DIAGNOSTICO PARA LA IMPLEMENTACIÓN DE SEGURIDAD DE LA INFORMACIÓN SEGÚN EL ESTÁNDAR NTC ISO/IEC 27001:2013 PARA LA UNIDAD ACADEMICA VIRTUAL Y A DISTANCIA UNIVIDA.

LUISA FERNANDA OROZCO PÉREZ

Tesis para proyecto de grado

Director:

Esp. ANDRES FELIPE ARBOLEDA GAETH

Fundación Universitaria de Popayán

Facultad de Ingeniería

Línea de Investigación Ingeniería de la información

Popayán, diciembre de 2018

LUISA FERNANDA OROZCO PÉREZ

DIAGNOSTICO PARA LA IMPLEMENTACIÓN DE SEGURIDAD DE LA INFORMACIÓN SEGÚN EL ESTÁNDAR NTC ISO/IEC 27001:2013 PARA LA UNIDAD ACADEMICA VIRTUAL Y A DISTANCIA UNIVIDA.

Trabajo de grado presentado a la Facultad de Ingeniería

De la Fundación Universitaria de Popayán

Para obtener el título de

Ingeniero de Sistemas

Director:

Esp. ANDRES FELIPE ARBOLEDA GAETH

Popayán

2018

TRABAJO DE GRADO

DIAGNOSTICO PARA LA IMPLEMENTACIÓN DE SEGURIDAD DE LA INFORMACIÓN SEGÚN EL ESTÁNDAR NTC ISO/IEC 27001:2013 PARA LA UNIDAD ACADEMICA VIRTUAL Y A DISTANCIA UNIVIDA.

Autor:

LUISA FERNANDA OROZCO PÉREZ.

Director:

ANDRES FELIPE ARBOLEDA GAETH

FUNDACIÓN
UNIVERSITARIA
DE POPAYÁN
35 ANIVERSARIO

ACTA DE ACEPTACIÓN

Los jurados del trabajo denominado **"Diagnostico Para La Implementación de Seguridad de la Información Según el Estándar NTC ISO/IEC27001:2013 para la Unidad Académica Y A Distancia UNIVIDA"**, presentado por la estudiante Luisa Fernanda Orozco Perez, una vez revisado la monografía y aprobada la sustentación del mismo, autoriza para se realice los tramites concernientes para optar por el título de Ingeniera de Sistemas.

Firma Jurado 1
Ing. Mónica Torrado

Firma Jurado 2
Ing. Cesar David Ojeda

Popayán, 08, de octubre de 2018

Dedicatoria

Luisa Fernanda Orozco Pérez.

A Dios *por Haberme permitido llegar hasta el final de mi Carrera y haberme dado salud para lograr mis objetivos, además de su infinita bondad y amor.*

A mi familia por la paciencia y todo el tiempo que me han animado para sacar este proyecto adelante.

A mi hijo por ser el motor que me impulso a emprender este sueño.

A mi compañero de vida por ser ese alguien que no dejo que me quedara a mitad del camino.

A todos ellos va dedicado este proyecto.

Resumen

Este trabajo presenta un diagnostico sobre el estado actual con relación a la seguridad de la información en la Unidad Académica Virtual y a Distancia UNIVIDA, basado en el estándar NTC ISO/IEC 27001: 2013, el cual tiene como propósito iniciar con una concientización sobre la importancia que tienen los activos de información (son todos los recursos informáticos o relacionados con éste para que la organización funcione correctamente y alcance los objetivos propuestos por su dirección), que interactúan en sus procesos, para que de esa manera se logre gestionar y salvaguardar éstos.

Para el desarrollo del trabajo de investigación, se tomó como referente el ciclo Denning o PHVA que propone el estándar en mención (ISO/IEC 27001:2013), específicamente como referente su etapa de planificación para iniciar con la identificación de la situación actual en cuanto a la seguridad de la información basados con los criterios del estándar, determinado el alcance y a su vez la criticidad de los riesgos, para analizarlos y evaluarlos conllevando así a la creación de un documento de aplicabilidad de controles y por ende a generar una propuesta de política de seguridad de la información alineado al quehacer estratégico del área.

No obstante, este proyecto se desarrolló bajo el enfoque de investigación exploratorio mediante la ejecución de tres fases, el cual permitirán alcanzar los objetivos propuestos.

Palabras clave: Sistema de gestión de seguridad de la información, riesgo, activos, información, estándar, controles.

Abstract

This paper presents an diagnostic of the current state with a view to information security in the Academic Virtual unit and distantly (Univida), based on the NTC ISO / IEC 27001 standard of 2013, which aims to start with an awareness of the importance they have the information assets (are all the computer resources or related to it for the organization to function properly and achieve the objectives proposed by its address), which interact in their processes, so that in this way it is managed safely manage these.

For the development of the research work, the Denning or PHVA cycle that proposes the standard in question (ISO / IEC 27001: 2013) was taken as a reference, specifically as a reference to its planning stage to begin with the identification of the current situation as soon as possible. to the security of the information based on the criteria of the standard, determined the scope and in turn the criticality of the risks, to analyze and evaluate them leading to the creation of a document of applicability of controls and therefore to generate a policy proposal of information security aligned with the strategic task of the field.

However, this project will be developed under the exploratory research approach through the execution of three phases, which will allow achieving the proposed objectives.

Keywords: Security management system for information, risk, assets, information, standard, controls.

Tabla de Contenido

LISTA DE TABLAS. **Pág.**

LISTA DE FIGURAS **Pág.**

Introducción

El presente proyecto tiene como objetivo principal resolver la problemática que se viene presentando en la Unidad académica virtual y a distancia UNIVIDA, unidad que hace parte de la Fundación Universitaria de Popayán, en esta área se ha identificado que existen unas constantes amenazas, entre ellas se destacan las personas, las tecnológicas y las físicas, ocasionando pérdida de información, debido a la ausencia de lineamientos claros relacionadas con una política de seguridad, así como también desconocen los riesgos que se encuentran asociados a los activos de información que poseen en la organización, lo que les impide poder determinar cuáles serían los controles apropiados y el valor que puede representar ese activo para la misma en caso de tener un incidente de seguridad frente a un activo que no se encuentre controlado.

En el capítulo 1, comprende lo que es la problemática, así como los objetivos planteados para resolver el problema, y el porqué de abordar este tema y su importancia para llegar a encaminar la unidad académica virtual y a distancia UNIVIDA a una certificación bajo el estándar NTC ISO/IEC 27001:2013 [1].

En el capítulo 2, aborda una revisión bibliográfica para referenciar algunos trabajos relacionados con el tema, trabajos que han sido elaborados recientemente siguiendo los lineamientos del estándar NTC ISO/IEC 27001:2013, del mismo modo la revisión del tema legal que abarca la seguridad de la información en Colombia y su aplicabilidad al proyecto.

En el capítulo 3, comprende el desarrollo de la metodología de investigación seleccionada y aplicada a las diferentes fases para llegar a la resolución y alcance de los objetivos propuestos en este trabajo de investigación, la comparación de las metodologías usadas para la evaluación del riesgo, y como resultado final de este proyecto se anexan los lineamientos sugeridos a seguir por la unidad académica virtual y a distancia UNIVIDA para iniciar su proceso para la certificación NTC ISO/IEC 27001:2013 [1].

En el capítulo 4, comprende las conclusiones a las que llegamos después de la investigación y trabajos futuros.

Capítulo 1

Este capítulo comprende el problema, así como también los objetivos que se plantearon para poder resolver la problemática planteada, a continuación se presenta el desarrollo del mismo:

1. PLANTEAMIENTO DEL PROBLEMA

La Unidad Académica Virtual y a Distancia UNIVIDA es una área que lleva a cabo actividades educativas de manera virtual y también dentro de sus procesos tiene como función la elaboración de software educativo para el uso propio y de personas externas; dentro de los procesos que se realizan en esta área se ha identificado que existen unas constantes amenazas entre ellas se destacan las personas (empleados), tecnológicas (Software maliciosos y/o mala configuración de plataformas) y las físicas (Físicas y naturales), ocasionando pérdida de información, debido a la ausencia de lineamientos claros relacionadas con una política de seguridad, así como también desconocen los riesgos que se encuentran asociados a los activos de información que poseen en la organización, lo que les impide poder determinar cuales serian los controles apropiados y el valor que puede representar ese activo para la misma en caso de tener un incidente de seguridad frente a un activo que no se encuentre controlado.

Es importante mencionar que en la actualidad son muy pocas las instituciones de educación superior certificadas bajo el estándar NTC ISO/IEC 27001:2013 [1] que hace referencia a los requisitos de implementación del SGSI (***Sistema de Gestión de Seguridad de la Información***), esto no implica que no sea importante el iniciar con este proceso, sino por el contrario este bajo índice se debe en ocasiones al desconocimiento del estándar por parte de las organizaciones o a la poca relevancia y valor que se le da a la información dentro de las entidades educativas.

Por lo anterior y partiendo de la relevancia que tiene para la Unidad Académica

Virtual y a Distancia UNIVIDA con el manejo de la información a través de las plataformas tecnológicas, se convierte en una prioridad el iniciar con el diagnostico de los requisitos de implementación de seguridad de la información basados en la NTC ISO/IEC 27001:2013, aplicado a un procedimiento de esta unidad, el cual se determinó que será el que se encuentre enmarcado dentro de uno de los procesos que posea una criticidad algida que pueda colocar en riesgo la información que se maneja al interior.

OBJETIVOS

1.2.1 OBJETIVO GENERAL

- Presentar un diagnostico acerca de la seguridad de la información bajo el estándar NTC ISO/IEC 27001:2013 para la Unidad Académica Virtual y a Distancia UNIVIDA.

1.2.1.1 OBJETIVOS ESPECÍFICOS

- Identificar la situación actual en cuanto a la seguridad de la información de la Unidad Académica Virtual y a Distancia UNIVIDA, basada en los dominios del estándar NTC ISO/IEC 27001:2013
- Establecer el alcance para iniciar el diagnostico en cuanto a la seguridad de la información, determinado de acuerdo a la criticidad de los riesgos.
- Identificar mediante el análisis y evaluación de riesgo, las diferentes amenazas y vulnerabilidades a las que están expuestos los activos de información.

1.3 JUSTIFICACIÓN

Actualmente las organizaciones tienen como prioridad garantizarle a sus usuarios seguridad en la información que almacenan en sus sistemas de información y/o documentos físicos, no solo por mantener su reputación dentro del mercado sino a

su vez por los lineamientos legales que aparan a los usuarios en materia de protección de datos exigidos en la legislación colombiana: Ley 1581 de 2012 y la Ley de delitos informáticos 1273 de 2009, determinándole la obligatoriedad implementar protección en ellos.

Dado a lo anterior, se denota la importancia y relevancia del proyecto, del por qué iniciar con el diagnostico para la implementación de un sistema de seguridad de la información en la Unidad Académica Virtual y a Distancia UNIVIDA, esto con el propósito de empezar a identificar las vulnerabilidades, amenzas y riesgos que poseen los procesos que se desarrollan al interior e iniciar con la identificación de controles adecuados que permita mantener una confidencialidad, disponibilidad e integridad de los activos de información que hacen parte de ellos.

Así mismo, también otro de los beneficios que traerá este diagnostico para la implementación de un sistema de seguridad de la información en la Unidad Académica Virtual y a Distancia UNIVIDA, será un análisis del estado real en cuanto a la seguridad y un documento de aplicabilidad que le permitirá gestionar los riesgos avocando en unos lineamientos claros a seguir que estarán plasmados en una propuesta de política de seguridad de información que podrán tomar como referente.

Capítulo 2

Este capítulo contempla los referentes conceptuales, legales y los antecedentes que se tuvieron en cuenta para la formalulación y desarrollo del proyecto.

2. MARCO CONCEPTUAL

A continuación, se relacionan los diferentes conceptos que han contribuido en el desarrollo de la investigación:

2.1 Seguridad de la información

Para toda organización, es importante que la información que se encuentre almacenada en ella esté protegida bajo medidas de seguridad. Es ahí donde nace la necesidad de imlementar seguridad de la información, con el propósito de mantener a salvo todos los datos almacenados conservando la integridad, disponibilidad y confidencialidad de los mismos, desde los que pertenecen a la propia organización como los vinculados con trabajadores y clientes [2].

2.1.2 Seguridad informática

La seguridad informática se define como aquellas reglas, técnicas y actividades destinadas a prevenir, salvaguardar, proteger y resguardar los activos de información tanto físicos como lógicos de una organización, así como también toda aquella infraestructura tecnológica que ha sido destinada para proteger y salvaguardar los activos de información. [3]

2.1.3 Estándares relacionados con la seguridad de la información

Son estándares de seguridad publicados por la Organización Internacional para la Estandarización (ISO) y la Comisión Electrotécnica Internacional (IEC).

La serie contiene las mejores prácticas recomendadas en seguridad de la información para desarrollar, implementar y mantener especificaciones para los Sistemas de Gestión de la Seguridad de la Información (SGSI).

Entre los estándares destacados y que permean este trabajo de investigación se encuentra:

2.1.3.1 ISO/IEC 27000

Este contiene todo el vocabulario en el que se apoya el resto de estándares de esta familia de la ISO/IEC 27000, el cual entrega conceptos claros relacionados con la seguridad de la información [3].

2.1.3.2 ISO/IEC 27001

Es un estándar que contempla los requisitos de implementación para un Sistema de Gestión de Seguridad de la Información, mediante su ciclo Dennig, el cual contempla en cada una de sus etapas una serie de actividades que permitiran establecer lienamientos que salvaguarden la información.

Es de mencionar que es una norma que puede certificarce y ser aplicada a un proceso de la empresa [4].

