	A

ACTIVOS			
		datos manejadas en la Universidad	
	Servidor Aplicaciones	Servidor que soporta las aplicaciones del Sistema de Información Académico	A
	Servidor de Reportes	Servidor que almacena los reportes académicos propios de las consultas de estudiantes y reportes en general	A
	Servidor Web	Servidor que soporta el Portal Institucional que da acceso a la gestión de estudiantes y gestión docente	A
	Estación de trabajo	Computadores de escritorio marca Dell de última generación (1500 en la intranet)	B
	Estación de trabajo portable	Computadores portátiles marca Dell de última generación (200 en la intranet)	B
	Estación de trabajo externa	Computadores de cualquier tipo usados por los estudiantes para la gestión desde internet	B
	Impresoras	Impresoras láser marca HP para impresión de recibos de pago y constancias de estudio	M
	DVD – DL	Discos magnéticos en formato DVD DL para la generación de copias de seguridad de las bases de datos	M
Software	Windows Server 2008	Sistema Operativo base de Servidor	M
	Windows Server 2012	Sistema Operativo base de Servidor	A
	Linux Red Hat Enterprise	Sistema Operativo base de Servidor	A
	Windows 10 profesional	Sistema Operativo Base estación de trabajo	B

ACTIVOS			
	SQL Server	Software Gestor de Bases de Datos	A
	Oracle	Software Gestor de Bases de Datos	A
	Joomla	Sistema de Gestión de Contenidos portal Web	M
	Universitas XXI	Software Académico	A
	GII	Software Apoyo Académico	M
Redes	Red LAN	Red interna de la Universidad	M
	Red MAN	Red extendida de la Universidad	M
	Switches Core	Conmutador de comunicación principal	A
	Switches de Zona	Conmutador de comunicación secundario	M
	Router	Enrutador de conexión a internet	A
	Firewall	Corta fuegos	M
	MPLS	Conexiones seguras de intercomunicación entre zonas	M
Personal	Vicerrectoría Académica	Alta dirección del proceso Académico	B
	Registro Académico	Departamento dueño del proceso Académico	M
	Directores Académicos	Operadores del proceso Académico	B
	Docentes	Operadores del proceso Académico	M
	Coordinador de Plataforma	Propietario de la gestión de plataforma tecnológica	A
	DBA	Administrador de Base de Datos	A
	Administrador Aplicaciones	Soporte técnico a las aplicaciones	M
	Estudiantes	Usuarios finales de la aplicación	B
	Profesional de Seguridad	Auditoría y gestión de seguridad del proceso académico	M
Ubicación	Sede Principal	Sede principal de la Universidad	A

ACTIVOS			
	Sede Secundaria	Sede secundaria de la Universidad	B
	Sede alterna	Sede alterna de la Universidad	B
	Sedes aledañas	Sedes aledañas de servicios secundarios	B
	DataCenter	Centro de datos donde se almacenan los servidores	A
	Planta Eléctrica	Planta de Energía Eléctrica para la sede principal y Secundarias	A
	UPS	Sistema de Alimentación Ininterrumpida para todas las sedes	A
	Planta Telefónica	Planta telefónica mixta (Análoga y Digital)	M
Estructura de la Organización	Vice Académica	Vicerrectoría Académica	B
	Vice Administrativa	Vicerrectoría Administrativa	B
	Tecnología Informática	Departamento de Tecnología Informática	A
	Recursos Humanos	Departamento de Recursos Humanos	B
	Registro Académico	Departamento de Registro Académico	M
	Crédito y Cartera	Departamento de Crédito y Cartera	B
	Tesorería	Departamento de Tesorería	B
	Admisiones	Departamento de Admisiones	M
	Control Interno	Departamento de Control Interno	B

Fuente: El autor

8.4.3 Identificación De Amenazas

En la siguiente tabla se pueden evidenciar los tipos de amenazas que se pueden presentar en la Universidad, estas se clasifican según el origen que puede ser D (Deliberadas), A (Accidentales) y E (Ambientales).

Se basa en la Norma NTC-ISO/IEC 27005. Para este análisis.

Tabla 7. Identificación de Amenazas en la Universidad

Tipo	Amenazas	Origen
Daño Físico	Fuego	D, A, E
	Daño por Agua	D, A, E
	Contaminación	D, A, E
	Accidente Importante	D, A, E
	Destrucción del Equipo o los medios	D, A, E
	Polvo, Corrosión, Congelamiento	D, A, E
Eventos Naturales	Fenómenos Climáticos	E
	Fenómenos Sísmicos	E
	Inundación	E
Pérdida de los servicios esenciales	Falla en el Sistema de Aire Acondicionado	D, A
	Pérdida de Suministro de Energía	D, A, E
	Falla en el equipo de Telecomunicaciones	D, A, E
Perturbación debida a la radiación	Radiación Electromagnética	D, A, E
	Radiación Térmica	D, A, E
	Impulsos Electromagnéticos	D, A, E
Compromiso de la Información	Espionaje Remoto	D
	Escucha Encubierta	D
	Hurto de Medios o Documentos	D
	Hurto de Equipo	D
	Recuperación de Medios reciclados o desechados	D
	Divulgación	D
	Datos provenientes de fuentes no confiables	D
	Manipulación con Software	D, A
Fallas Técnicas	Falla del Equipo	A
	Mal funcionamiento del equipo	A
	Saturación del sistema de información	D, A
	Mal funcionamiento del software	A
	Incumplimiento en el mantenimiento del Sistema	D, A
Acciones no Autorizadas	Uso no autorizado del equipo	D
	Uso de software Falso	D
	Corrupción de los Datos	D

Tipo	Amenazas	Origen
	Procesamiento ilegal de los datos	D
Compromiso de las funciones	Error en el uso	A
	Abuso de derechos	D, A
	Falsificación de Derechos	D
	Negación de Acciones	D
	Incumplimiento en la disponibilidad de personal	D, A, E

Fuente: El autor

En la siguiente tabla es posible observar las diferentes vulnerabilidades presentes en los activos detectados en la Universidad específicamente del Sistema de Información Académico, además se adicionan las amenazas que se pueden explotar por dichas vulnerabilidades.

Tabla 8. Identificación de Vulnerabilidades en la Universidad

Tipos de Activos	Vulnerabilidades	Amenazas
Actividades y Procesos del Negocio	Ausencia de auditorías al Sistema de Gestión	Corrupción de los Datos
	Ausencia de monitoreo de recursos del Sistema	Saturación del sistema de información
	Ausencia de plan de capacitación sobre el uso del Sistema	Error en el uso
	Ausencia del proceso de supervisión de los derechos de acceso	Abuso de derechos
	Ausencia del proceso de supervisión de accesos al sistema	Falsificación de Derechos
	Ausencia del proceso de parametrización de usuarios	Negación de Acciones
	Ausencia del proceso de entrega de cargo pos ausencia	Incumplimiento en la disponibilidad de personal
Información	Ausencia del proceso de monitoreo de acceso a la red	Espionaje Remoto
	Ausencia del proceso de encriptación de datos	Escucha Encubierta
	Ausencia del proceso de custodia de medios y documentos	Hurto de Medios o Documentos
	Ausencia de controles de acceso a al DataCenter	Hurto de Equipo
	Ausencia del proceso de destrucción de medios	Recuperación de Medios reciclados o desechados

Tipos de Activos	Vulnerabilidades	Amenazas
	Ausencia del proceso de manejo seguro de la información	Divulgación
	Ausencia de controles de verificación de datos	Datos provenientes de fuentes no confiables
	Ausencia de políticas de instalación de software en la red interna	Manipulación con Software
	Ausencia de auditoría sobre las bases de datos	Corrupción de los Datos
	Ausencia de políticas de manipulación de datos	Procesamiento ilegal de los datos
	Ausencia de procedimiento de capacitación de uso del sistema	Error en el uso
	Ausencia del proceso de supervisión de los derechos de acceso	Abuso de derechos
Hardware	Ausencia de sistema de extinción de incendios	Daño por Fuego
	Ausencia de controles de humedad	Daño por Agua
	Ausencia de sistemas de purificación de aire	Contaminación
	Ausencia de protocolos de señalización	Accidente Importante
	Ausencia de programa de garantía extendida	Destrucción del Equipo o los medios
	Ausencia de proceso de mantenimiento preventivo	Polvo, Corrosión, Congelamiento
	Ausencia de pólizas de seguro	Hurto de Equipo
Software	Ausencia de proceso de actualización de software	Mal funcionamiento del equipo
	Ausencia de proceso de mantenimiento preventivo	Incumplimiento en el mantenimiento del Sistema
	Ausencia de control de instalación software	Mal funcionamiento del software
	Ausencia de control de versión de software	Mal funcionamiento del equipo
	Ausencia de protocolo de pruebas de software	Mal funcionamiento del software
	Ausencia de controles de acceso a las aplicaciones	Corrupción de los Datos
	Ausencia de protocolo de manejo de aplicaciones	Procesamiento ilegal de los datos
	Ausencia de documentación	Error en el uso

Tipos de Activos	Vulnerabilidades	Amenazas
Redes	Líneas de comunicación sin protección	Escucha encubierta
	Tráfico sensible sin protección	Escucha encubierta
	Conexiones deficientes en los cables	Falla en el equipo de Telecomunicaciones
	Arquitectura insegura de red	Espionaje remoto
	Transferencia de contraseñas en claro	Espionaje remoto
	Gestión inadecuada de la red	Saturación del sistema de información
	Conexiones de red pública sin protección	Uso no autorizado del equipo
	Centros de datos secundarios sin seguridad	Accidente Importante
Personal	Ausencia de personal	Incumplimiento en la disponibilidad de personal
	Procedimientos inadecuados de contratación	Destrucción de equipos o medios
	Entrenamiento insuficiente	Error en el uso
	Uso incorrecto de software o hardware	Error en el uso
	Falta de conciencia acerca de seguridad	Error en el uso
	Trabajo no supervisado del personal externo o limpieza	Hurto de medios o documentos
	Ausencia de políticas para el uso correcto de los medios de telecomunicaciones y mensajería	Uso no autorizado del equipo
Ubicación	Falta de control de acceso físico a las edificaciones	Destrucción de equipos o medios
	Ubicación en área susceptible a inundación	Inundación
	Red energética inestable	Pérdida del suministro de energía
	Ausencia de protección física a las edificaciones	Hurto de equipo
Estructura de la Organización	Ausencia de auditorías regulares	Abuso de derechos
	Ausencia de procedimientos de identificación y tratamiento de riesgos	Abuso de derechos
	Ausencia de procedimientos de control de cambios	Incumplimiento en el mantenimiento del sistema

Tipos de Activos	Vulnerabilidades	Amenazas
	Ausencia del proceso de SGSI	Corrupción de datos
	Ausencia de planes de continuidad	Falla del equipo
	Ausencia de políticas de seguridad de la información	Hurto de equipo
	Ausencia de procesos de manejo de información clasificada	Error en el uso

Fuente: El autor

8.4.4 Análisis De Riesgos

Para el análisis de riesgos es necesario precisar las escalas de valoración expuestas en las tablas siguientes.

Se basa en la norma NTC-ISO/IEC 27005. Para este análisis.

Tabla 9. Nivel de probabilidad

Nivel	Probabilidad	Descriptor	
		Ocurrencia	Frecuencia
1	Raro	El evento puede ocurrir en circunstancias excepcionales	No ha ocurrido en los últimos 5 años
2	Improbable	Que es difícil o poco posible que suceda	Al menos una vez en los últimos 5 años
3	Posible	El evento puede ocurrir en algún momento	Al menos una vez en los últimos 2 años
4	Probable	El evento probablemente ocurrirá en la mayoría de las circunstancias	Al menos una vez en el último año
5	Casi seguro	Se espera que el evento ocurra en la mayoría de las circunstancias	Más de una vez al año

Fuente: El autor.

Tabla 10. Nivel de impacto

Nivel	Impacto	Descriptor			
		Magnitud del Impacto	Pérdida Sobre		
			Integridad	Disponibilidad	Confidencialidad
1	Muy bajo	Si el hecho llegara a presentarse, tendría consecuencias o efectos mínimos sobre la institución	0 % datos alterados	1 hora sin servicio	Comunicados institucionales
2	Bajo	Si el hecho llegara a presentarse, tendría bajo efecto o impacto sobre la institución	5 % datos alterados	4 horas sin servicio	Información de acreditación
3	Moderado	Si el hecho llegara a presentarse, tendría medianas consecuencias sobre la institución	10 % datos alterados	8 horas sin servicio	Información de programas académicos
4	Alto	Si el hecho llegara a presentarse, tendría altas consecuencias sobre la institución	15 % datos alterados	12 horas sin servicio	Datos de carácter personal
5	Muy alto	Si el hecho llegara a presentarse, tendría desastrosas consecuencia	20 % o más datos alterados	24 horas o más sin servicio	Datos de historias académicas

Nivel	Impacto	Descriptor			
		Magnitud del Impacto	Pérdida Sobre		
			Integridad	Disponibilidad	Confidencialidad
		s sobre la institución			

Fuente: El autor.

El nivel de Riesgo es la magnitud de un riesgo o de una combinación de riesgos, expresada en términos de la combinación del impacto y su probabilidad de ocurrencia.

El nivel de Riesgo = Nivel de Probabilidad * Nivel de Impacto

La etapa de evaluación del riesgo, corresponde a la comparación de los resultados del análisis del riesgo con los criterios de riesgo establecidos, con el fin de determinar si el riesgo y su magnitud son aceptables o no y decidir acerca del tratamiento y controles que deberán implementarse.

Los criterios de riesgo establecidos para la Universidad son los siguientes:

Alto – Inaceptable	Todos los riegos con un nivel igual o superior a 10 requieren atención inmediata, pues deben ser mitigados, requieren documentar acción correctiva.
Moderado	Todos los riesgos con un nivel >= 5 y < 10 se deben gestionar mediante procedimientos de monitoreo, requiere documentar acción preventiva.
Bajo – Inaceptable	Todos los riesgosa con un nivel = 1 y < 5 se catalogan como aceptables, estos riesgos deben monitorearse, pero es probable que no requieran la implementación de acciones específicas.

Esta evaluación se reflejará en la siguiente matriz:

Tabla 11. Matriz de Riesgo Inherente

	PROBABILIDAD					
5	CASI SEGURO	5	10	15	20	25
4	PROBABLE	4	8	12	16	20
3	POSIBLE	3	6	9	12	15
2	IMPROBABLE	2	4	6	8	10
1	RARO	1	2	3	4	5
	IMPACTO	Muy bajo	Bajo	Moderado	Alto	Muy alto
		1	2	3	4	5

Fuente: El autor.

La siguiente tabla expone el nivel de riesgo por cada amenaza presente partiendo de la probabilidad y el impacto. Se basa en la Tabla 9. Identificación de Vulnerabilidades en la Universidad.

Tabla 12. Análisis de Riesgos

ANÁLISIS DE RIESGOS			
AMENAZA	**PROBABILIDAD**	**IMPACTO**	**RIESGO**
ACTIVIDADES Y PROCESOS DEL NEGOCIO			
Corrupción de los Datos	2	5	10
Saturación del sistema de información	4	5	20
Error en el uso	5	5	25
Abuso de derechos	1	5	5
Falsificación de Derechos	1	5	5
Negación de Acciones	1	5	5
Incumplimiento en la disponibilidad de personal	4	5	20
INFORMACIÓN			
Espionaje Remoto	1	3	3
Escucha Encubierta	1	3	3
Hurto de Medios o Documentos	1	3	3
Hurto de Equipo	1	5	5
Recuperación de Medios reciclados o desechados	1	3	3
Divulgación	3	2	6
Datos provenientes de fuentes no confiables	1	5	5
Manipulación con Software	1	4	4
Corrupción de los Datos	1	5	5
Procesamiento ilegal de los datos	1	5	5