2.1.3.3 ISO/IEC 27002

Es el código de buenas prácticas para la gestión de seguridad de la información. Fue publicada en julio de 2005 como ISO/IEC 17799:2005 y recibió su nombre oficial ISO/IEC 27002:2005 el 1 de julio de 2007 [5].

2.1.3.4 ISO/IEC 27003

Es una guía de ayuda en la implementación de un SGSI. Sirve como apoyo a la norma 27001, indicando las directivas generales necesarias para la correcta implementación de un SGSI. Incluye instrucciones sobre cómo lograr la implementación de un SGSI con éxito, [6].

2.1.3.5 ISO/IEC 27005

Trata la gestión de riesgos en seguridad de la información. Es la que proporciona recomendaciones y lineamientos de métodos y técnicas de evaluación de riesgos de Seguridad en la Información, en soporte del proceso de gestión de riesgos de la norma ISO/IEC 27001. Es la más relacionada a la actual British Standard BS 7799 parte 3. Publicada en junio de 2008 [7].

2.1.4 Sistema de Gestión de la Seguridad de la Información SGSI

La seguridad de la información, según ISO/IEC 27001, consiste en la preservación de su confidencialidad, integridad y disponibilidad, así como de los sistemas implicados en su tratamiento, con el fin de alcanzar los objetivos de negocio de la entidad [6]

2.1.5 Análisis y Evaluación de Riesgos

Es un método sistemático para la identificación de riesgos a los que son susceptibles los sistemas de información, se caracteriza por brindar como resultado las medidas de control que posteriormente se puedan emplear para minimizar los riesgos asociados a los activos de información de una organización [8].

Entre los elementos claves en el análisis y evaluación de riesgos según la recopilación de información asociada a los activos son:

Amenaza: es la posibilidad de ocurrencia de cualquier tipo de acción o acontecimiento no deseado que puede ocasionar consecuencias perjudiciales sobre los elementos de un sistema, en este caso, sobre los activos de información. Las amenazas se pueden clasificar dependiendo de su origen en Humanas o Natural, destacando que las fallas de origen humano se pueden tipificar como malintencionadas o circunstanciales. Las Amenazas también se pueden calificar según su origen como internas o externas.

Vulnerabilidad: Es la debilidad de un activo, control o proceso, que pueda ser explotada por una amenaza, esta también puede ser calificada como una característica negativa asociada a un activo de información.

Riesgo: Es la posibilidad de que algún incidente impacte negativamente sobre activos de información. La determinación de la probabilidad de ocurrencia y la valoración del impacto tienen lugar en el proceso de gestión del riesgo, que dá como producto la decisión de distribuir o aplicar los controles, generando como resultado la determinación del nivel de riesgo aceptable y la identificación del riesgo a mitigar.

Impacto: Acontecimientos que resultan de los eventos evaluados anteriormente

por la organización.

Confidencialidad: El término hace referencia a la propiedad de la información de ser accesible para los usuarios certificados e inaccesibles para los no autorizados. Los métodos de autenticación están diseñados en beneficio de la confidencialidad.

Integridad: Hace referencia a la propiedad de la información de ser confiable y a su vez garantizar su fuente de origen y sus métodos de procesamiento no permitan alterarla.

Disponibilidad: Propiedad de la información que asegura que los usuarios certificados tienen acceso a esta cuando la requieran, tanto como a sus activos asociados y medios de procesamiento.

Proceso: Es un conjunto de tareas que se interrelacionan para convertir una entrada en un resultado de salida, generalmente una entrada es procedente de la salida de otro proceso.

Procedimiento: Cada uno de los pasos que se realizan para llevar a cabo un proceso, se pueden definir como procedimientos.

Método de las Elipses: El método de las elipses es un mecanismo que permite identificar dentro de un proceso todas las relaciones de sus subprocesos y actividades con otras áreas de la organización, y entidades externas. Una vez establecidas las relaciones, es casi natural poder identificar los activos de información que se usan en dichas relaciones. [9].

De acuerdo a la ISO/IEC 27001:2013, para definir el alcance se incluyen:

- Todas las interfaces que operan en la organización
- Todas las áreas involucradas en los procesos
- Todos aquellos proveedores que incidan en el SGSI

Dado a los requerimientos que ofrece este método, se determina como el más adecuado para determinar el alcance de un SGSI. Este método establece que se han de tomar cada uno de los procesos de una organización y separarlos para su análisis

de la siguiente manera:

- Identificar los procesos básicos y listar los subprocesos de cada uno de ellos. Estos se ubican en la elipse central o concéntrica.
- Ubicar en la elipse intermedia las interacciones que el proceso analizado tiene con otros procesos dentro de la organización, ligándolos a través de flechas.
- En la última elipse o capa más externa, se identifican y se ligan las organizaciones externas a la entidad y que tienen alguna relación o con el proceso analizado.

2.1.6 Activos de información

Son todos aquellos elementos que hacen parte del proceso o procedimiento como, por ejemplo: personas, servicio, hardware, software, recursos auxiliares e infraestructura.

2.2 MARCO LEGAL

El marco legal comprende las diferentes legislaciones colombianas, por el cual debe regirse el sistema de gestión de seguridad de la información.

2.2.1 Ley 1273 de 2009

El 5 de enero de 2009, el Congreso de la República de Colombia promulgó la Ley 1273, “por medio del cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado – denominado “De la Protección de la información y de los datos”- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones”.

Dicha ley tipificó como delitos una serie de conductas relacionadas con el manejo de datos personales, por lo que es de gran importancia que las empresas se blinden jurídicamente para evitar incurrir en alguno de estos tipos penales [10].

2.2.2 Ley 1581 de 2012

Es una ley que complementa la regulación vigente para la protección del derecho

fundamental que tienen todas las personas naturales a autorizar la información personal que es almacenada en bases de datos o archivos, así como su posterior actualización y rectificación. Esta ley se aplica a las bases de datos o archivos que contengan datos personales de personas naturales [11].

2.2.3 Decreto 1377 de 2013

Mediante la Ley 1581 de 2012 se expidió el Régimen General de Protección de Datos Personales, el cual de conformidad con su artículo 1, tiene por objeto "Desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política"; así como el derecho a la información consagrado en el artículo 20 de la misma. Este Decreto tiene como objeto reglamentar parcialmente la Ley 1581 de 2012, por la cual se dictan disposiciones generales para la protección de datos personales [12].

2.2.4 Ley 527 de 1999

Constituye el marco jurídico integral y general que autoriza el uso de los mensajes de datos en todas las actividades de los sectores público y privado. Su campo de acción va más allá de las operaciones comerciales a través de medios electrónicos (comercio electrónico). Aunque regula aspectos de dicha materia y es conocida como la Ley de Comercio Electrónico, fue redactada de manera que comprenda, salvo dos excepciones, dentro de las cuales no se encuentra el contrato de transporte ni los documentos de transporte, todas las actividades en que se involucre el uso de mensajes de datos. [13]

2.3 ANTECEDENTES

A continuación, se relacionan un conjunto de trabajos que han sido referentes para el planteamiento de la investigación:

Los siguientes autores: Jhon Jairo Perafan Ruiz y Mildred Caicedo Cuchimba, en su tesis titulada "**Análisis de Riesgos de la Seguridad de la Información para la Institución Universitaria Colegio Mayor Del Cauca"** publicada en el año 2014, exponen que en la actualidad las empresas y organizaciones de cualquier tipo de índole deben considerar dentro de sus planes de gobierno el aseguramiento de la información generando políticas y controles bien sea en busca de garantizar la continuidad del negocio o de una certificación como carta de presentación y de distinción ante la competencia, cuentan también que La Institución Universitaria debe tomar conciencia de la necesidad de alinear sus objetivos institucionales, asegurar el flujo de información, optimizar recursos y garantizar la confidencialidad, disponibilidad e integridad de la misma, ellos afirman que se debe tener un análisis de riesgos para la Institución Universitaria Colegio Mayor del Cauca con el fin de garantizar mayor efectividad y eficiencia dentro de cada uno de los procesos; teniendo en cuenta que al conocer las fortalezas y debilidades se mejora el control y administración de recursos tecnológicos acorde a las directrices nacionales e internacionales que buscan proporcionar mecanismos y herramientas para adoptar buenas prácticas de seguridad y que de esta forma se logren los objetivos institucionales toman como referencia los estándares ISO/IEC 27000 y las metodologías de implantación de SGSI [14].

Según Yini Dayan Peñuela Vázquez en su monografía titulada **"ANÁLISIS E IDENTIFICACIÓN DEL ESTADO ACTUAL DE LA SEGURIDAD INFORMÁTICA, DIRIGIDO A LAS ORGANIZACIONES EN COLOMBIA, QUE BRINDE UN DIAGNÓSTICO GENERAL SOBRE LA IMPORTANCIA Y MEDIDAS NECESARIAS PARA PROTEGER EL ACTIVO DE LA INFORMACIÓN",** publicación que se realizó recientemente, explica que para realizar este proyecto se tuvo en cuenta los análisis e informes presentados por las empresas de antivirus más grandes del mundo Kaspersky, Symantec, McAfee, ESET y Norton, además teniendo en cuenta reportes

realizados por la ONU, la ISO, la Asociación Colombiana de Ingenieros de Sistemas (ACIS) y también para contextualizar se tomó los informes del Ministerio de Tecnologías de Información y las Comunicaciones de Colombia y la policía nacional de Colombia, donde plantean que se debe tener en cuenta a todo el personal para el conocimiento del SGSI, además debe estar documentado y este es un requisito fundamental para garantizar la administración de la seguridad en una organización, siempre basados en el principio del ciclo de mejora continua PDCA y añade que los beneficios de la implementación de un Sistema de Gestión de la Seguridad de la información son: mejorar la imagen de la organización, disminución del impacto de los riesgos, mayor confianza por parte de los clientes, contar siempre con un plan de contingencia garantizando la continuidad de la organización, valor agregado a su organización, además del cumplimiento de la ley y las normas todo esto basado en el estándar ISO 27001 [15].

Los Autores Yesid Camilo Guerrero Angulo y Rober Marcelo Tobango Goyes en su tesis titulada **“SISTEMA DE GESTION PARA LA SEGURIDAD DE LA INFORMACION (SGSI) BASADO EN LA NORMA ISO 27001 Y 27002 PARA LA UNIDAD DE INFORMATICA Y TELECOMUNICACIONES DE LA UNIVERSIDAD DE NARIÑO”** publicada en el año 2014, ellos afirman que hoy en día ninguna organización está exenta de alguna clase de vulnerabilidades amenazas o ataques, que estos deben ser detectados a tiempo para así diseñar una seria de controles que las contrarresten y que para lograrlo se crearon las diferentes normas, entre ellas existe la norma ISO 27000, la cual proporciona un marco de gestión de la seguridad de la información que puede adaptarse por cualquier organización ya sea pública o privada, grande o pequeña. Así mismo este proyecto tuvo como referente también la ISO/IEC 27001:2005, le permitio identificar los activos que necesitaban protegerse para la unidad de informática y telecomunicaciones de la universidad de Nariño, junto con los riesgos, vulnerabilidades , amenazas y controles existentes para cada uno de ellos, una vez se realizó esto, procedieron a definir nuevos controles necesarios para cada uno de los activos, como resultado obtuvieron el sistemas de gestión de la seguridad de la información (SGSI) ajustado a las necesidades actuales que les

permiten gestionar de manera eficiente la información para la unidad, asegurando la integridad, confidencialidad y disponibilidad de la misma y con esto la mejora continua de la institución [16].

Capítulo 3

Este capítulo comprende el desarrollo de la metodología de investigación seleccionada y aplicada a las diferentes fases para llegar a la resolución y alcance de los objetivos propuestos en este trabajo de investigación.

3. METODOLOGÍA

Este proyecto se llevó a cabo con la metodología de investigación exploratoria, ya que por medio de la investigación que se realizo basados en el estándar NTC ISO/IEC 27001:2013, se dio inicio con el proceso de evaluación del diagnostico para la implementación de seguridad de la información en la Unidad Académica Virtual y a distancia UNIVIDA, para llegar a formular las posibles soluciones a las diferentes amenazas que tienen asociadas los activos de información que contempla el proceso a seleccionar.

Por lo anterior, y como su nombre lo indica, se trata de una investigación cuyo objetivo es proporcionar una visión general sobre una realidad o un aspecto de ella, de una manera tentativa o aproximada. Este tipo de estudios es necesario cuando todavía no se dispone de los medios o no hay acceso para abordar una investigación más formal o de mayor exhaustividad. Justamente, la mayoría de las veces, se hace una investigación exploratoria previamente a otra, que se encuentra en proceso de planeación. [17].

Esta iniciativa se desarrolló en tres etapas alineadas a la metodología que son:

FASE 1: Identificación de la situación actual en cuanto a la seguridad de la información de la Unidad Académica Virtual y a Distancia UNIVIDA.

Actividad 1: ***Diseñar Instrumento para la recolección de la información.***

Esta actividad se desarrollo teniendo como criterio el estándar NTC ISO/IEC 27001:2013, específicamente el anexo A, el cual comprende 14 dominios, 35 objetivos de control y 114 controles que fueron referentes para la elaboración de un instrumento Checklist (Lista de chequeo empleada como herramienta para un auditoria), que permitiera recolectar la información y poder determinar el estado real

con respecto a estos en la Unidad Académica Virtual y a distancia UNIVIDA, Ver anexo 1. Lista de Chequeo.

Actividad 2: Realizar un diagnóstico sobre el estado actual con relación al estándar ISO/IEC 27001:2013 a la Unidad Académica Virtual y a distancia (Univida).