ANÁLISIS DE RIESGOS			
AMENAZA	**PROBABILIDAD**	**IMPACTO**	**RIESGO**
Error en el uso	4	5	20
Abuso de derechos	3	3	9
HARDWARE			
Daño por Fuego	1	5	5
Daño por Agua	1	5	5
Contaminación	1	5	5
Accidente Importante	3	5	15
Destrucción del Equipo o los medios	1	5	5
Polvo, Corrosión, Congelamiento	3	5	15
Hurto de Equipo	2	5	10
SOFTWARE			
Mal funcionamiento del equipo	3	5	15
Incumplimiento en el mantenimiento del Sistema	3	5	15
Mal funcionamiento del software	5	5	25
Mal funcionamiento del equipo	3	3	9
Mal funcionamiento del software	3	5	15
Corrupción de los Datos	3	3	9
Procesamiento ilegal de los datos	3	3	9
Error en el uso	3	5	15
REDES			
Escucha encubierta	1	3	3
Escucha encubierta	1	3	3
Falla en el equipo de Telecomunicaciones	3	5	15
Espionaje remoto	1	5	5
Espionaje remoto	1	5	5
Saturación del sistema de información	3	3	9
Uso no autorizado del equipo	3	5	15
Accidente Importante	1	5	5
PERSONAL			
Incumplimiento en la disponibilidad de personal	3	1	3
Destrucción de equipos o medios	1	5	5
Error en el uso	3	5	15
Error en el uso	1	3	3
Error en el uso	3	3	9
Hurto de medios o documentos	1	1	1
Uso no autorizado del equipo	1	1	1
UBICACIÓN			
Destrucción de equipos o medios	2	5	10

ANÁLISIS DE RIESGOS			
AMENAZA	**PROBABILIDAD**	**IMPACTO**	**RIESGO**
Inundación	1	5	5
Pérdida del suministro de energía	5	5	25
Hurto de equipo	1	5	5
ESTRUCTURA DE LA ORGANIZACIÓN			
Abuso de derechos	1	3	3
Abuso de derechos	3	3	9
Incumplimiento en el mantenimiento del sistema	3	1	3
Corrupción de datos	1	5	5
Falla del equipo	1	5	5
Hurto de equipo	1	5	5
Error en el uso	3	3	9

Fuente: El autor

En la tabla anterior es posible evidenciar los riesgos que más repercuten en la Universidad, los cuales tiene el puntaje más alto de acuerdo a la tabla de niveles de riesgo.

8.4.5 Identificación De Controles Existentes En La Organización

La Universidad en el proceso de implementación del Sistema de Calidad ISO 9001, ha desarrollado diferentes procesos, procedimientos, instructivos y mecanismos que abarcan el tratamiento de las distintas amenazas existentes, por lo cual este proceso da un verdadero vistazo al estado actual del Sistema de Información Académico frente a su seguridad.

Se hace uso de la tabla No. 12 (Tabla de valoración del riesgo), para definir la nomenclatura y la valoración del riesgo y el riesgo residual.

Tabla 13. Estado Actual del Sistema de Información Académico de la U

CONTROLES EXISTENTES			
AMENAZA	**RIESGO**	**CONTROL IMLPEMENTADO**	**RIESGO RESIDUAL**
ACTIVIDADES Y PROCESOS DEL NEGOCIO			
Corrupción de los Datos	10	N.A	10

CONTROLES EXISTENTES			
AMENAZA	**RIESGO**	**CONTROL IMLPEMENTADO**	**RIESGO RESIDUAL**
Saturación del sistema de información	20	Monitoreo con NAGIOS (sin documentar)	10
Error en el uso	25	Procedimiento AD-20-P-06 Inducción (Capacitación inicial a funcionarios sobre el sistemas de información)	3
Abuso de derechos	5	N.A	5
Falsificación de Derechos	5	N.A	5
Negación de Acciones	5	Procedimiento AD-27-P-01 Administración de Usuarios en Aplicativos Institucionales y Servicios Básicos de Red	3
Incumplimiento en la disponibilidad de personal	20	Instructivo de Entrega de Cargo por Suplencia (Instructivo documentado pero sin aprobar)	10
INFORMACIÓN			
Espionaje Remoto	3	N.A.	3
Escucha Encubierta	3	N.A.	3
Hurto de Medios o Documentos	3	Instructivos AD-13-I-01 Entrega de Copias de Respaldo a Custodia Externa	1
Hurto de Equipo	5	Instructivo AD-14-I-010 Acceso a Granja de Servidores	3
Recuperación de Medios reciclados o desechados	3	N.A.	3
Divulgación	6	N.A.	6
Datos provenientes de fuentes no confiables	5	Parametrización en las aplicaciones (Sin Documentar)	4
Manipulación con Software	4	Instructivo AD-14-I-002 Acondicionamiento de equipo a nuevo usuario	3
Corrupción de los Datos	5	Auditoría Anual Externa firma Deloitte (Sin documentar)	3
Procesamiento ilegal de los datos	5	N.A.	5

CONTROLES EXISTENTES			
AMENAZA	**RIESGO**	**CONTROL IMLPEMENTADO**	**RIESGO RESIDUAL**
Error en el uso	20	Procedimiento AD-20-P-06 Inducción (Capacitación inicial a funcionarios sobre el sistemas de información)	9
Abuso de derechos	9	Procedimiento AD-27-P-01 Administración de Usuarios en Aplicativos Institucionales y Servicios Básicos de Red	3
HARDWARE			
Daño por Fuego	5	Sistema de Extinción de Incendios (Sin documentar)	3
Daño por Agua	5	Aplicación de normativa de aislamiento de ductos de agua (Sin documentar)	3
Contaminación	5	Sistema de aire acondicionado (Sin documentar)	3
Accidente Importante	15	N.A.	15
Destrucción del Equipo o los medios	5	Instructivo AD-14-I-009 Trámite de garantías relacionadas con equipos de computo	3
Polvo, Corrosión, Congelamiento	15	Instructivo AD-14-I-008 Mantenimiento preventivo de equipos de Cómputo	3
Hurto de Equipo	10	Procedimiento AD-34-P-007 Reclamación de Seguros Patrimoniales	3
SOFTWARE			
Mal funcionamiento del equipo	15	Procedimiento AD-19-P-003 Soporte y Mantenimiento de Software	9
Incumplimiento en el mantenimiento del Sistema	15	Procedimiento AD-19-P-003 Soporte y Mantenimiento de Software	9

CONTROLES EXISTENTES			
AMENAZA	**RIESGO**	**CONTROL IMLPEMENTADO**	**RIESGO RESIDUAL**
Mal funcionamiento del software	25	Instructivo AD-14-I-003 Revisión de Equipo de Cómputo	9
Mal funcionamiento del equipo	9	Procedimiento AD-19-P-008 Desarrollo de Software	3
Mal funcionamiento del software	15	Procedimiento AD-19-P-008 Desarrollo de Software	9
Corrupción de los Datos	9	Procedimiento AD-27-P-01 Administración de Usuarios en Aplicativos Institucionales y Servicios Básicos de Red	3
Procesamiento ilegal de los datos	9	Procedimiento AD-20-P-06 Inducción (Capacitación inicial a funcionarios sobre el sistemas de información)	3
Error en el uso	15	N.A.	15
REDES			
Escucha encubierta	3	N.A.	3
Escucha encubierta	3	N.A.	3
Falla en el equipo de Telecomunicaciones	15	N.A.	15
Espionaje remoto	5	Instructivo AD-14-I-006 Supervisión de Centros de Cableado	3
Espionaje remoto	5	N.A.	3
Saturación del sistema de información	9	Monitoreo con NAGIOS (sin documentar)	9
Uso no autorizado del equipo	15	Procedimiento AD-27-P-005 Gestión de Acceso a la Red privada institucional	9
Accidente Importante	5	Instructivo AD-14-I-006 Supervisión de Centros de Cableado	3
PERSONAL			
Incumplimiento en la disponibilidad de personal	3	Instructivo de Entrega de Cargo por Suplencia (Instructivo documentado pero sin aprobar)	3
Destrucción de equipos o medios	5	Procedimiento AD-20-P-002 Vinculación de	3