Para realizar el diagnóstico sobre el estado actual con respecto a los criterios establecidos en el estándar NTC SO/IEC 27001:2013 se realizó una auditoria, el cual se tomó el instrumento elaborado (Anexo 1) , para la evaluación de cada uno de los controles y aplicarlos a la Unidad Académica Virtual y a distancia UNIVIDA, es importante mencionar que previamente se elaboró el plan de auditoría (Anexo 2), para que de esta manera se pudiera tener el espació, la autorización y la disponibilidad de las personas encargadas en esas áreas y poder así tener una radiografia con respecto al estado real frente a esos 114 controles a evaluar, de los cuales se obtuvo un procentaje de cumplimiento del 52% que equivale a 59 controles y un porcentaje de no cumplimiento del 48% equivalentes a 55 controles,como se muestra en la figura siguiente:

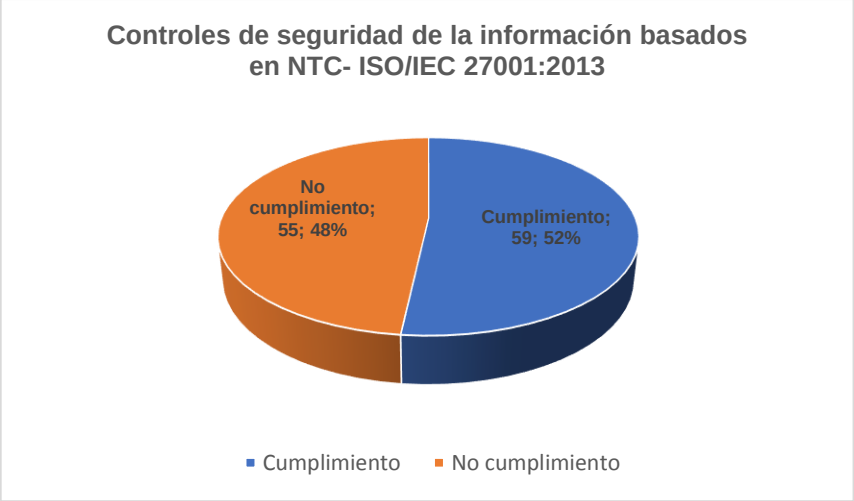

Figura 1. Controles de seguridad de la información basados en la NTC-ISO/IEC 27001:2013

Dado a lo anterior, se llega a concluir que el área de la Unidad Académica Virtual y a distancia UNIVIDA, si desean llegar a tener sus activos de información protegidos deberían iniciar con la implementación de medidas tanto preventivas como correctivas en aquellos controles que no se encuentran implementados para garantizar un riesgo residual y la seguridad de ellos.

A continuación, en se realiza un análisis con respecto al cumplimiento de cada dominio a partir de los hallazgos encontrados:

Dominio A.5 Política de seguridad de la información

A partir del diagnóstico realizado se observa en la figura 3, el no cumplimiento de los controles de este dominio en un 100%, de un total de 2 controles.

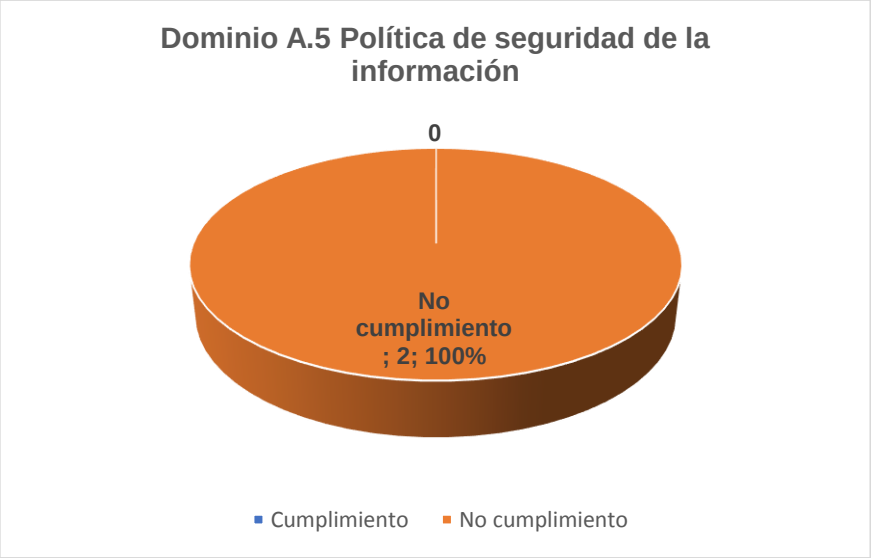

Figura 2. Dominio A.5 Política de seguridad de la información

Dominio A.6 Aspectos organizativos de la seguridad de la información

En este dominio se identificó que tiene un 43% de cumplimiento, el cual es equivalente a 3 controles, y posee un 57% de no cumplimiento que es igual a 4 controles que no se cuentan con ninguna medida que permita salvaguardar la información, como se muestra en la figura 3.

Figura 3. Dominio A.6 Aspectos organizativos de la seguridad de la información

Dominio A.7 Seguridad ligada a los recursos humanos

En el siguiente dominio se identificó que cumple con 4 de sus controles equivalentes al 67% de cumplimiento y en cuanto a los controles que no se cumplen se evidencia un 33% equivalente a 2 controles como se muestra en la figura 4.

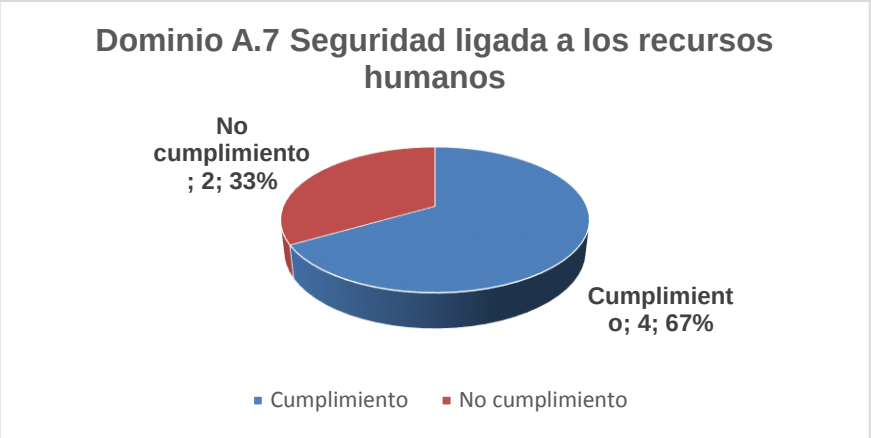

Figura 4. Dominio A.7 Seguridad ligada a los recursos humanos.

Dominio A.8 Gestión de activos.

Se identifica a través de este domino el cumplimento del 40% de los controles equivalentes a 4 de ellos y no cumplimiento de 6 con un promedio del 60%, como se muestra en la figura 5.

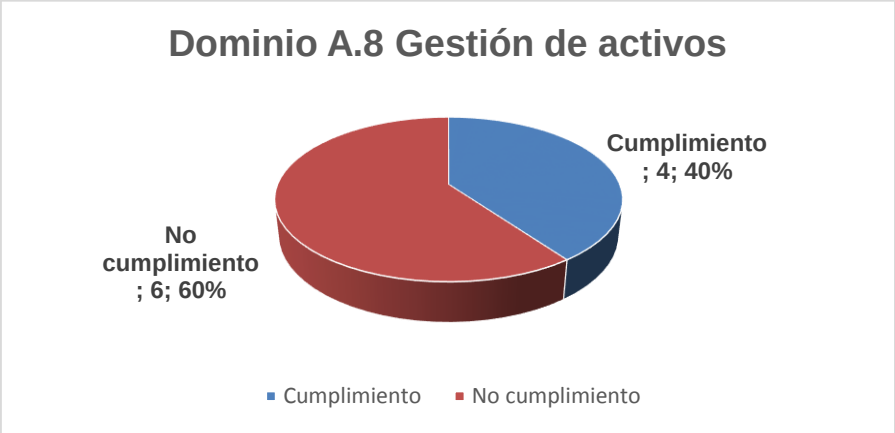

Figura 5. Dominio A.8 Gestión de activos.

Dominio A.9 Control de accesos.

En lo que refiere al dominio de control de accesos se puede constatar que su cumpliento en 4 de los controles equivalentes al 29% y 10 controles de este mismo dominio no se cumplen, los cuales hacen referencia al 71%, como se muestra en la figura 6.

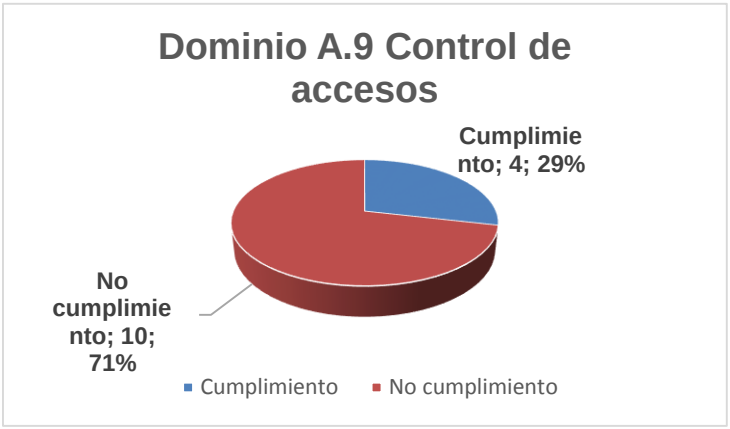

Figura 6. Dominio A.9 Control de Accesos.

Dominio A.10. Cifrado.

El dominio de cifrado no se cumple en sus 2 controles, mostrándonos así el 100% de no cumplimiento, como se muestra en la figura 7.

Figura 7. Dominio A.10 Cifrado.

Dominio A.11 Seguridad física y ambiental.

En lo referente a la seguridad física y ambiental este dominio se cumple en un 47% cumpliendo con 7 de sus controles, por otra parte, no se cumple con el 53%, en los cuales implican 8 de sus controles como se muestra en la figura 8.

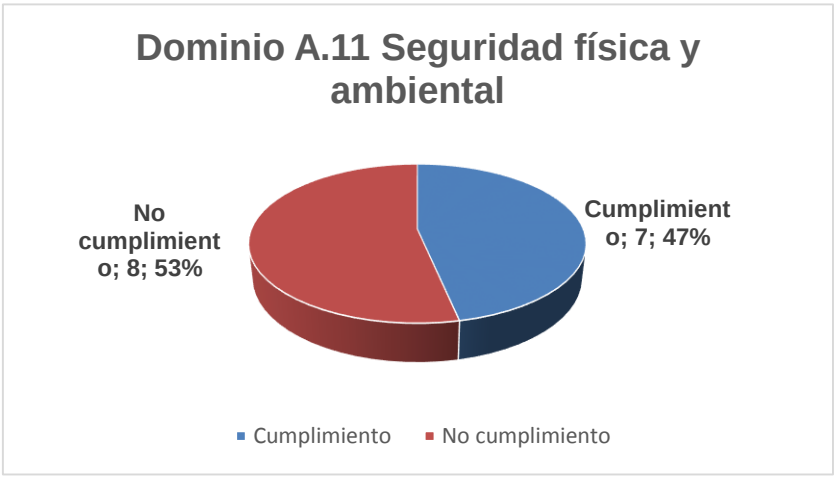

Figura 8. Dominio A.11 Seguridad Física y ambiental.

Dominio A.12 Seguridad de las Operaciones.

En cuanto a la seguridad de las operaciones los controles se cumplen con 11 equivalentes al 79% y 3 de dominio no se cumplen llegando al 21% de no cumplimiento, como se muestra en la figura 9.

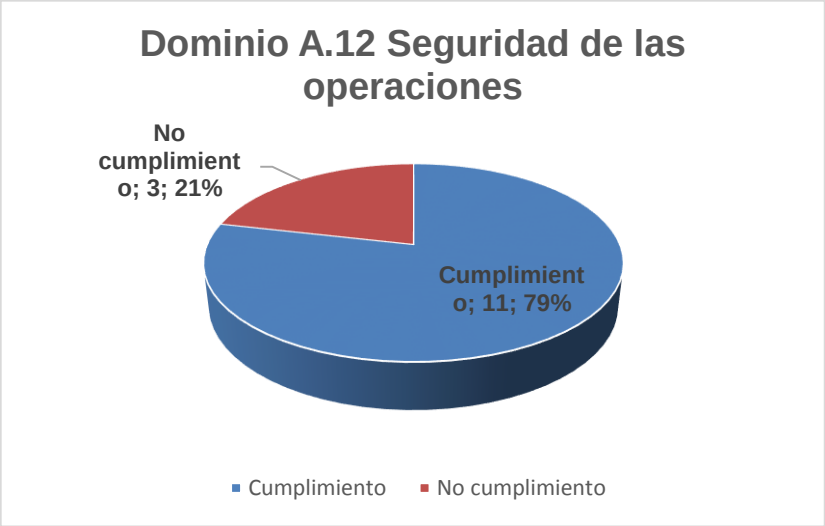

Figura 9. Dominio A.12 Seguridad de las Operaciones.

Dominio A.13 Seguridad en las telecomunicaciones.

En cuanto a seguridad de las telecomunicaciones al que se refiere este dominio, se comprobó que se cumple con 6 de estos controles equivalentes al 86%, y en el no cumplimiento se refiere a 1 solo control que equivale al 14%, como se muestra en la figura 10.

Figura 10. Dominio A.13 Seguridad en las telecomunicaciones.

Dominio A.14 Adquisición, desarrollo y mantenimiento de los sistemas de información.

Se logra verificar que en el dominio A.14 se llega al cumplimento del 69% con 9 controles, y al 31% en el no cumplimento de 4 de estos, como se muestra en la figura 11.

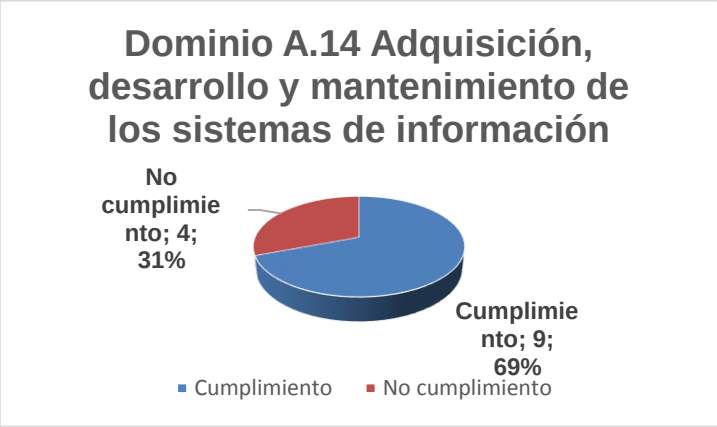

Figura 11. Dominio A.14 Adquisición, desarrollo y mantenimiento de los sistemas de información.

Dominio A.15 Relación con los proveedores.

En cumplimento de este dominio se relacionan 3 controles equivalentes al 60% que se cumplen y 2 que no cumplen a cabalidad el requerimiento, los cuales se refieren a un 40% de no cumplimiento, como se muestra en la figura 12.

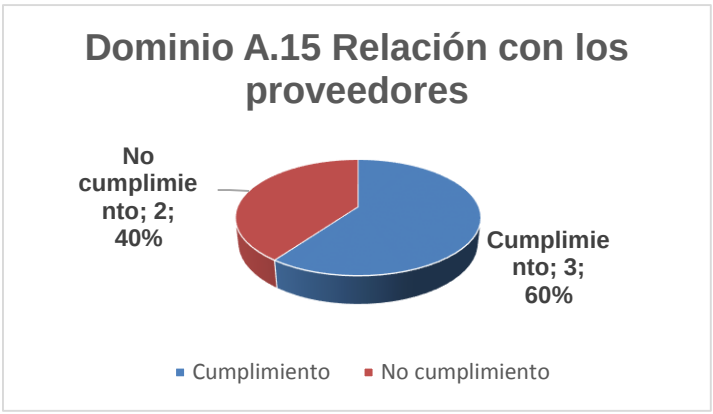

Figura 12. Dominio A.15 Relación con los proveedores.

Dominio A.16 Gestión de incidentes en la seguridad de la información.

Para este dominio que hace referencia a la seguridad de incidentes en la seguridad de la información, se logra establecer que en un 71% hace cumplimiento a 5 controles y en un 29% no cumple con 2 de los controles establecidos para este dominio, como se muestra en la figura 13.

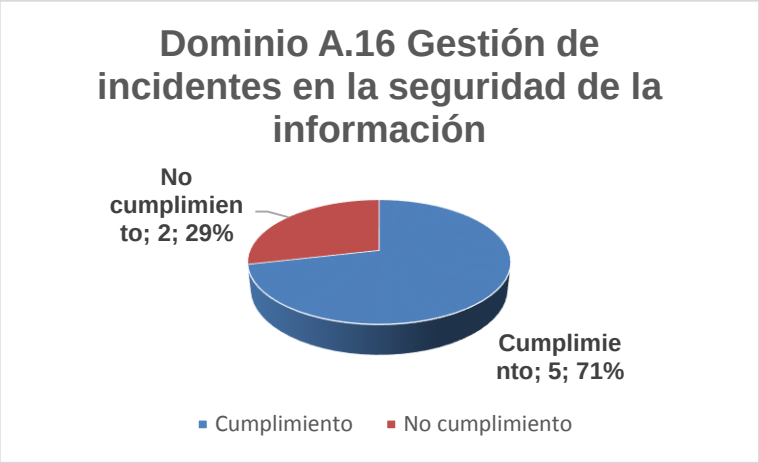

Figura 13. **Dominio A.16 Gestión de incidentes en la seguridad de la información.**

Dominio A.17 Aspectos de seguridad de la información en la gestión de la continuidad del negocio.

En este dominio se cumplen 3 de sus controles con un 75% de cumplimiento y posee un no cumplimiento del 25% equivalente a 1 control, como se muestra en la figura 14.

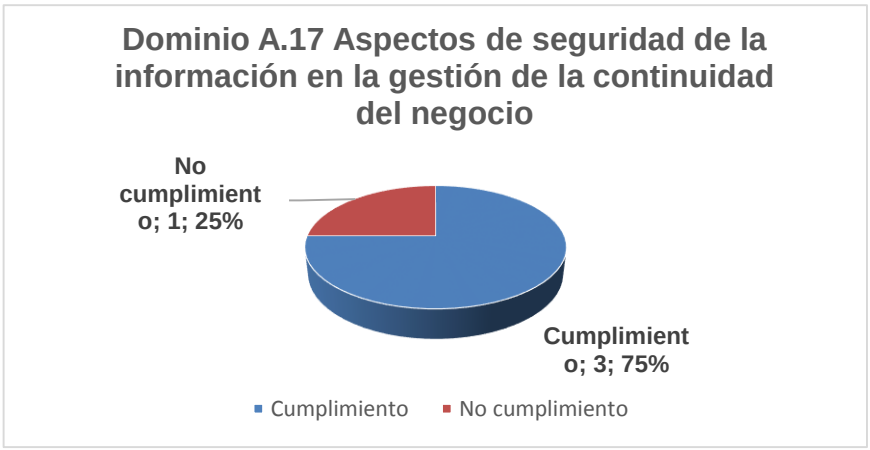

Figura 14. Dominio A.17 Aspectos de seguridad de la información en la gestión de la continuidad del

negocio.

Dominio A.18 Cumplimiento.

En este dominio se identifica que no cumple con 7 de los controles que equivalen a un 88% de no cumplimiento y un 12% de cumplimiento con 1 control, como se muestra en la figura 15.

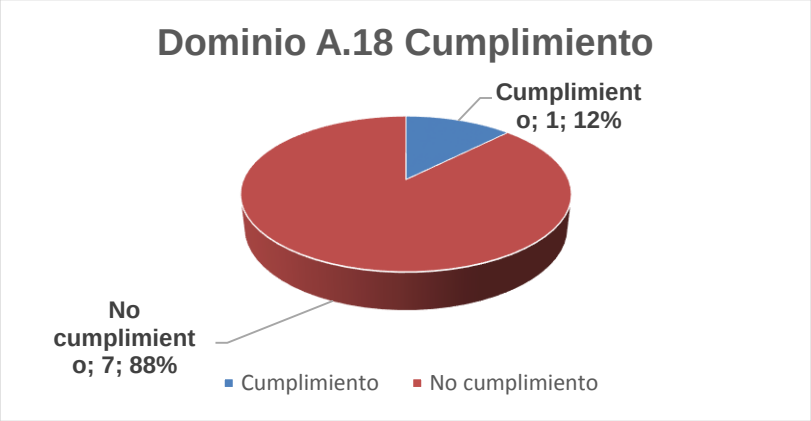

Figura 15. Dominio A.18 Cumplimiento.

De manera detallada se adjunta como Anexo 3. El informe de auditoría generado durante el proceso de evaluación.

FASE 2: Determinación del alcance para iniciar el Diagnostico para implementación de la seguridad de la información, en la Unidad Académica virtual y a Distancia UNIVIDA, de acuerdo a la criticidad de los riesgos.

Actividad 1: **Especificar el alcance para la implementación de la seguridad de la Información de acuerdo a las necesidades identificadas.**

En la sección 4.3. Del estándar NTC ISO/IEC 27001:2013, es un requerimiento obligatorio establecer el alcance como punto de partida para la implementación de un SGSI. Una vez determinado éste dentro de la organización, se procedió a identificar los distintos activos de información, los cuales se convierten en el eje principal del análisis y evaluación del riesgo.

No obstante el alcance para realizar el diagnostico para la implementación de

seguridad de la información según el estándar NTC ISO/IEC 27001:2013 para la Unidad Académica virtual y a Distancia UNIVIDA, se llevó a cabo mediante la metodología de la Elipse, el cual esta permitió visualizar y establecer de manera puntual el flujo de información e interacción de los actores que interactúan con el proceso de Docencia así mismo los procedimientos que abarcan éstos; de esta manera determinar los subprocesos que hacen parte del él; por lo que a través de la elipse en su eje central se situaron éstos que son: (1)Creación de programas académicos virtuales y a distancia, (2)Capacitar en el uso de las Tic, (3)Crear contenidos virtuales, (4)Prestar los servicios académicos virtuales y a distancia, (5)Ejecutar planes y (6)Ejecutar el presupuesto.

Es importante anotar que para determinar e identificar los diferentes procedimientos que integran este proceso se requirió tener como referencia la caracterización del proceso contemplado en el formato **D-UV-CP-001 Caracterización del proceso de Docencia Univida**, así mismo se contó con la descripción de los diferentes procedimientos que integran está, el cual se levantó la información mediante entrevistas sostenidas con los actores y con la documentación proporcionada por cada uno de ellos.

Al tener la información que contempla este proceso de manera organizada se procedió a implementar ésta de la siguiente manera:

En la primera elipse interna se ubicaron los procedimientos que hacen parte del proceso de docencia, los cuales se mencionaron al inicio (1)Creación de programas académicos virtuales y a distancia, (2)Capacitar en el uso de las Tic, (3)Crear contenidos virtuales, (4)Prestar los servicios académicos virtuales y a distancia, (5)Ejecutar planes y (6)Ejecutar el presupuesto), la segunda elipse se ubicaron los actores y/o activos de información que interactúan de manera directa con estos procedimientos y finalmente en la elipse externa se ubicaron los diferentes actores y/o entes que interactúan con estos procedimientos de manera externa como entregando lineamientos, aprobaciones, entre otros.

Seguidamente se procedió a realizar las diferentes interacciones lo que permitió

identificar y determinar el alcance a partir de la mayor cantidad de activos de información que interactúa con este, llegando a concluir que el procedimiento más crítico es el de “Creación de programas académicos virtuales y a Distancia”.

Como se evidencia a continuación en la figura 16, Determinación del alcance basada en la Elipse.

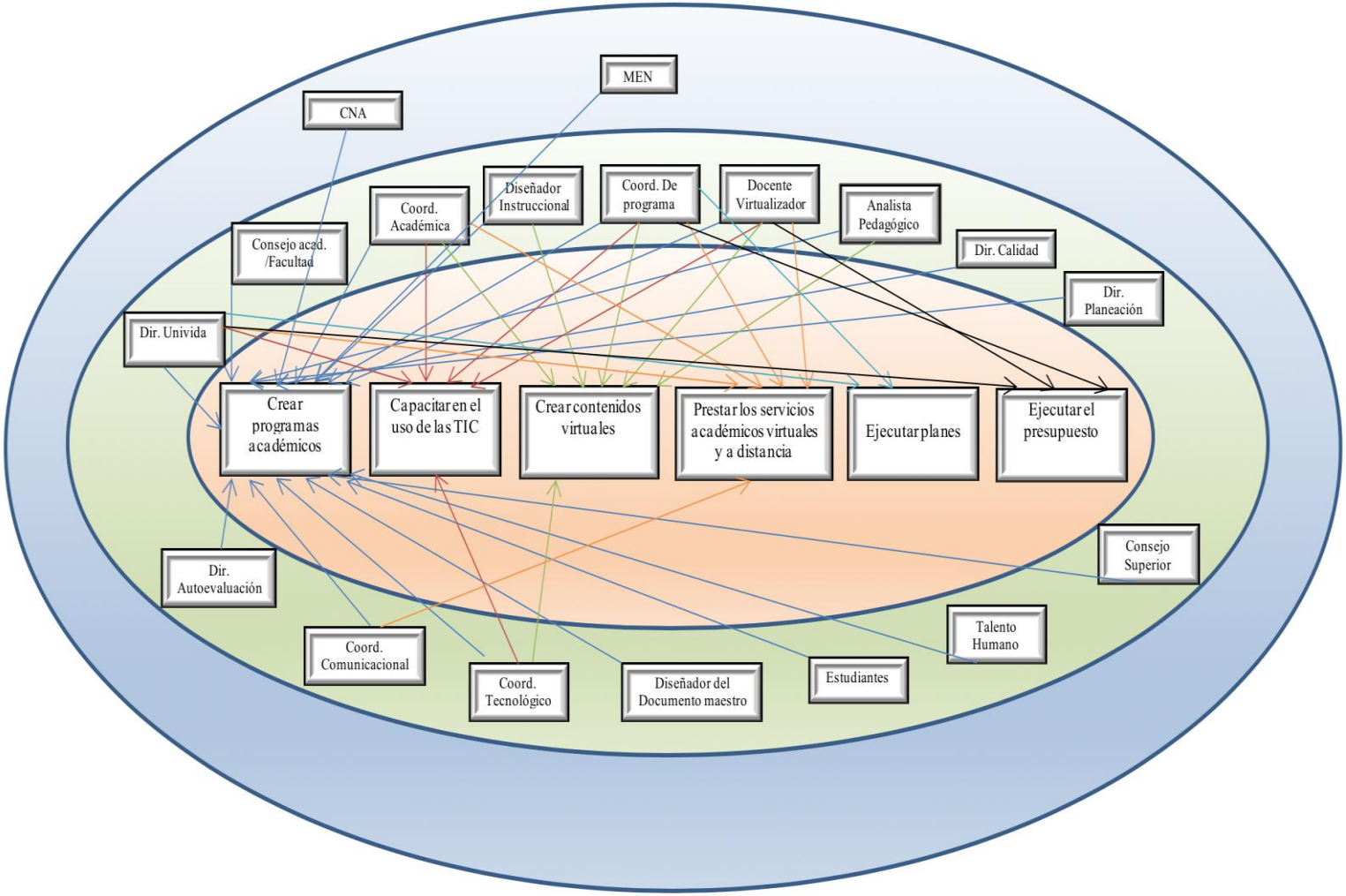

Figura 16. Determinación del alcance basada en la metodología de la Elipse.