CONTROLES EXISTENTES			
AMENAZA	**RIESGO**	**CONTROL IMLPEMENTADO**	**RIESGO RESIDUAL**
		Personal de medio tiempo y tiempo completo.	
Error en el uso	15	Procedimiento AD-20-P-06 Inducción (Capacitación inicial a funcionarios sobre el sistemas de información)	9
Error en el uso	3	Procedimiento AD-20-P-06 Inducción (Capacitación inicial a funcionarios sobre el sistemas de información)	1
Error en el uso	9	N.A.	9
Hurto de medios o documentos	1	Procedimiento AD-23-P-001 Investigaciones Disciplinarias	1
Uso no autorizado del equipo	1	Políticas de Seguridad y Gobierno de Datos (Sin aprobar)	1
UBICACIÓN			
Destrucción de equipos o medios	10	Procedimiento AD-16-P-008 Control sobre el ingreso o salida de activos y otros elementos	9
Inundación	5	N.A.	5
Pérdida del suministro de energía	25	Planta Eléctrica Propia (Sin documentar)	15
Hurto de equipo	5	Control de acceso con seguridad de vigilancia privada (Sin Documentar)	3
ESTRUCTURA DE LA ORGANIZACIÓN			
Abuso de derechos	3	Auditoría Anual Externa firma Deloitte (Sin documentar)	3
Abuso de derechos	9	N.A.	9
Incumplimiento en el mantenimiento del sistema	3	N.A.	3
Corrupción de datos	5	N.A.	5
Falla del equipo	5	Existen por separado (Sin documentar)	5
Hurto de equipo	5	Políticas de Seguridad de la Información (Sin Documentar)	5

CONTROLES EXISTENTES			
AMENAZA	**RIESGO**	**CONTROL IMLPEMENTADO**	**RIESGO RESIDUAL**
Error en el uso	9	N.A.	9

Fuente: El autor

En la tabla anterior es evidente que existen muchos controles implementador, pero muchos de ellos no se han documentado de la manera adecuada o no están aprobados; para el análisis del riesgos residual se parte del hecho que si no existe ningún control el riesgo se mantiene, si existe un control aprobado y documentado el riesgo disminuye al nivel anterior (ejemplo de riesgo Alto a riesgo Medio), ya que debe verificarse la existencia de indicadores que den cumplimiento al control implementado; si existe un control pero este no está documentado el nivel de riesgo disminuye su valor y en algunos casos el suficiente como para cambiar el nivel de criticidad.

Los criterios de riesgo establecidos para la Universidad, una vez calculado el riesgo residual, son los siguientes:

Tabla 14. Criterios de riesgo

Nivel de Exposición del Riesgo	Opción del Tratamiento	Acciones a Tomar
ALTO - INACEPTABLE (Riesgos con calificación igual o superior a 10)	Evitar Reducir Transferir Compartir	Se deberá implementar inmediatamente las acciones para abordar riesgos que conlleven a evitar, reducir, transferir o compartir el riesgo. Las acciones para abordar riesgos deberán conllevar a implementar nuevos controles que prevengan la materialización del riesgo y a mitigar el impacto. Se debe implementar el plan de contingencia frente a estos riesgos.
MODERADO (Riesgos con calificación entre 5 y 9)	Reducir Transferir Compartir	Se deberá implementar acciones para abordar riesgos que conlleven a reducir, transferir o compartir el riesgo. Se deberá implementar acciones para abordar riesgos que conlleven a mejorar o documentar los controles existentes. La implementación de un plan de contingencia estará sujeto a las necesidades del usuario de Sistema de Información Académico.

BAJO – ACEPTABLE (Riesgos con calificación inferior o igual a 4)	Asumir	Se debe realizar seguimiento a los riesgos con el fin de verificar su impacto, probabilidad y la valoración de los controles.

Fuente: El autor

8.4.6 Declaración De Aplicabilidad

El objeto de alcance de este proyecto está enfocado a los riesgos con nivel Alto presentes en el Sistema de Información Académico de la Universidad, por este motivo, de la Tabla 14. Estado Actual del Sistema de Información Académico de la U, se extraen las amenazas que tiene un nivel alto en el Riesgo Residual y de esta manera determinar los objetivos de control dispuestos en el Anexo A de la norma NTC-ISO-IEC 27001.

Se hace uso de la tabla No. 12 (Tabla de valoración del riesgo), para definir la nomenclatura y la valoración del riesgo residual.

Tabla 15. Declaración de aplicabilidad Norma ISO 27001 Anexo A

CONTROLES DE REFERENCIA			
AMENAZA	**CONTROL IMPLEMENTADO**	**RIESGO RESIDUAL**	**CONTROLES DE REFERENCIA**
ACTIVIDADES Y PROCESOS DEL NEGOCIO			
Corrupción de los Datos	N.A.	10	A.18.2.3 Revisión del cumplimiento técnico. Control: Los sistemas de información se deben revisar periódicamente para determinar el cumplimiento de las políticas y normas de seguridad de la información.
Saturación del sistema de información	Monitoreo con NAGIOS (sin documentar)	10	A.12.1.1 Procedimientos de

CONTROLES DE REFERENCIA			
AMENAZA	**CONTROL IMPLEMENTADO**	**RIESGO RESIDUAL**	**CONTROLES DE REFERENCIA**
ACTIVIDADES Y PROCESOS DEL NEGOCIO			
			operación documentados. Control: Los procedimientos de operación se deben documentar y poner a disposición de todos los usuarios que lo necesitan.
Incumplimiento en la disponibilidad de personal	Instructivo de Entrega de Cargo por Suplencia (Instructivo documentado pero sin aprobar)	10	A.7.2.1 Responsabilidades de la dirección. Control: La dirección debe exigir a todos los empleados y contratistas la aplicación de la seguridad de la información de acuerdo con las políticas y procedimientos establecidos por la organización.
HARDWARE			
Accidente Importante	N.A.	15	A.11.1.5 Trabajo en áreas seguras. Control: Se deben diseñar y aplicar procedimientos para trabajo en áreas seguras.
SOFTWARE			
Error en el uso	N.A.	15	A.14.2.5 Principios de construcción de los sistemas seguros. Control: Se deben establecer, documentar y mantener principios para la construcción de

CONTROLES DE REFERENCIA			
AMENAZA	**CONTROL IMPLEMENTADO**	**RIESGO RESIDUAL**	**CONTROLES DE REFERENCIA**
ACTIVIDADES Y PROCESOS DEL NEGOCIO			
			sistemas seguros, y aplicarlos a cualquier actividad de implementación de sistemas de información.
REDES			
Falla en el equipo de Telecomunicaciones	N.A.	15	A.13.1.1. Controles de redes. Control: Las redes se deben gestionar y controlar para proteger la información en sistemas y aplicaciones.
UBICACIÓN			
Pérdida del suministro de energía	Planta Eléctrica Propia (Sin documentar)	15	A.11.2.2 Servicios de suministros. Control: Los equipos se deben proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministros.

Fuente: El autor

8.4.7 Plan De Tratamiento De Riesgos

Para las amenazas presentes con nivel de riesgo alto, se realizarán tareas propias para la reducción del riesgo.

Estas tareas se realizarán bajo el modelo de mejora continua, obteniendo el siguiente resultado para cada amenaza.