FASE 3: Análisis y evaluación de riesgo.

Actividad 1: Realizar un análisis comparativo de las diferentes metodologías y evaluación del riesgo.

A continuación, se relaciona el cuadro comparativo donde se adelantó una investigación exhaustiva para lograr identificar cada una de las ventajas y desventajas de cada metodología y en donde se llegó a la conclusión y del porque realizar la evaluación del riesgo por medio de la estándar NTC ISO/IEC 27005, ya que se pudo evidenciar que permite identificar las necesidades de la organización sobre los requisitos de seguridad de información, de esta manera direccionar a una implementación del SGSI de manera efectiva, abordando los riesgos de manera eficaz y oportuna donde y cuando sea necesario, es parte de la integridad de todas las actividades de gestión de seguridad de la información tanto para su aplicación como para la operación continua de un SGSI.

Tabla 1. Cuadro comparativo de metodologías de evaluación de riesgo

COMPARATIVO DE LAS DIFERENTES METODOLOGIAS		
METODOLOGIAS	VENTAJAS	DESVENTAJAS
MAGERIT	Es metódica por lo que se hace fácil su comprensión. Los activos se identifican - Tipifican, se buscan sus dependencias, se valoran en cuanto a: disponibilidad, confidencialidad, autenticidad, integridad y trazabilidad. - Comprende los procesos de Análisis y gestión de riesgos. Usa un modelo de análisis de Riesgos cualitativo y cuantitativo. - Soporta herramientas comerciales EAR y NO comerciales PILAR, así como las normas ISO/IEC 27001:2005, ISO/IEC 15408:2005, ISO/IEC 17799:2005	No toma en cuenta el principio de no repudio de la información como objetivo de seguridad. No toma en cuenta un análisis de vulnerabilidades. La recomendación de los controles no la incluye dentro del análisis de riesgos si no de la gestión y evaluación. Comprende como elementos del modelo de análisis solo: activos y dependencias. la estimación del impacto se realiza en el proceso de gestión y evaluación de riesgos.
OCTAVE	Cualquier metodología que aplica los criterios y resultado es considerado compatible con metodología octave. -Involucra todo el personal de la entidad. -Es la más completa que Involucra como elementos de su modelo de análisis procesos activos y dependencias recursos vulnerabilidades amenazas y salvaguardas	Aplicable solamente en PYME pequeña y mediana empresa. No tiene compatibilidad con estándares
MEHARI	-Tiene la capacidad de evaluar y simular lo niveles de riesgos derivados de medidas adicionales. -Soporta herramientas comerciales y no comerciales como RISICARE DE BUC S.A. -Es compatible con el estándar ISO/IEC 27001:2005, ISO/IEC 27005:2008. -Usa un modelo de análisis de	Solo toma en cuenta los principios de confidencialidad, integridad y disponibilidad de la información como objetivos de seguridad dejando a un lado el no repudio. La estimación del impacto se realiza en el proceso de gestión y evaluación de riesgos. La recomendación de los controles no la incluye dentro del análisis de riesgos si no en la gestión de riesgos.

	riesgos cualitativo y cuantitativo. -Es una metodología para la gestión de riesgos	
NIST SP 800:30	-Bajo costo relacionado con el riesgo analizado y solventado. -Proporciona una guía para la evaluación de riesgos de seguridad en las infraestructuras TI. -Presenta un resumen de los elementos clave de las pruebas de seguridad técnica y la evaluación con énfasis en técnicas específicas para sus beneficios, limitaciones y recomendaciones para su uso. -Se aplica en el análisis y la gestión de los riesgos.	En su modelo no tiene contemplados elementos como procesos, los activos ni las dependencias.
CRAMM	-Aplica los conceptos de manera formal, estructurada y disciplinada protegiendo los principios de seguridad y sus activos. -Identifica y clasifica los activos TI. -Evalúa el impacto empresarial. Identifica y evalúa amenazas y vulnerabilidades, evalúa niveles de riesgo e identifica los controles requeridos. Combina análisis y evaluación de riesgos	En su modelo no tiene contemplados elementos como los procesos y los recursos.
EBIOS	-Es una herramienta de negociación y de arbitraje. -Es utilizada para múltiples finalidades y procedimientos de seguridad. -Herramienta de código libre y reutilizable, se acopla al cumplimiento de los estándares ISO 27001, 27005, 31000. -Posee una base de conocimiento que describe tipos de entidades, métodos de ataque, vulnerabilidades, objetivos y requerimientos de seguridad.	Se constituye como una herramienta de soporte

ESTÁNDAR 27005	Permite identificar las necesidades de la organización sobre los requisitos de seguridad de información. - Ayuda a crear los SGSI eficaz. - Aborda los riesgos de manera eficaz y oportuna, donde y cuando sea necesario. - Es parte de integridad de todas las actividades de gestión de seguridad de la información tanto para su aplicación como para su operación continua de un SGSI.	No recomienda una metodología concreta dependerá de una serie de factores como el alcance real del sistema de gestión de la seguridad de la información (SGSI), el sector comercial de la propia industria.

Actividad 2: Seleccionar y aplicar la metodología o lineamientos que permitan realizar la identificación y evaluación del riesgo en el área establecida a partir del alcance.

A partir del análisis comparativo realizado por las diferentes metodologías de evaluación de riesgo, se seleccionó el estándar NTC ISO/IEC 27005 para obtener los lineamientos y requisitos que permitieron realizar una identificación y evaluación del riesgo en el procedimiento de creación de programas académicos***,*** de esta manera conocer las amenazas, las vulnerabilidades que tienen asociados los activos que integran esté. A continuación, se visualiza en la tabla 2, esta evaluación el cual sus datos fueron obtenidos y valorados por uno de los integrantes (coordinador tecnológico) de este proceso, que se realizó a través de una entrevista como medio para recolectar información y se logró realizar la tasación de la evaluación los riesgos de los activos (Clasificación del riesgo A (Alto), M (Medio), B (Bajo)), por medio de un rango numérico asciado a una valoración cualitativa, la cual permitió determinar el peso de la valoración y promediar los resultados.

Tabla 2. Evaluación de riesgo activo de información

Activos	Tasacion				Amenazas	Probabilidad de ocurrencia	Vulnerabilidad	Posible Explotación	Valor activo	Posible ocurrencia
	Confidencialidad	Intergridad	Disponibilidad	Total						
Hardware:	A	A	A	A	Bajón de energía,	B	Corte de energía sin previo aviso	B	A	B
1)Servidor					mal uso por parte del funcionario	B	No capacitar previamente al funcionario	B		
2)Pc's					uso no autorizado, falla del equipo.	B	No indicar al empleado que se debe o no usar	B		
							No se realiza mantenimiento en periodos cortos de tiempo.	B		
Recurso Humano:	A	A	A	A	Ausencia de personal	B	Incumplimiento en la disponibilidad del personal	B	A	B
1)Personal del área tecnológica					Que haya una mala contratación	B	Que el personal no cumpla con el perfil adecuado	B		
					Trabajo no supervisado	B	Robo de equipos o información	B		
					uso inadecuado de software y hardware	B	Uso no autorizado del equipo	B		
Infraestructura:	A	A	A	A	Posibilidad de inundación	B	Ubicación en un área susceptible	B	A	B
1)Oficina de coordinación Tecnológica					Robo de equipos	B	ausencia de la protección física de la edificación, puertas y ventanas	B		
					Perdida parcial del suministro de energía.	B	Red energética inestable.	B		
Recursos auxiliares:	A	A	A	A	Tiempo de respuesta del soporte técnico del proveedor	B	Que haya disponibilidad del asistente técnico	B	A	B
1)Impresoras.					Fallas técnicas en la impresora	B	Tiempo de respuesta del proveedor de la impresora.	B		
1)Servicios	A	A	A	A	Acceso equivoco a personal no autorizado.	B	El personal no autorizado modifique información clasificada.	B	A	B

Actividad 3: Generar un documento de aplicabilidad basada en los riesgos.

El análisis y gestión de los riesgos consiste en clasificar las vulnerabilidades dependiendo a que activos de información puede afectar, en lo que concierne al documento de aplicabilidad es determinar el objetivo de control y control seleccionado del mismo para minimizar el riesgo de una amenaza sobre la vulnerabilidad identificada de un activo, mediante el análisis y valoración del riesgo.

Por ejemplo: En la tabla 1, como activo de información se encuentra el hardware “Servidor y Pcs”, para el cual se detectaron las siguientes vulnerabilidades; “Corte de enegía sin previo aviso”. De acuerdo el estándar NTC ISO/IEC 27001:2013, se aplicó el objetivo de control identificado con la clasificación A.11.2 correspondiente a “Equipos” y el control específico asociado a esa vulnerabilidad se determinó el A.11.2.2 relacionado a servicios de suministro, en virtud de que se debe minimizar la pérdida de la información frente a fallas eléctricas. Es así como se procedió a evaluar las diferentes amenazas detectadas e implementación de controles, con el propósito de alcanzar un riesgo residual sobre los activos.

Tabla 3. Documento de aplicabilidad

Activos	Objetivos de Control	Control	Justificación
Hardware	A. 11.2 Equipos	A.11.2.2 Servicios de suministros	Minimiza el riesgo de pérdida de la información frente a fallas en los servicios de suministro de energía
	A. 6.1. Organización Interna	A. 6.1.1 Roles y responsabilidades para la seguridad de la información	Con este se definen todas las responsabilidades relacionadas con la seguridad de la información, haciendo que el empleado realice un manejo adecuado de los activos.
Personas	A. 6.1. Organización Interna	A. 6.1.1 Roles y responsabilidades para la seguridad de la información	Con este se definen todas las responsabilidades relacionadas con la seguridad de la información, haciendo que el empleado realice un manejo adecuado de los activos y asuma las resposnabilidades de acuerdo a sus funciones.
	A. 7.1 Antes de asumir el empleo	A.7.1.1 Selección	Durante el proceso de selección, se debe verificar los antecedentes del empleado, de esta manera se minimizará el riesgo a contratar a personas que no cumplan con el perfil de la labor a desempeñar.
	A. 7.2 Durante la ejecución del empleo	A. 7.2.2 Toma de conciencia, educación y formación en la seguridad de la información.	Realizar actividades de capacitación que permitan concientizar a los empleados sobre la importancia que tienen los activos de información con respecto a la seguridad.
	A. 11.2 Equipos	A.11.2.7 Equipos de usuarios desatendido.	Con la implementación de este control, se minimizará el riesgo de que el personal no autorizado pueda acceder a la información que no se le está permitida.
Infraestructura	A. 11.1 Áreas seguras - A. 11.2 Equipos	A.11.1.1, Perimetro de seguridad fisica A.11.1.2 Controles de acceso fisicos, A.11.1.4Proteccion contra amenazasexternas y ambientales, A.11.1.5Trabajo en areas seguras, A. 11.2.1 Ubicación y proteccion de equipos, A.11.2.8 Equipo de usuario desantentido, A.11.2.2 Servicio de suministro	Con la implementación de estos controles les permitirá tener unas barreras de seguridad física frente al recinto que conforma la Unidad Académica virtual y a distancia.
Recursos alternos	A.15.2. Gestión de prestación de servicios a proveedores	A.15.2.1 Seguimiento y revisión de los servicios de los proveedores	Con este control le permitirá hacer seguimiento de los servicios que prestan los proveedores en lo concernientes al soporte requerido de los activos.
Servicios	A. 18.2.Revisiones de seguridad de la información	A.18.2.3 Revisión del cumplimiento técnico	Este control permitirá que la persona encargada del sistema realice revisones de manera periodica en lo relacionado con el cumplimiento de las directrices y normas de seguridad frente al sistema.

Actividad 4: Entregar lineamientos alineados a una propuesta de política de seguridad de la información.

Lineamientos para una propuesta de Políticas Generales De Seguridad Y Privacidad De La Información.

La dirección de la unidad académica Virtual y a distancia UNIVIDA, entendiendo la importancia de una adecuada gestión de la información, se ha comprometido con la implementación de un sistema de gestión de seguridad de la información (SGSI) Buscando mejorar en el marco de la confianza en el ejercicio de sus deberes para con la Fundación Universitaria de Popayán y los ciudadanos, todo enmarcado en el estricto cumplimiento de las leyes y en concordancia con la misión y visión de la Unidad Académica Virtual y a Distancia UNIVIDA.

Para la Unidad Académica Virtual y a Distancia UNIVIDA, la protección de la información busca la disminución del impacto generado sobre sus activos, por los riesgos identificados de manera metódica con el objeto de mantener el nivel de exposición que permita responder por la integridad, confidencialidad y la disponibilidad de la misma, acorde con las necesidades de los diferentes grupos de interés identificados.

La Unidad Académica Virtual y a Distancia UNIVIDA, para asegurar la dirección estratégica del área, establece la compatibilidad de la política de la seguridad de la información y los objetivos de seguridad de la información, estos últimos correspondientes a:

- Minimizar el riesgo de los procesos misionales del área.
- Cumplir con los principios de seguridad de la información.
- Cumplir con los principios de la función administrativa.
- Mantener la confianza de los funcionarios, contratistas y terceros.
- Apoyar la innovación tecnológica.
- Implementar el sistema de gestión de la seguridad de la información.
- Proteger los activos de la información.
- Fortalecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
- Fortalecer la cultura de seguridad de la información en los funcionarios, terceros, aprendices, practicantes y clientes de la Unidad Académica Virtual y a Distancia UNIVIDA.
- Garantizar la continuidad del negocio frente a incidentes.

Alcance-Aplicabilidad.

Esta política aplica a toda el área, sus funcionarios, contratistas y terceros de la Unidad Académica Virtual y a Distancia UNIVIDA y comunidad en general.

Nivel de cumplimiento.

Todas las personas cubiertas por el alcance y aplicabilidad deberán dar cumplimiento 100% de la política.

A continuación, se establecen las 12 políticas de seguridad que soportan el SGSI de la Unidad Académica Virtual y a Distancia UNIVIDA:

- La Unidad Académica Virtual y a Distancia UNIVIDA se ha decidido definir, implementar, operar y mejorar de forma continua un sistema de gestión de la seguridad de la información, soportado en lineamientos claros y alineados a las necesidades del área y a los requerimientos regulatorios que le aplican a su naturaleza.
- Las responsabilidades frente a las seguridades de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de los empleados, contratistas y terceros.
- La Unidad Académica Virtual y a Distancia UNIVIDA, protegerá la información generada, procesada o resguardada por los procesos del área y activos de información que hacen parte de los mismos.
- La Unidad Académica Virtual y a Distancia UNIVIDA, protegerá la información creada, procesada, transmitida o resguardada por sus procesos de área, con el fin de minimizar impactos financieros, operativos o legales debido al uso incorrecto de esta. Para ello es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o en custodia.
- La Unidad Académica Virtual y a Distancia UNIVIDA, protegerá la información de las amenazas originadas por parte del personal.
- La Unidad Académica Virtual y a Distancia UNIVIDA, protegerá las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.
- La Unidad Académica Virtual y a Distancia UNIVIDA, controlara la operación de sus procesos del área garantizando la seguridad de los recursos tecnológicos y las redes de datos.

- La Unidad Académica Virtual y a Distancia UNIVIDA, implementara control de acceso a la información, sistemas y recursos de red.
- La Unidad Académica Virtual y a Distancia UNIVIDA, garantizara que la seguridad sea parte integral del ciclo de vida de los sistemas de información.
- La Unidad Académica Virtual y a Distancia UNIVIDA, garantizara a través de una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de la información una mejora efectiva de su modelo de seguridad.
- La Unidad Académica Virtual y a Distancia UNIVIDA, garantizara la disponibilidad de sus procesos del área y la continuidad de su operación basada en el impacto que puedan generar los eventos.
- La Unidad Académica Virtual y a Distancia UNIVIDA, garantizara el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas.

El incumplimiento a las políticas de seguridad y privacidad de la información, traerá consigo, las consecuencias legales que apliquen a la normativa de la Unidad Académica Virtual y a Distancia UNIVIDA, incluyendo lo establecido en las normas que competen al Gobierno Nacional en cuanto a seguridad y privacidad de la información se refiere.

Capítulo 4

En esta sección se contemplan las conclusiones y trabajos futuros, que se pueden derivar a partir del proyecto.

Conclusiones

Mediante el análisis y evaluación de riesgos que se realizó para el desarrollo de este trabajo, y a partir de las metodologías evaluadas, se consigue llegar a un listado de controles específicos que permite evidenciar ante la Unidad virtual, una serie de amenazas y vulnerabilidades que pueden poner en riesgo la integridad en el procedimiento de creación de programas académicos , permitiendole formular una serie de controles adecuados para reducir el riesgo que corren los diferentes activos de información que integran éste.

Se concluye con respecto al disgnóstico incial que se realizó con relación a la auditoría efectuada, que la Unidad Virtual tiene un procentaje bastante significativo de no cumplimiento de los controles de seguridad, el cual le impide brindar seguridad a la información que reposa en esta área.

Del mismo modo se sugiere que desde el departamento de sistema se tomen medidas con relación a los lineamientos de seguridad, dado que se detectaron malas prácticas en lo concerniente al manejo de los equipos (borrado seguro, seguridad física y lógica).

A través de la evaluación de la elipse se logró detectar el procedimiento con más interacción de activos y a su vez se consiguió hallar el valor de éstos con respecto a los pilares de la seguridad.

En virtud a lo anterior, se recomienda a la universidad y a la Unidad académica Virtual y a distancia UNIVIDA, evaluar primeramente los controles y a su vez revisar la ley de gobierno en linea especificamente su cuarto eje correspondiente a la seguridad informática, con el ánimo de que inicien con el proceso de implementación al menos con el señalado en este estudio, dado que para el 2020 será un requisito indispensable que las empresas del sector público tengan sus activos asegurados, por tanto no tardaran en solicitarcelos a las empresas del caracter privado.

Trabajos futuros

Con la realización de este trabajo de investigación se propone continuar con el proceso que hoy se inicia a partir del diagnóstico que le permitirá a la Fundación Universitaria de Popayán, iniciar con la preparación de un proceso de certificación bajo el estándar NTC ISO/IEC 27001:2013.

Los instrumentos que se generaron a partir del proyecto podrán ser usados por el personal que designe la organización, para la labor de implementación de estos y a su vez serán los encargados de velar de que los controles que se hayan determinado aquí sean implementados, dando la responsabilidad de la organización en cabeza de sus encargados de velar por la confidencialidad integridad y disponibilidad de la información en caso de que la norma llegase a actualizarse, deberán de realizar sus respectivos ajustes de acuerdo a los nuevos lineamientos establecidos. Cabe aclarar que esta herramienta es única y podrá ser modificada en la manera que el estándar NTC ISO/IEC 27001:2013 sea actualizado y/o modificado, además podrá ser aplicado en las diferentes áreas de la organización independientemente del tipo de proceso que maneje.

Así mismo como trabajo futuro se propone la implementación de los controles, luego evaluar su efectividad mediante una auditoría.

Bibliografía

[1] A. M. A. Quiceno, «Repositorio universidad Poncificia Bolivariana,» 5 4 2018. [En línea]. Available: https://repository.upb.edu.co/handle/20.500.11912/2763.

[2] B. School, «Seguridad de la información, un conocimiento imprescindible,» 24 05 2018. [En línea]. Available: https://www.obs-edu.com/int/blog-investigacion/sistemas/seguridad-de-la-informacion-un-conocimiento-imprescindible.

[3] O. I. p. l. Estandarización, 15 05 2018. [En línea]. Available: https://www.iso.org/isoiec-27001-information-security.html.

[4] I. O. f. Standardization, Requisitos de implementación SGSI 2013, 2013.

[5] I. O. f. Standardization, Guía de buenas prácticas de seguridad, 2013.

[6] Standardization, Guía de implementación de un SGSI 27001:2013.

[7] I. O. f. Standardization, Metodlogía evaluación de riego 27005.

[8] «Gestión de riesgos,» [En línea]. Available: http://www.udistrital.edu.co:8080/documents/276352/356568/Cap5GestionRiesgo.pdf.

[9] J. A. A. Segovia, «Implementacion del primer sistema de gestion de la seguridad de la informacion, en el ecuador,certificado bajo la norma ISO 207001:2005,» 17 3 2018. [En línea]. Available: (https://www.dspace.espol.edu.ec/bitstream/123456789/8080/1/Implementaci%C3%B3n%20del%20primer%20Sistema%20de%20Gesti%C3%B3n%20de%20Seguridad%20de%20la%20Informaci%C3%B3n.pdf) .

[10] C. p. Colombiano, *Ley delitos informáticos,* 2009.

[11] M. d. l. T. -. Mintic, 2012.

[12] M. d. l. T. -. Mintic, *Decreto 1377 de 2013,* 2013.

[13] Cardenas, Erick Rincon, «Ambito Juridico,» 3 4 2018. [En línea]. Available: https://www.ambitojuridico.com/noticias/tic/uso-de-medios-electronicos-i-la-ley-527-de-1999-como-instrumento-normativo-suficiente.

[14] J. J. P. R.-M. C. Cuchimba, «Analisis de riesgos de la seguridad de la informacion,» 3 4 2018. [En línea]. Available: https://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/2655/3/76327474.pdf.

[15] Y. D. P. Vazquez, «ANÁLISIS E IDENTIFICACIÓN DEL ESTADO ACTUAL DE LA SEGURIDAD INFORMÁTICA, DIRIGIDO A LAS ORGANIZACIONES EN COLOMBIA, QUE BRINDE UN DIAGNÓSTICO GENERAL SOBRE LA IMPORTANCIA Y MEDIDAS NECESARIAS PARA PROTEGER EL ACTIVO DE LA INFORMACIÓN.,» 3 4 2018. [En línea]. Available: https://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/17260/1/35254395.pdf.

[16] Y. C. G. A.-R. M. T. Goyes, «sired.udenar.edu.co,» 3 4 2018. [En línea]. Available: http://sired.udenar.edu.co/2374/.

[17] V. M. R. Niño, Metologia de la investigacion, Bogota: Ediciones de la U, 2011.

ANEXOS. ***Pág.***

Anexo 1

UNIDAD ACADÉMICA VIRTUAL Y A DISTANCIA (UNIVIDA)

FACULTAD DE INGENIERIAS - INGENIERIA DE SISTEMAS

CHECKLIST BASADA EL ESTANDAR NTC ISO/IEC 27001:2013 / DOMINIOS 5-18/

CONTROL	PREGUNTA	RESPUESTA		
		SI	NO	OBSERVACIONES
A.5. POLÍTICAS DE SEGURIDAD.				
5.1 Directrices de la Dirección en seguridad de la información.				
A.5.1.1	**Conjunto de políticas para la seguridad de la información.**			
	Hay definido un conjunto de políticas para la seguridad de la información, aprobada por la dirección, publicada y comunicada a los empleados y partes externas pertinentes.			
A.5.1.2	**Revisión de las políticas para la seguridad de la información.**			
	¿La política para la seguridad de la información es revisada en intervalos planificados?			
A.6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMAC.				
6.1 Organización interna.				

A.6.1.1	**Asignación de responsabilidades para la seguridad de la información.**			
	¿Se encuentran definidos los roles y responsabilidades acerca de la seguridad de la información?			
	¿Cada activo y proceso de la seguridad de la información cuenta con un responsable designado?			
A.6.1.2	**Separación de deberes.**			
	¿El equipo de trabajo de TI tiene debidamente distribuidas sus funciones y áreas de responsabilidad?			
A.6.1.3	**Contacto con las autoridades.**			
	¿La entidad cuenta con un listado de contactos para reportar de manera oportuna un incidente de seguridad de la información?			
A.6.1.4	**Contacto con grupos de interés especial.**			
	¿La entidad cuenta con convenios con otras entidades para intercambiar información con el fin de aumentar la protección de la seguridad de la información?			
A:6.1.5	**Seguridad de la información en la gestión de proyectos.**			

	¿Actualmente se asocia la seguridad de la información en los proyectos que ejecuta la entidad?			
6.2 Dispositivos para movilidad y teletrabajo.				
A.6.2.1	**Política para dispositivos móviles.**			
	¿La entidad cuenta con políticas de seguridad donde se establezcan el uso de dispositivos móviles?			
	¿Se realiza algún tipo de campaña con el fin de concientizar a los usuarios acerca del uso de dispositivos móviles relacionados con las actividades del negocio?			
A.6.2.2	**Teletrabajo.**			
	¿La entidad permite desarrollar actividades de teletrabajo?			
	¿El equipo de trabajo de TI tiene			

	debidamente distribuidas sus funciones y áreas de responsabilidad?			
	¿Existe una política acerca del teletrabajo?			
	¿Se realiza algún tipo de campaña acerca de las buenas prácticas sobre la información que es procesada y almacenada mediante actividades de teletrabajo?			
A.7. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.				
7.1 Antes de la contratación.				
A.7.1.1	**Selección**			
	¿Cuándo la entidad abre una convocatoria para ocupar un empleo en esta, se realiza una verificación de todos los antecedentes de los candidatos?			
A.7.1.2	**Términos y condiciones del empleo**			
	¿En los acuerdos contractuales con empleados y contratistas se establece algún acuerdo de confidencialidad y no divulgación			

	sobre la información?			
7.2 Durante la contratación.				
A.7.2.1	**Responsabilidades de la dirección.**			
	¿A los empleados se les informa acerca de sus roles y responsabilidades de seguridad de la información, antes de ser otorgado todo tipo de acceso a información o sistemas de información confidencial?			
A.7.2.2	**Toma de conciencia, educación y formación en la seguridad de la información**			
	¿Se brinda a los empleados y contratistas de la entidad, educación y formación de conciencia apropiada sobre las políticas y procedimientos existentes?			
A.7.2.3	**Proceso disciplinario.**			
	¿Existe algún proceso disciplinario formal para emprender acciones contra empleados que hayan cometido una violación a la seguridad de la información?			

	¿Es comunicada a todos los empleados y contratistas?			
7.3 Terminación y cambio de empleo				
A.7.3.1	**Terminación o cambio de responsabilidades de empleo.**			
	¿Hay definidas responsabilidades y deberes acerca de la seguridad de la información después de la terminación o cambio de empleo?			
	¿Se le comunica al empleado o contratista estas responsabilidades y deberes?			

CONTROL	PREGUNTA	RESPUESTA		
		SI	NO	OBSERVACIONES
A.8. GESTIÓN DE ACTIVOS.				
8.1. Responsabilidad por los activos				
A.8.1.1	**Inventario de activos.**			
	¿Está identificada la información asociada a los activos de información y las áreas de procesamiento de información?			
	¿Existe un inventario de activos de información?			
	Esta identificado el ciclo de vida de la información, ¿desde su creación, procesamiento, almacenamiento, transmisión, eliminación y destrucción?			
A.8.1.2	**Propiedad de los activos.**			
	¿Los activos de información cuentan con un responsable?			