Tabla 16. Plan de tratamiento de riesgos

PLAN DE TRATAMIENTO DE RIESGO 1	
Tipo de Activo	Actividades y procesos del negocio
Vulnerabilidad	Ausencia de auditorías al Sistema de Gestión
Amenaza	Corrupción de los Datos
Riesgo	Alto
Control de referencia ISO 27001 Anexo A	A.18.2.3 Revisión del cumplimiento técnico. Control: Los sistemas de información se deben revisar periódicamente para determinar el cumplimiento de las políticas y normas de seguridad de la información.
Propuesta	Procedimiento de Auditoría a los Sistemas de Información
Etapa de Planeación	• Objetivo y Alcance • Normatividad Relacionada • Lineamientos Generales • Procedimiento Detallado • Diagrama de Flujo • Relación de Anexos • Resumen de Cambios
Etapa de Realización	• Solicitud de creación del documento en el SIGA • Cargue del documento en el SIGA • Aprobación del procedimiento • Divulgación del procedimiento
Etapa de Verificación	• Seguimiento al cumplimiento del procedimiento • Definición de indicadores de gestión • Recolección de sugerencias y cambios • Auditoría al cumplimiento del procedimiento
Etapa de Corrección	• Control de cambios • Acciones de mejora • Propuesta de nueva versión • Análisis de riesgos sobre la amenaza analizada y la efectividad del tratamiento propuesto
PLAN DE TRATAMIENTO DE RIESGO 2	
Tipo de Activo	Actividades y procesos del negocio
Vulnerabilidad	Ausencia de monitoreo de recursos del Sistema
Amenaza	Saturación del sistema de información
Riesgo	Alto

Control de referencia ISO 27001 Anexo A	A.12.1.1 Procedimientos de operación documentados. Control: Los procedimientos de operación se deben documentar y poner a disposición de todos los usuarios que lo necesitan.
Propuesta	Procedimiento de monitoreo al Sistemas de Información Académico con la herramienta Nagios
Etapa de Planeación	• Objetivo y Alcance • Normatividad Relacionada • Lineamientos Generales • Procedimiento Detallado • Diagrama de Flujo • Relación de Anexos • Resumen de Cambios
Etapa de Realización	• Solicitud de creación del documento en el SIGA • Cargue del documento en el SIGA • Aprobación del procedimiento • Divulgación del procedimiento
Etapa de Verificación	• Seguimiento al cumplimiento del procedimiento • Definición de indicadores de gestión • Recolección de sugerencias y cambios • Auditoría al cumplimiento del procedimiento
Etapa de Corrección	• Control de cambios • Acciones de mejora • Propuesta de nueva versión • Análisis de riesgos sobre la amenaza analizada y la efectividad del tratamiento propuesto
PLAN DE TRATAMIENTO DE RIESGO 3	
Tipo de Activo	Actividades y procesos del negocio
Vulnerabilidad	Ausencia del proceso de entrega de cargo pos ausencia
Amenaza	Incumplimiento en la disponibilidad de personal
Riesgo	Alto
Control de referencia ISO 27001 Anexo A	A.7.2.1 Responsabilidades de la dirección. Control: La dirección debe exigir a todos los empleados y contratistas la aplicación de la seguridad de la información de acuerdo con las políticas y procedimientos establecidos por la organización.

Propuesta	Revisar el Instructivo de Entrega de Cargo por Suplencia buscando su aprobación en el SIGA
Etapa de Planeación	• Objetivo y Alcance • Normatividad Relacionada • Lineamientos Generales • Procedimiento Detallado • Diagrama de Flujo • Relación de Anexos • Resumen de Cambios
Etapa de Realización	• Solicitud de creación del documento en el SIGA • Cargue del documento en el SIGA • Aprobación del procedimiento • Divulgación del procedimiento
Etapa de Verificación	• Seguimiento al cumplimiento del procedimiento • Definición de indicadores de gestión • Recolección de sugerencias y cambios • Auditoría al cumplimiento del procedimiento
Etapa de Corrección	• Control de cambios • Acciones de mejora • Propuesta de nueva versión • Análisis de riesgos sobre la amenaza analizada y la efectividad del tratamiento propuesto
PLAN DE TRATAMIENTO DE RIESGO 4	
Tipo de Activo	Hardware
Vulnerabilidad	Ausencia de protocolos de señalización
Amenaza	Accidente Importante
Riesgo	Alto
Control de referencia ISO 27001 Anexo A	A.11.1.5 Trabajo en áreas seguras. Control: Se deben diseñar y aplicar procedimientos para trabajo en áreas seguras.
Propuesta	Procedimiento para trabajo en áreas seguras
Etapa de Planeación	• Objetivo y Alcance • Normatividad Relacionada • Lineamientos Generales • Procedimiento Detallado • Diagrama de Flujo • Relación de Anexos • Resumen de Cambios

Etapa de Realización	• Solicitud de creación del documento en el SIGA • Cargue del documento en el SIGA • Aprobación del procedimiento • Divulgación del procedimiento
Etapa de Verificación	• Seguimiento al cumplimiento del procedimiento • Definición de indicadores de gestión • Recolección de sugerencias y cambios • Auditoría al cumplimiento del procedimiento
Etapa de Corrección	• Control de cambios • Acciones de mejora • Propuesta de nueva versión • Análisis de riesgos sobre la amenaza analizada y la efectividad del tratamiento propuesto
PLAN DE TRATAMIENTO DE RIESGO 5	
Tipo de Activo	Software
Vulnerabilidad	Ausencia de documentación
Amenaza	Error en el uso
Riesgo	Alto
Control de referencia ISO 27001 Anexo A	A.14.2.5 Principios de construcción de los sistemas seguros. Control: Se deben establecer, documentar y mantener principios para la construcción de sistemas seguros, y aplicarlos a cualquier actividad de implementación de sistemas de información.
Propuesta	Instructivos de manejo del software tanto de cliente como de administrador del Sistema de Información Académico
Etapa de Planeación	• Objetivo y Alcance • Normatividad Relacionada • Lineamientos Generales • Procedimiento Detallado • Diagrama de Flujo • Relación de Anexos • Resumen de Cambios
Etapa de Realización	• Solicitud de creación del documento en el SIGA • Cargue del documento en el SIGA • Aprobación del procedimiento • Divulgación del procedimiento

Etapa de Verificación	• Seguimiento al cumplimiento del procedimiento • Definición de indicadores de gestión • Recolección de sugerencias y cambios • Auditoría al cumplimiento del procedimiento
Etapa de Corrección	• Control de cambios • Acciones de mejora • Propuesta de nueva versión • Análisis de riesgos sobre la amenaza analizada y la efectividad del tratamiento propuesto
PLAN DE TRATAMIENTO DE RIESGO 6	
Tipo de Activo	Redes
Vulnerabilidad	Conexiones deficientes en los cables
Amenaza	Falla en el equipo de Telecomunicaciones
Riesgo	Alto
Control de referencia ISO 27001 Anexo A	A.13.1.1. Controles de redes. Control: Las redes se deben gestionar y controlar para proteger la información en sistemas y aplicaciones.
Propuesta	Procedimiento de monitoreo de la red LAN de la Universidad.
Etapa de Planeación	• Objetivo y Alcance • Normatividad Relacionada • Lineamientos Generales • Procedimiento Detallado • Diagrama de Flujo • Relación de Anexos • Resumen de Cambios
Etapa de Realización	• Solicitud de creación del documento en el SIGA • Cargue del documento en el SIGA • Aprobación del procedimiento • Divulgación del procedimiento
Etapa de Verificación	• Seguimiento al cumplimiento del procedimiento • Definición de indicadores de gestión • Recolección de sugerencias y cambios • Auditoría al cumplimiento del procedimiento
Etapa de Corrección	• Control de cambios • Acciones de mejora • Propuesta de nueva versión

	• Análisis de riesgos sobre la amenaza analizada y la efectividad del tratamiento propuesto
PLAN DE TRATAMIENTO DE RIESGO 7	
Tipo de Activo	Ubicación
Vulnerabilidad	Red energética inestable
Amenaza	Pérdida del suministro de energía
Riesgo	Alto
Control de referencia ISO 27001 Anexo A	A.11.2.2 Servicios de suministros. Control: Los equipos se deben proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministros.
Propuesta	Procedimiento de la operación y gestión de la planta eléctrica de propiedad de la Universidad
Etapa de Planeación	• Objetivo y Alcance • Normatividad Relacionada • Lineamientos Generales • Procedimiento Detallado • Diagrama de Flujo • Relación de Anexos • Resumen de Cambios
Etapa de Realización	• Solicitud de creación del documento en el SIGA • Cargue del documento en el SIGA • Aprobación del procedimiento • Divulgación del procedimiento
Etapa de Verificación	• Seguimiento al cumplimiento del procedimiento • Definición de indicadores de gestión • Recolección de sugerencias y cambios • Auditoría al cumplimiento del procedimiento
Etapa de Corrección	• Control de cambios • Acciones de mejora • Propuesta de nueva versión • Análisis de riesgos sobre la amenaza analizada y la efectividad del tratamiento propuesto

Fuente: El autor.

9. COLABORADORES DEL PROYECTO

PROPONENTES PRIMARIOS:

JOHAN FELIPE MUÑOZ LESMES, ING DE SISTEMAS, EN PROCESO DE SUSTENTACIÓN PARA SER ESPECIALISTA EN SEGURIDAD INFORMÁTICA, CON MAS DE 10 AÑOS DE EXPERIENCIA EN SOPORTE A USUARIO FINAL, ADMINISTRACIÓN DE SERVIDORES Y MANTENIMIENTO A LA PLATAFORMA TECNOLÓGICA. CON MAS DE 3 AÑOS DE EXPERIENCIA EN SEGURIDAD INFORMÁTICA, MANEJO DE INCIDENTES, NORMATIVIDAD Y CUMPLIMIENTO.

PROPONENTES SECUNDARIOS:

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD

INGENIERO JUAN JOSÉ CRUZ GARZÓN

INGENIERO MARTÍN CAMILO CANCELADO RUÍZ

UNIVERSIDAD CENTRAL

DIRECTIVOS UNIVERSIDAD

FUNCIONARIOS ACADÉMICO ADMINISTRATIVOS UNIVERSIDAD

10.RECURSOS DISPONIBLES

Materiales institucionales y financieros

Tabla 17. Recursos disponibles

RECURSO	DESCRIPCIÓN	USO
Equipo Humano	Ingeniero de Seguridad Informática	Ejecución de la propuesta y desarrollo del proyecto
Equipos y Software	Computador de escritorio con software ofimático Impresora láser Resma de papel Bolígrafo La Universidad proporciona los equipos	Documentación de las actividades realizadas. Impresión de documentos necesarios para el proyecto. Insumos necesarios para el desarrollo de las actividades propias del proyecto
Viajes y Salidas de Campo	Se realiza el trabajo en las instalaciones de la Universidad	El análisis al sistema de información académico se realizará propiamente en las instalaciones de la Universidad al igual que los contactos con los funcionarios de la institución
Materiales y suministros	Contrato de autorización de acceso y pruebas al Sistema de Información Académico y a las instalaciones de la Universidad. Inventarios de aplicativos Web. Inventarios de Activos Informáticos. Inventarios de contratos de bienes y servicios. Inventarios de proveedores de bienes y servicios. Listado de funcionarios, cargos y responsabilidades del personal	El uso del contrato es la formalización del proyecto aplicado. Documentos necesarios para realizar la gestión de riesgos al sistema de información académico.

RECURSO	DESCRIPCIÓN	USO
	administrativo. La Universidad proporciona la información.	
Bibliografía	Magerit, Familia de Normas ISO 27000, Norma ISO 22301, Norma NIST 800-30, Norma ISO 31000. La Universidad cuenta con este material.	Documentación necesaria para el análisis inicial que determinar la normativa a utilizar en el desarrollo del proyecto y para el desarrollo del proyecto en sí.

Fuente: El autor.

11.RESULTADOS E IMPACTOS

Es recomendable para el caso de la Universidad, una vez finalizado el proceso de tratamiento de riesgos establecido anteriormente; desarrollar nuevamente todo el proceso de valoración de activos, análisis de amenazas, análisis de vulnerabilidades, valoración del riesgo y tratamiento de riesgos, lo anterior fundamentado bajo la norma ISO 27005 e ISO 27002; esto debido a que la dinámica en temas de seguridad informática es muy cambiante y es evidente que las amenazas pueden variar en el paso del tiempo, pero fundamentalmente es enfocar a la Universidad en la dinámica de la mejora continua en cuanto a sus procesos en seguridad informática.

Frente al monitoreo y la revisión de los riesgos, los riesgos y controles deben monitorearse y revisarse de manera regular, por lo que se deben definir mecanismos para la verificación, supervisión y determinación del estado de los riesgos y controles, con el fin de mejorar continuamente la gestión de riesgos.

Realizan seguimiento y revisión, periódicamente se debe realizar monitoreo a los riesgos y a la efectividad del plan de tratamiento, las estrategias y el sistema de administración que se establece para controlar la implementación; lo anterior para asegurar que las circunstancias cambiantes no alteren las prioridades de los riesgos y la aparición de riesgos remanentes.

Es importante que el Departamento de Tecnología Informática de la Universidad se esfuerce en la preservación de los ambientes productivos de sus aplicaciones. Para lo cual es muy importante que todo cambio que se realice, por pequeño que sea, en dichos ambientes, quede debidamente documentado con fecha, hora, descripción y responsable. Lo anterior debe impactar positivamente la disponibilidad de los sistemas de información para la comunidad universitaria.

Todos los funcionarios de Tecnología Informática y la comunidad universitaria en general deben conocer los procedimientos documentados y aplicarlos en las labores que así lo ameriten asegurando de esta manera el cumplimiento de la normatividad interna establecida y enfocar los esfuerzos a la mejora continua.

La Coordinación de Soporte Técnico es la única dependencia que está autorizada para instalar software en los equipos PC de la Universidad. Toda instalación de software debe ser solicitada por mesa de ayuda a dicha instancia, limitando de esta

manera el acceso de software pirata o malicioso a la infraestructura computacional de la Universidad. Todo software que se utilice en la Universidad debe ser adquirido con las normas establecidas y siguiendo los procedimientos definidos para tal fin (Procedimiento AD-19-P-005 en Borrador). Debe prevalecer la cultura informática al interior de la organización que garantice el conocimiento de los funcionarios de las implicaciones de instalar y utilizar software ilegal en los computadores de la Universidad.

Se recomienda pruebas de los scripts antes de llevarlos a producción del Sistema de Información Académico, con lo cual se logra verificar que la sentencia no tiene errores de sintaxis, verificar que no se dañan los datos, verificar que las modificaciones esperadas se realizan.

Las cuentas de acceso al sistema de información académico son personales e intransferibles. Por ningún motivo deben existir cuentas de acceso que sean compartidas por varios usuarios, además es importante verificar de manera periódica que las cuentas tengan los permisos adecuados que no excedan el nivel de acceso requerido por los usuarios.

Es importante precisar que muchas fallas de seguridad informática están asociadas a versiones de software obsoleto o con deficiencias en seguridad comprobadas por el fabricante, es precisamente por lo anterior que salen versiones de software nuevo que corrigen defectos en seguridad o compatibilidad, es importante prestar atención cuidado a las versiones de software que se utilizan regularmente ya sea en los equipos de trabajo, los servidores o en los dispositivos móviles con los cuales se accede al Sistema de Información Académico, por lo anterior es recomendable efectuar la comprobación de actualizaciones o versiones recientes del software y realizar la respectiva instalación si así se amerita; si se trata de los equipos de cómputo de la Universidad, solicitar a soporte técnico que realice dicha validación e instalación de actualizaciones de software.

Las sesiones de acceso del usuario son realmente importantes cuando se habla de temas de seguridad, esto radica en que son la puerta de entrada a las diferentes aplicaciones que se utilizan habitualmente como es el caso de las cuentas de correo electrónico, redes sociales, banca y programas de aplicación. Una vez utilizada una aplicación es importante cerrar la sesión evitando de esta manera la manipulación no autorizada de las cuentas y los datos, además mantener las sesiones activas puede provocar acciones no deseadas en las aplicaciones por descuidos y desatenciones.

12.DIVULGACIÓN

Se presenta a la Dirección, los cuadros de análisis generados a raíz de:

- Identificación de activos.
- Valoración de activos.
- Identificación de amenazas.
- Análisis de riesgos.
- Identificación de controles existentes en la Universidad.
- Riesgo residual.
- Análisis de controles aplicados según la norma ISO 27002.
- Plan de tratamiento de riesgos.

Los análisis son aceptados y se solicita la ejecución del plan de tratamiento de riesgos con fecha de inicio de ejecución del 01/06/2018 hasta el 31/12/2018.