A.8.1.3	**Uso aceptable de los activos.**			
	¿Hay identificadas, documentadas e implementadas reglas para el uso aceptable de información y de activos asociados con información?			
	¿Existen campañas de concientización dirigidas a empleados y usuarios externos acerca del uso de activos de la organización?			
8.2. Clasificación de la información.				
A.8.2.1	**Clasificación de la información**			
	¿La información se encuentra clasificada en función de algún tipo de requisito? (legal, valor, criticidad, susceptibilidad a divulgación o a modificación no autorizada).			

	¿Los activos diferentes de información se encuentran clasificados? (almacenamiento, procesos que maneja o protección del activo).			
	Etiquetado de la información.			
A.8.2.2	¿Se encuentra implementado un proceso para el etiquetado de la información de acuerdo a la clasificación adoptada por la entidad?			
	Manejo de activos.			
A.8.2.3	¿Se encuentra implementado un proceso para el manejo de activos según la clasificación adoptada por la entidad?			
8.3 Manejo de medios				
	Gestión de medios removibles.			
A.8.3.1	¿Existe un procedimiento para la gestión de medios removibles?			

A.8.3.2	**Disposición de los medios.**			
	¿Existe un procedimiento formal para la disposición segura de medios removibles, con el fin de minimizar los riesgos de fuga de información confidencial a personas no autorizadas?			
A.8.3.3	**Transferencia de medios físicos.**			
	¿Los medios que contienen información cuentan con protección contra acceso no autorizado, uso indebido o corrupción durante el transporte?			
A.9. CONTROL DE ACCESO				
9.1 Requisitos del negocio para control de acceso				
A.9.1.1	**Política de control de acceso.**			
	¿Hay establecida, documentada y revisada una política de control de acceso?			
A.9.1.2	**Acceso a redes y a servicios en red.**			

	¿Existe una política acerca del acceso o del uso de redes y de servicios de red?			
9.2. Gestión de acceso de usuarios				
A.9.2.1	**Registro y cancelación del registro de usuarios.**			
	¿Existe un proceso formal de registro y de cancelación de registro de usuarios para la asignación de derechos de acceso?			
A.9.2.2	**Suministro de acceso de usuarios.**			
	¿Hay implementado un proceso de asignación o revocación de suministro de acceso a usuarios de los sistemas y servicios?			
A.9.2.3	**Gestión de derechos de acceso privilegiado.**			
	¿Existe un proceso para la autorización formal de asignación de derechos de acceso privilegiado?			

A.9.2.4	**Gestión de información de autenticación secreta de usuarios.**			
	¿Existe un proceso formal para el control de asignación de información de autenticación secreta?			
A.9.2.5	**Revisión de los derechos de acceso de usuarios.**			
	¿Se realiza una revisión periódica de los derechos de acceso físicos y lógicos asignados?			
A.9.2.6	**Retiro o ajuste de los derechos de acceso.**			
	¿Al terminar el contrato o acuerdo laboral entre el empleado y la entidad son retirados los derechos de acceso?			
9.3 Responsabilidades de los usuarios				
A.9.3.1	**Uso de información de autenticación secreta.**			
	¿Se les exige a los usuarios mantener la confidencialidad acerca de la información empleada para la autenticación?			

9.4 Control de acceso a sistemas y aplicaciones				
A.9.4.1	**Restricción de acceso a la información.**			
	¿Las restricciones de acceso a la información están basadas en los requisitos de las aplicaciones o en una política de control de acceso?			
A.9.4.2	**Procedimiento de ingreso seguro**			
	¿Existe una técnica de autenticación adecuada para corroborar la Identidad de un usuario?			
A.9.4.3	**Sistema de gestión de contraseñas.**			
	¿Se cuenta con la implementación de un sistema de gestión de contraseñas?			
A.9.4.4	**Uso de programas utilitarios privilegiados.**			
	¿Existe una restricción o control acerca del uso de programas utilitarios que permitan anular el sistema y			

	el control de las aplicaciones?			
A.9.4.5	**Control de acceso a códigos fuente de programas**			
	¿Existe un control acerca del acceso a los códigos fuente de los programas?			
A.10. CRIPTOGRAFIA				
10.1 Controles criptográficos				
A.10.1.1	**Política sobre el uso de controles criptográficos.**			
	¿Existe una política acerca del uso de controles criptográficos para la protección de la información?			
A.10.1.2	**Gestión de llaves.**			
	¿Existe una política acerca del uso de protección y tiempo de vida de las llaves criptográficas durante su ciclo de vida?			

A.11. SEGURIDAD FISICA Y DEL ENTORNO

11.1 Áreas seguras				
A.11.1.1	**Perímetro de seguridad física**			
	¿El área cuenta con sistema de seguridad física en sus alrededores?			
A.11.1.2	**Controles de acceso físico**			
	¿Hay controles de acceso para el ingreso al área?			
A.11.1.3	**Seguridad de las oficinas recintos e instalaciones**			
	¿En el interior del área se aplica un sistema de seguridad para la protección de sus recursos?			
A.11.1.4	**Protección contra amenazas externas y ambientales**			
	¿Hay infraestructura contra desastres naturales, ataques maliciosos o accidentes?			
	Trabajo en áreas Seguras			

A.11.1.5	¿Hay procedimientos que garanticen que el trabajo que se realice, se está ejecutando en áreas seguras?			
A.11.1.6	**Áreas de despacho y carga**			
	No aplica.			
11.2 Equipos				
A.11.2.1	**Ubicación y protección de los equipos**			
	¿Los equipos cuentan con un entorno correcto para su utilización?			
A.11.2.1	¿Los equipos cuentan con un sistema de ventilación adecuada para su funcionamiento?			
	Servicios de suministro			

A.11.2.2	¿Los equipos cuentan con reguladores de fuente y una fuente alterna en caso de desconexión?			
A.11.2.3	**Seguridad del cableado**			
	¿Cuenta con las protecciones adecuadas para el cableado del entorno en donde se encuentran los equipos?			
A.11.2.4	**Mantenimiento de equipos**			
	¿Con qué regularidad realizan mantenimiento preventivo (Limpieza, formato, ETC) a los equipos?			

A.11.2.4	¿A los equipos se les realiza formato total de sus memorias?			
A.11.2.5	**Retiro de Activos**			
	¿Los equipos tienen dispositivos de seguridad como Candados, llaves de seguridad o cualquier medio que garantice la inmovilidad del equipo de manera no autorizada?			
A.11.2.6	**Seguridad de equipos y activos fuera de las instalaciones**			
	¿Toman precauciones en los préstamos de equipos para trabajos en entornos externos a las instalaciones?			
A.11.2.7	**Disposición segura o reutilización de equipos**			
	¿Cuenta con software licenciado en sus equipos?			

A.11.2.8	**Equipos de usuarios desatendidos**			
	¿Tiene licencias para protección de datos			
A.11.2.8	¿Evita recuperaciones posteriores de información de parte de personas no autorizadas?			
	Política de escritorio limpio y pantalla limpia			
A.11.2.9	¿Conoce sobre la política de escritorio limpio?			
A.11.2.9	¿Existe una política de escritorio limpio físico y lógico?			

Evidencias auditoría	
Imagen #1	
Descripción	A.11.1.2

Evidencias auditoría	
Imagen #2	
Descripción	A11.1.4- A11.2.1

Evidencias auditoría	
Imagen #3	
Descripción	A.11.1

Evidencias auditoría	
Imagen #4	
Descripción	A.11.2.2

Evidencias auditoría	
Imagen #5	
Descripción	A.11.1.4

Evidencias auditoría	
imagen #6	
descripción	A.11.2.3

Evidencias auditoría	
imagen #7	
Descripción	A.11.1.3

Evidencias auditoría	
Imagen #8	
Descripción	A.11.1.4

Evidencias auditoría	
Imagen #9	
Descripción	A.11.1.4

Evidencias auditoría	
Imagen #10	
Descripción	A.11.2.1

Evidencias auditoría	
Imagen #11	
Descripción	A.11.1.1

Evidencias auditoría	
Imagen #12	
Descripción	A.11.2.8-A.11.2.7

Evidencias auditoría	
Imagen #13	
Descripción	A.11.2.8-A.11.2.7

A.12. SEGURIDAD DE LAS OPERACIONES				
A 12.1.1	**12.1 PROCEDIMIENTO OPERACIONALES Y RESPOSABILIDADES**			
	¿Los procedimientos de operación se encuentran correctamente documentados?			
A 12.1.2	¿Se realizan cambios periódicos en los procesos de negocios, en las instalaciones y sistemas de procesamiento de información? ¿Estos cambios se realizan de manera controlada?			
A 12.1.3	¿Se realiza seguimiento, actualizaciones y reposiciones a los recursos asignados a los empleados?			

A 12.1.4	¿Se cuentan con diferentes ambientes donde se realizan pruebas controladas con el fin de no alterar la información?			
	12.2 PROTECCIÓN CONTRA CÓDIGO			
A 12.2.1	¿Existen controles de prevención explicadas al personal para la concientización sobre la protección de la información? ¿Se han implementado controles para la detección y recuperación sobre los códigos maliciosos?			
	12.3 COPIAS DE RESPALDO			
A 12.3.1	¿Oportunamente se realizan copias de seguridad de la información, software, de los sistemas?			
	12.4 REGISTRO Y SEGUIMIENTO			
A 12.4.1	¿Los sistemas de información cuentan con registros de auditoría donde se puedan revisar las actividades de los usuarios, fallas y eventos que presenta el sistema?			
A 12.4.2	¿Las instalaciones y la información se encuentran			

	correctamente protegidos contra alteraciones y accesos no autorizados?			
A 12.4.3	¿Se tienen definidas las actividades que realiza el administrador del sistema y éstas son revisadas periódicamente?			
A 12.4.4	¿Los relojes de los equipos y los sistemas de información se encuentran sincronizados?			
A 12.5.1	**12.5 CONTROL DE SOFTWARE OPERACIONAL**			
	¿Existe una política que controle y supervise la instalación de software en los sistemas operativos?			
	12.6 GESTIÓN DE LA VULNERABILIDAD TÉCNICA			
A 12.6.1	¿Oportunamente se cuenta con información de las vulnerabilidades de los sistemas de información? ¿Estás vulnerabilidades son evaluadas para medir el impacto en la organización y así tomar medidas?			
A 12.6.2	¿Existen políticas o procedimientos donde se le explica al			

	usuario el correcto uso de los sistemas operativos y la NO instalación de software no autorizados por el área de sistemas?			
	12.7 CONSIDERACIONES SOBRE AUDITORÍAS DE SISTEMAS DE INFORMACIÓN			
A 12.7.1	¿Se revisan constantemente los registros de auditoría del sistema para evaluar estrategias que minimicen las interrupciones?			
A.13. SEGURIDAD DE LAS COMUNICACIONES				
	13.1 GESTIÓN DE LA SEGURIDAD DE LAS REDES			
A 13.1.1	¿Existe una apolítica donde se establezca que se debe administrar y controlar las redes para proteger la información en sistemas y aplicaciones?			
A 13.1.2	¿Se tienen identificados los mecanismos de seguridad, así como los niveles de servicio y los servicios de red internos y			

	externos?			
A 13.1.3	¿Se encuentran correctamente separados los usuarios, los grupos y sistemas de información en las redes?			
A 13.2.1	**13.2 TRANSFERENCIA DE INFORMACIÓN**			
	¿Se cuenta con políticas y/o controles para la trasferencia de información mediante el uso de tipos de instalaciones?			
A 13.2.2	¿Los acuerdos entre la organización y personal externo tratan sobre la protección segura de la información?			
A 13.2.3	¿Los mensajes que transitan por la mensajería electrónica está totalmente protegida?			
A 13.2.4	¿Existen acuerdos de confidencialidad para la protección de la información?			

A.14. Adquisición, desarrollo y mantenimiento de Sistemas				
	A.14.1 Análisis y especificación de requisitos de seguridad de la información			
A. 14.1.1	Dentro del proceso de construcción y desarrollo de una aplicación sw, tienen en cuentan al menos unos requisitos mínimos de seguridad, durante estos procesos.			
	Seguridad de servicios de las aplicaciones en redes públicas			
A.14.1.2	¿La información que se encuentra en los sistemas de información se encuentra protegidas y disponible solo a las personas autorizadas?			
	Protección de transacciones de los servicios de las aplicaciones			
A.14.1.3	Toda transacción sobre las aplicaciones la información se			

	encuentra protegida para evitar la alteración de ella y/o acceso no autorizado?			
A.14.2 Seguridad en los procesos de desarrollo y de soporte				
	A.14.2 Política de desarrollo seguro			
A.14.2.1	¿Cuentan con unos lineamientos establecidos en una política para el desarrollo seguro en las aplicaciones?			
	Procedimientos de control de cambios en el sistema			
	Cuentan con un procedimiento formal para realizar algún cambio en los sistemas y/o desarrollos.			
A.14.2.2	Revisión técnica de las aplicaciones después de cambios en la plataforma de operación.			
A.14. 2.3	Se realizan pruebas a las aplicaciones y/o plataformas antes de implementarlas al negocio?			

A.14.2.4	Se realizan pruebas a las aplicaciones y/o plataformas antes de implementarlas al negocio?			
A.14.2.5	¿Se cuenta con un documento que establezca los principios para realizar una construcción de sistemas seguros? ¿Siguen las especificaciones de los lineamientos establecidos por la organización en cuanto desarrollo seguro?			
A.14.2.7	Univida, Realiza seguimiento a las actividades y/o productos que son contratados y ejecutados por externos.			
A.14.2.8	¿Durante la etapa de desarrollo se llevan a cabo pruebas de funcionalidad en el campo de la seguridad a los productos sw?			
A.14.2.9	¿Cuentan con pruebas de aceptación y/o criterios de aceptación cuando adquieren un nuevo sistema de información ¿			
14.3 Datos de prueba				
A.14.3.1	¿Los datos de pruebas son seleccionados cuidadosamente? les brindan protección a éstos?			