Tabla 18. Cuadro de resultados

RESULTADO/PRODUCTO ESPERADO	BENEFICIARIO
Cuadro comparativo de las principales metodologías analizadas para la gestión de riesgos.	Estudiante – Universidad
Plan de trabajo para la implementación de la metodología de gestión de riesgos.	Estudiante – Universidad
Identificación de activos	Estudiante – Universidad
Identificación de amenazas	Estudiante – Universidad
Análisis de riesgos	Estudiante – Universidad
Identificación de controles existentes en la organización	Estudiante – Universidad
Matriz general de riesgos, salvaguardas y riesgo residual.	Estudiante – Universidad
Declaración de aplicabilidad	Estudiante – Universidad
Plan de tratamiento de riesgos	Estudiante – Universidad

Fuente: El autor

13.CRONOGRAMA

Tabla 19. Cronograma de ejecución

ACTIVIDAD	MES 1	MES 2	MES 3	MES 4	MES 5	MES 6
Análisis de estándares.	x					
Definición de Metodología		x				
Propuesta de modelo de trabajo		x				
Desarrollo de la metodología		x	x	x	x	
Entrega de informes						x

Fuente: El autor.

14.CONCLUSIONES

La Universidad al contar con la certificación ISO 9001, tiene avances significativos en la estructura de sus procesos y procedimientos, contando con una aplicación denominada Isolucion, en la cual se administra toda la documentación y las acciones de mejora pertinentes a la implementación de dicha certificación; es evidente que mucha documentación como es el caso de los procesos, procedimientos e instructivos, utilizados para la certificación de ISO 9001, tienen aplicabilidad para el tema de gestión de riesgos como es el caso de la documentación ligada al personal, la seguridad física y los aspectos propios de Tecnología Informática.

En el desarrollo del diagnóstico propuesto para el Sistema de Información Académico de la Universidad, es evidente que muchos factores que inciden de manera directa en la seguridad informática ya han sido cubiertos gracias a los procesos y procedimientos implementados en el desarrollo del a certificación ISO 9001, pero no obstante se evidencian otros que de igual manera deben ser tratados de manera oportuna en veras de mitigar los riesgos que amenazan la integridad del Sistema de Información.

Las diferentes metodologías que pueden ser aplicadas para el diagnóstico de seguridad de un sistema de información, tienen elementos comunes que permiten su integración, en el caso específico de la Universidad, el tener implementado el sistema de calidad bajo la norma ISO 9001, facilita en gran medida el análisis de seguridad bajo el enfoque de la norma ISO 27001 y sus normas complementarias.

La aplicabilidad de las diferentes normas en el sistema de información académico de la Universidad, evidencia falencias en factores críticos de seguridad, pero de igual manera revela un gran avance en cuanto a procesos de seguridad implementados y operativos, así estos procesos no estén documentados o enmarcados bajo una normativa de seguridad de la información específica.

Es recomendable para el caso de la Universidad, una vez finalizado el proceso de tratamiento de riesgos establecido anteriormente; desarrollar nuevamente todo el proceso de valoración de activos, análisis de amenazas, análisis de vulnerabilidades, valoración del riesgo y tratamiento de riesgos, lo anterior fundamentado bajo la norma ISO 27005 e ISO 27002; esto debido a que la dinámica en temas de seguridad informática es muy cambiante y es evidente que las amenazas pueden variar en el paso del tiempo, pero fundamentalmente es enfocar a la Universidad en la dinámica de la mejora continua en cuanto a sus procesos en seguridad informática.

15.POSIBILIDADES DE PUBLICACIÓN

Se autoriza la publicación del presente proyecto aplicado única y exclusivamente al interior de la UNAD, para fines de consulta por parte de los estudiantes y profesores que llegasen a interesarse en el tema tratado.

BIBLIOGRAFÍA

MOLANO VEGA, Diego “DECRETO 1377 DE 2013”. {En línea}. {27 junio de 2013} disponible en: (http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=53646#0).

CORONADO, Paulo “Introduction OWASP Top Ten Project/es - OWASP”. {En línea}. {20 de Julio de 2009} disponible en: (https://www.owasp.org/index.php/Introduction_OWASP_Top_Ten_Project/es).

RUIZ, Javier “ISO27000.es - El portal de ISO 27001 en español. Gestión de Seguridad de la Información”. {En línea}. {2005} disponible en: (http://www.iso27000.es/).

ISAZA, Andrés “Ley de Delitos Informáticos en Colombia”. {En línea}. {2 de mayo de 2016} disponible en: (http://www.deltaasesores.com/articulos/autores-invitados/otros/3576-ley-de-delitos-informaticos-en-colombia).

Redacción de El País y Colprensa “Lo que tiene que saber sobre la nueva ley de Protección de Datos”. {En línea}. {05 de Agosto de 2013} disponible en: (http://www.elpais.com.co/colombia/lo-que-tiene-que-saber-sobre-la-nueva-ley-de-proteccion-de-datos.html).

ICETEX “MANUAL DE ADMINISTRACION DEL PLAN DE CONTINUIDAD DEL NEGOCIO”. {En línea}. {Mayo de 2013} disponible en: (http://www.icetex.gov.co/dnnpro5/Portals/0/Documentos/La%20Institucion/manuales/Manual_continuidad_negocio.pdf).

ALARCÓN ALARCÓN, Beatriz “Norma técnica colombiana de accesibilidad a páginas web”. {En línea}. {31 de Enero de 2012} disponible en: (http://colnodo.apc.org/novedades.shtml?apc=k-xx-1-&x=526).

Secretaría General de Administración Digital “MAGERIT v.3: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información”. {En línea}. {Octubre de 2012} disponible en: (http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.WNRF2mdPvct).

Universidad Central “Portal de Aplicaciones Internas (PAI)”. {En línea}. { 31 Enero 2017} disponible en: (http://www.ucentral.edu.co/universidad-central/portal-de-aplicaciones-internas-pai).

INSTITUTO COLOMBIANO DE NORMAS TECNICAS Y CERTIFICACION. Compendio, tesis y otros trabajos de grado. Quinta Actualización. Bogotá. ICONTEC, 2002.

INSTITUTO COLOMBIANO DE NORMAS TECNICAS Y CERTIFICACION. Continuidad de Negocio. Sistemas de Gestión de Continuidad de Negocio. Requisitos. Primera Actualización. Bogotá. ICONTEC, 2012.

INSTITUTO COLOMBIANO DE CRÉDITO EDUCATIVO Y ESTUDIOS TÉCNICOS EN EL EXTERIOR- ICETEX. MANUAL DE ADMINISTRACION DEL PLAN DE CONTINUIDAD DE NEGOCIOS. Versión 1. Bogotá. ICETEX, 2013.

ANEXOS

Anexo A. Permiso de la universidad para la ejecución del proyecto

Doctor
ING. PEDRO HERNÁN OCAMPO VILLEGAS
Director Tecnología Informática
Universidad Central
Bogotá D.C.

Asunto: Solicitud permiso y autorización para ejecutar proyecto aplicado, "Diagnóstico de seguridad al sistema de información académico de la Universidad Central".

Cordial Saludo:

Respetado Ingeniero, atentamente me dirijo a Ud. con el fin de solicitar permiso y autorización para realizar mi proyecto de grado respecto al diagnóstico de seguridad al sistema de información académico de la Universidad Central, para optar el título de Especialista en Seguridad Informática que estoy realizando con la Universidad Nacional Abierta y Distancia "UNAD".

Sin otro particular.

Cordialmente,

ING. JOHAN FELIPE MUÑOZ LESMES
C.C. [redacted]

Anexo B. Resumen analítico especializado RAE

RESUMEN ANALÍTICO ESPECIALIZADO	
1. Título	DIAGNÓSTICO DE SEGURIDAD AL SISTEMA DE INFORMACIÓN ACADÉMICO DE LA UNIVERSIDAD CENTRAL
2. Autor	Johan Felipe Muñoz Lesmes
3. Edición	**Editorial Universidad Nacional Abierta y a distancia UNAD Especialización en Seguridad Informática**
4. Fecha	25 de Septiembre de 2018
5. Palabras Claves	Activo, Información, Vulnerabilidad, Amenaza, Riesgo, Integridad, Confidencialidad, Disponibilidad, Incidente de seguridad, Salvaguarda, Norma, Metodología, Administración del plan de continuidad del negocio, Incidente de trabajo, Problema de continuidad del negocio, Desastre, Planes de contingencia, Plan de Continuidad del Negocio (PNC), Plan de recuperación de desastres (DRP), Análisis de impacto del negocio (BIA), Frecuencia.
6. Descripción	El documento se basa en dos momentos, el primer momento es un análisis de las diferentes metodologías y estándares utilizados para el tema de análisis y gestión de riesgos en donde se determinará la metodología más adecuada para ser aplicada en el Sistema de Información Académico de la Universidad. Un segundo momento se enfoca en el desarrollo de la metodología seleccionada para el análisis y tratamiento de riesgos al Sistema de Información Académico de la Universidad.
7. Fuentes	MOLANO VEGA, Diego “DECRETO 1377 DE 2013”. {En línea}. {27 junio de 2013} disponible en: (http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=53646#0).

RESUMEN ANALÍTICO ESPECIALIZADO	
	CORONADO, Paulo "Introduction OWASP Top Ten Project/es - OWASP". {En línea}. {20 de Julio de 2009} disponible en: (https://www.owasp.org/index.php/Introduction_OWASP_Top_Ten_Project/es). RUIZ, Javier "ISO27000.es - El portal de ISO 27001 en español. Gestión de Seguridad de la Información". {En línea}. {2005} disponible en: (http://www.iso27000.es/). ISAZA, Andrés "Ley de Delitos Informáticos en Colombia". {En línea}. {2 de mayo de 2016} disponible en: (http://www.deltaasesores.com/articulos/autores-invitados/otros/3576-ley-de-delitos-informaticos-en-colombia). Redacción de El País y Colprensa "Lo que tiene que saber sobre la nueva ley de Protección de Datos". {En línea}. {05 de Agosto de 2013} disponible en: (http://www.elpais.com.co/colombia/lo-que-tiene-que-saber-sobre-la-nueva-ley-de-proteccion-de-datos.html). ICETEX "MANUAL DE ADMINISTRACION DEL PLAN DE CONTINUIDAD DEL NEGOCIO". {En línea}. {Mayo de 2013} disponible en: (http://www.icetex.gov.co/dnnpro5/Portals/0/Documentos/La%20Institucion/manuales/Manual_continuidad_negocio.pdf). ALARCÓN ALARCÓN, Beatriz "Norma técnica colombiana de accesibilidad a páginas web". {En línea}. {31 de Enero de 2012} disponible en: (http://colnodo.apc.org/novedades.shtml?apc=k-xx-1-&x=526). Secretaría General de Administración Digital "MAGERIT v.3: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información". {En línea}. {Octubre de 2012} disponible en: (http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.WNRF2mdPvct). Universidad Central "Portal de Aplicaciones Internas (PAI)". {En línea}. { 31 Enero 2017} disponible en: (http://www.ucentral.edu.co/universidad-central/portal-de-aplicaciones-internas-pai). INSTITUTO COLOMBIANO DE NORMAS TECNICAS Y CERTIFICACION. Compendio, tesis y otros trabajos de grado. Quinta Actualización. Bogotá. ICONTEC, 2002.

RESUMEN ANALÍTICO ESPECIALIZADO	
	INSTITUTO COLOMBIANO DE NORMAS TECNICAS Y CERTIFICACION. Continuidad de Negocio. Sistemas de Gestión de Continuidad de Negocio. Requisitos. Primera Actualización. Bogotá. ICONTEC, 2012. INSTITUTO COLOMBIANO DE CRÉDITO EDUCATIVO Y ESTUDIOS TÉCNICOS EN EL EXTERIOR- ICETEX. MANUAL DE ADMINISTRACION DEL PLAN DE CONTINUIDAD DE NEGOCIOS. Versión 1. Bogotá. ICETEX, 2013.
8. Contenidos	Este proyecto se realizará en la Universidad Central, específicamente para el Sistema de Información Académico el cual involucra las áreas de Registro Académico, Tesorería, Crédito y Cartera, Admisiones y Tecnología Informática. El Sistema de Información Académico se compone de diferentes aplicaciones Web publicadas en el Portal Web Institucional, alojadas en un único servidor de aplicaciones, operadas desde diferentes estaciones de trabajo ubicadas en las áreas mencionadas anteriormente; estas aplicaciones Web están disponibles en internet para el servicio de los estudiantes de la Universidad. El proyecto tiene como alcance el análisis y gestión de riesgos el cual se realizará sobre todos los elementos (humanos, hardware, software, procesos e información), que componen el Sistema de Información Académico, esto mediante el desarrollo de la metodología seleccionada para el tratamiento de riesgos. En este proyecto se proponen las salvaguardas para subsanar los riesgos encontrados, además se contempla el acompañamiento en la implementación de las salvaguardas hasta llegar al riesgo residual junto a las soluciones planteadas; lo anterior implica decisiones de la alta dirección frente a inversión económica, modificación en los contratos con los proveedores y el personal vinculado a la universidad lo cual conlleva tiempos de ejecución excesivamente largos, por este motivo en la documentación del proyecto se hará énfasis en los riesgos residuales que impacten de manera significativa el Sistema de Información Académico de la Universidad junto con las propuestas de solución.

RESUMEN ANALÍTICO ESPECIALIZADO	
9. Metodología	Se utilizó la norma ISO 27001, como metodología de gestión documental. • Sistema de gestión de seguridad de la información. • Ciclo PHVA • Requisitos generales. • Establecimiento y gestión del SGSI (Alcance, Enfoque organizacional, Metodología para evaluación riesgos, Identificación de Riesgos, Evaluación de riesgos, Opciones de tratamiento de riesgos, Controles, Declaración de Aplicabilidad) • Anexo A. Objetivos de Control y Controles Se utilizó la norma ISO 27005, como metodología para la gestión de riesgos. • Alcance y límites. • Gestión del riesgo en la seguridad de la información. • Valoración, análisis y evaluación del riesgo. • Tratamiento del riesgo. • Reducción, retención, evitación, transferencia o aceptación del riesgo. • Comunicación de los riesgos. • Monitoreo bajo la mirada del ciclo PHVA. • Anexo B. Identificación y valoración de activos y valoración de impacto.
10. Conclusiones	La Universidad al contar con la certificación ISO 9001, tiene avances significativos en la estructura de sus procesos y procedimientos, contando con una aplicación denominada Isolucion, en la cual se administra toda la documentación y las acciones de mejora pertinentes a la implementación de dicha certificación; es evidente que mucha documentación como es el caso de los procesos, procedimientos e instructivos, utilizados para la certificación de ISO 9001, tienen aplicabilidad para el tema de gestión de riesgos como es el caso de la documentación ligada al personal, la seguridad física y los aspectos propios de Tecnología Informática. En el desarrollo del diagnóstico propuesto para el Sistema de Información Académico de la Universidad, es evidente que muchos factores que inciden de manera directa en la seguridad informática ya han sido cubiertos gracias a los procesos y procedimientos implementados en el desarrollo del a certificación ISO 9001, pero no obstante se evidencian otros que de igual manera deben ser tratados de manera oportuna en veras de mitigar los riesgos que amenazan la integridad del Sistema de Información.

RESUMEN ANALÍTICO ESPECIALIZADO	
	Las diferentes metodologías que pueden ser aplicadas para el diagnóstico de seguridad de un sistema de información, tienen elementos comunes que permiten su integración, en el caso específico de la Universidad, el tener implementado el sistema de calidad bajo la norma ISO 9001, facilita en gran medida el análisis de seguridad bajo el enfoque de la norma ISO 27001 y sus normas complementarias. La aplicabilidad de las diferentes normas en el sistema de información académico de la Universidad, evidencia falencias en factores críticos de seguridad, pero de igual manera revela un gran avance en cuanto a procesos de seguridad implementados y operativos, así estos procesos no estén documentados o enmarcados bajo una normativa de seguridad de la información específica. Es recomendable para el caso de la Universidad, una vez finalizado el proceso de tratamiento de riesgos establecido anteriormente; desarrollar nuevamente todo el proceso de valoración de activos, análisis de amenazas, análisis de vulnerabilidades, valoración del riesgo y tratamiento de riesgos, lo anterior fundamentado bajo la norma ISO 27005 e ISO 27002; esto debido a que la dinámica en temas de seguridad informática es muy cambiante y es evidente que las amenazas pueden variar en el paso del tiempo, pero fundamentalmente es enfocar a la Universidad en la dinámica de la mejora continua en cuanto a sus procesos en seguridad informática.
11. Autor del RAE	Johan Felipe Muñoz Lesmes