CONTROL	PREGUNTA	RESPUESTA		
		SI	NO	OBSERVACIONES
A.15. RELACIONES CON LOS PROVEEDORES				
15.1. Seguridad de la información en las relaciones con los proveedores.				
A.15.1.1	**Política de seguridad de la información para las relaciones con proveedores.**			
	¿Existe un acuerdo de confidencialidad entre la entidad y los proveedores, acerca del acceso que tienen los segundos a la información?			
	¿Los acuerdos se encuentran debidamente documentados?			
A.15.1.2	**Tratamiento de la seguridad dentro de los acuerdos con proveedores.**			

	¿Se ha establecido y documentado un acuerdo con los proveedores acerca de las obligaciones de ambas partes con relación al cumplimiento de los requisitos de seguridad de la información?			
A.15.1.3	**Cadena de suministro de tecnología de información y comunicaciones.**			
	¿Están definidos los requisitos de seguridad de la información para aplicar la adquisición de productos o servicios de tecnología de la información y de comunicaciones?			
	¿Han implementado un proceso de seguimiento para validar que los productos y servicios de tecnología de información y comunicación cumplan los requisitos de			

	seguridad establecidos?			
A.15.2.1	**Seguimiento y revisión de los servicios de los proveedores.**			
	¿La organización realiza seguimiento, revisión y auditoria de forma periódica sobre los servicios prestados por los proveedores?			
A.15.2.2	**Gestión de cambios en los servicios de los proveedores**			
	Se realizan ajustes o cambios a las cláusulas o contratos de suministro de servicios teniendo en cuenta la criticidad de la información, sistemas y procesos del negocio involucrados, ¿y la revaloración de los riesgos cuando es requerido?			

A.16. GESTION DE INCIDENTES DE SEGURIDAD DE LA INFORMACION				
	16.1 Gestión de incidentes y mejoras en la seguridad de la información			
A 16.1.1	¿Se han establecido responsabilidades y procedimientos de gestión para garantizar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información?			
A 16.1.2	¿Se cuenta con canales de comunicación adecuados para informar las fallas de seguridad?			
A 16.1.3	¿Se lleva un registro de las debilidades sospechosas que afectan la seguridad de la información en los sistemas o servicios?			
A 16.1.4	¿Se evalúan y clasifican los incidentes que afectan la seguridad de la información?			

A 16.1.5	¿Se da respuesta oportuna a los incidentes reportados que afectan la seguridad de la información?			
A 16.1.6	¿Se cuenta con un documento que contiene las lecciones aprendidas?			
A 16.1.7	¿Existen procedimientos necesarios para la identificación, recopilación, adquisición y preservación de la información que puede servir de evidencia?			
A.17. ASPECTOS DE SEGURIDAD DE LA INFORMACION DE LA GESTION DE CONTINUIDAD DE NEGOCIO				
	17.1 Continuidad de seguridad de la información			
A.17.1 1	Planificación de la continuada de la seguridad de la información: ¿La organización ha determinado los requisitos de seguridad para darle continuidad al negocio frente a situaciones adversas?			

A.17.1.2	Implementación de la continuidad de la seguridad de la información: ¿La organización tiene documentado e implementado un plan de continuidad del negocio?			
A.17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información: La organización verifica periódicamente los controles de seguridad establecidos e implantados en el plan de continuidad del negocio, ¿con el fin de validar si aún son eficaces?			
	17.2 Redundancias			
A.17.2.1	Disponibilidad de instalaciones de procesamiento de información: Las áreas de procesamiento de información tienen implementado mecanismos y controles de seguridad que permitan cumplir una alta disponibilidad sobre el procesamiento de la información.			
A.18. CUMPLIMIENTO				

18.1. Cumplimiento de requisitos legales y contractuales				
A.18.1.1	**Identificación de la legislación aplicable y de los requisitos contractuales**			
	Teniendo en cuenta el enfoque de la entidad, ¿están identificados y documentados todos los requisitos estatutarios, reglamentarios y contractuales pertinentes para cada sistema de información?			
	¿Cada cuánto se actualizan?			
A.18.1.2	**Derechos de propiedad intelectual**			
	¿Hay implementado un procedimiento para asegurar el cumplimiento de los requisitos legislativos, de reglamentación y contractuales relacionados con los derechos de propiedad intelectual y el uso de software patentado?			

A.18.1.3	**Protección de registros**			
	¿La entidad cuenta con esquema de clasificación de registros?			
	¿Existe un procedimiento de almacenamiento y manejo de los medios usados para el almacenamiento de registros?			
	¿Existe un procedimiento acerca del acceso a los datos que se encuentran almacenados e n medios electrónicos?			
	¿Existe un sistema que permita la recuperación de datos almacenados en tiempo y formato aceptable?			

A.18.1.4	**Privacidad y protección de información de datos personales**			
	¿Existe una política en la entidad sobre la privacidad y la protección de datos personales?			
A.18.1.5	**Reglamentación de controles criptográficos**			
	¿La entidad hace uso de controles criptográficos dando cumplimiento a todos los acuerdos, legislación y reglamentación pertinentes?			
18.2. Revisiones de seguridad de la información				
A:18.2.1	**Revisión independiente de la seguridad de la información**			
	¿Existe una revisión independiente para la búsqueda del aseguramiento de la conveniencia, la educación y la eficacia continua del enfoque de la entidad?			

A.18.2.2	**Cumplimiento con las políticas y normas de seguridad**			
	¿La alta dirección revisa con regularidad el cumplimiento de políticas y normas de seguridad implementadas en la entidad?			
A:18.2.3	**Revisión del cumplimiento técnico**			
	¿Los sistemas de información de la entidad revisan periódicamente las políticas y normas de seguridad de la información para determinar su cumplimiento?			

ANEXO 2

PLANEACION DE AUDITORIA					Versión 1.0	25/08/18 Página1de1
PLAN DE AUDITORÍA						
OBJETIVO: Verificar la eficiencia de los controles relacionados con el dominio 5, 6 ,7,8,9,10,11,12,13,14,15,16 17 y 18						
ALCANCE: Diagnosticar el estado real de los controles de seguridad de los dominios basados en la norma NTC-ISO/IEC 27001 de 2013 en Univida (coordinación tecnológica)						
CRITERIOS: NTC-ISO/IEC 27001 de 2013.						
Técnicas y Procedimientos: Entrevista, Lista de chequeo						
EQUIPO AUDITOR		**Líder Equipo Auditor:**	**Luisa Orozco**	**Auditor 1:**		
		Auditor 2:		**Auditor 3:**		
TIPO AUDITORÍA: INTERNA						
DATOS DE AUDITORÍA:	**Dirección**	**Calle 5 No. 8-58**				
	Reunión de apertura	**FECHA:10 de septiembre de 2018**		**HORA: 08:00 a.m. – 09:00 a.m.**		
	Reunión de cierre	**FECHA: 14 de septiembre de 2018**		**HORA: 5:00 p.m. – 6:00 p.m.**		
PROCESO Y/O ACTIVIDAD	**REQUISITO POR AUDITAR (Norma NTC ISO IEC 27001:2013 y Legales)**	**AUDITADOS CARGO Y NOMBRE**	**AUDITOR**	**FECHA**	**HORA**	**Lugar / Regional / Centro zonal**
Reunión de apertura.		Ing. Andrés Felipe Arboleda Ing. Mauricio Realpe	Luisa Orozco	Sept 10 de 2018	8:00 am - 9:00 am	Popayán - Cauca
Instalaciones de Univida - Oficina de Dirección y Coordinación Tecnológica	Dominio 5 y 6	Ing. Mauricio Realpe	Luisa Orozco	Sept 10 de 2018	9:00 am - 11:30 am	Popayán - Cauca
	Dominio 7 y 15	Ing. Andrés Felipe Arboleda	Luisa Orozco	Sept 10 de 2018	2:00 pm - 4:00 pm	Popayán - Cauca
	Dominio 8, 9 y10	Ing. Mauricio Realpe	Luisa Orozco	Sept 11 de 2018	8:00 am - 11:00 am	Popayán - Cauca
	Dominio 11, 12 y 13	Ing. Mauricio Realpe	Luisa Orozco	Sept 12 de 2018	2:00 pm - 6:00 pm	Popayán - Cauca
	Dominio 13, 14, 16	Ing. Mauricio Realpe	Luisa Orozco	Sept 13 de 2018	2:00 pm - 6:00 pm	Popayán - Cauca
	Dominio 17 y 18	Ing. Mauricio Realpe	Luisa Orozco	Sept 14 de 2018	9:00 am - 11:30 am	Popayán - Cauca
Reunión de Cierre				Sept 14 de 2018	5:00 pm - 6:00 pm	Popayán - Cauca
OBSERVACIONES:						
La información que se conocerá por la ejecución de esta Auditoría será tratada confidencialmente, por parte del auditor.						

Anexo 3

INFORME FINAL DE AUDITORÍA

SOLICITUD: Numero 1	
NOMBRE DE LA ORGANIZACIÓN: Unidad Académica Virtual y a distancia – UNIVIDA de la Fundación Universitaria de Popayán	
DOMICILIOS AUDITADOS: Coordinación tecnológica UNIVIDA	
FECHA DE AUDITORÍA: 10 de septiembre de 2018	
CRITERIO DE AUDITORÍA: Estándar NTC-ISO/IEC 27001:2013.	
OBJETIVO: Verificar la eficiencia de los controles de seguridad y organización de la información de la Coordinación Tecnológica UNIVIDA.	
ALCANCE: Diagnosticar el estado real de los controles de seguridad y organización de la información de los dominios contenidos en la norma NTC-ISO/IEC 27001 de 2013 en la Coordinación tecnológica UNIVIDA, sede Popayán	
SECTOR: Educativo.	
***PERSONAL CONTACTADO:**	
NOMBRE	**CARGO**
Mauricio Realpe	Coordinador Tecnológico.
Andrés Arboleda	Director UNIVIDA.

*Únicamente se nombran algunas personas entrevistadas

EQUIPO AUDITOR

AUDITOR LÍDER: Luisa Fernanda Orozco

1. INFORMACIÓN DE LA AUDITORÍA

Durante la revisión que se realizó en la Coordinación Tecnológica-UNIVIDA, a partir de los criterios de la norma **NTC-ISO 27001:2013 y los anexos** que se refieren a la seguridad de la información, se obtuvieron los siguientes resultados:

ELEMENTO/CRITERIO / ACTIVIDAD/		*1	*2
A.5.1 ORIENTACIÓN DE LA DIRECCIÓN PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN			
A.5.1.1	Política de seguridad de la información	**A**	**Nc**
A.5.1.2	Revisión de las políticas para la seguridad de la información.	**A**	**Nc**
A.6.1 ORGANIZACIÓN INTERNA			
A. 6.1.1	Roles y responsabilidades para la seguridad de la información.	**A**	**Nc**
A. 6.1.2	Separación de labores.	**A**	**C**
A. 6.1.3	Contacto con las autoridades.	**A**	**C**
A. 6.1.4	Contacto con grupos de interés especial.	**A**	**Nc**
A. 6.1.5	Seguridad de la información en las gestiones de proyectos.	**A**	**Nc**
A.6.2 DISPOSITIVOS MÓVILES Y TELETRABAJO			
A.6.2.1	Políticas para dispositivos móviles.	**A**	**NC**
A.6.2.2	Teletrabajo.	**A**	**C**

ELEMENTO/CRITERIO / ACTIVIDAD/		*1	*2
A.7.1 ANTES DE ASUMIR EL EMPLEO			
A.7.1.1	Selección	**A**	**C**
A.7.1.2	términos y condiciones del empleo	**A**	**C**

A.7.2 DURANTE LA EJECUCIÓN DEL EMPLEO			
A. 7.2.1	Responsabilidades de la dirección	**A**	**Nc**
A. 7.2.2	Toma de conciencia educación y formación en la seguridad de la información	**A**	**Nc**
A. 7.2.3	Proceso disciplinario	**A**	**C**
A.7.3 TERMINACIÓN Y CAMBIO DE EMPLEO			
A.7.3.1	Terminación o cambio de responsabilidades de empleo	**A**	**C**

ELEMENTO/CRITERIO / ACTIVIDAD/		*1	*2
A.8.1 RESPONSABILIDAD POR LOS ACTIVOS			
A.8.1.1	Inventario de activos	**A**	**C**
A.8.1.2	Propiedad de los activos	**A**	**C**
A.8.1.3	Uso aceptable de los activos	**A**	**Nc**
A.8.1.4	Devolución de los activos	**Na**	**Na**
A.8.2 CLASIFICACIÓN DE LA INFORMACIÓN			
A.8.2.1	Clasificación de la información	**A**	**NC**
A.8.2.2	Etiquetado de la información	**A**	**Nc**
A.8.2.3	Manejo de activos	**A**	**C**
A.8.3 MANEJO DE MEDIOS			
A.8.3.1	Gestión de medios removibles	**A**	**Nc**
A.8.3.2	Disposición de los medios	**A**	**Nc**
A.8.3.3	Transferencia de medios físicos	**A**	**Nc**

ELEMENTO/CRITERIO / ACTIVIDAD/		*1	*2
A.9.1 REQUISITOS DEL NEGOCIO PARA EL CONTROL DE ACCESO			
A.9.1.1	Política de control de acceso	**A**	**Nc**
A.9.1.2	Acceso a redes y a servicios en red	**A**	**Nc**
A.9.2 GESTIÓN DE ACCESO DE USUARIOS			
A.9.2.1	Registro y cancelación de registro de usuarios	**A**	**Nc**
A.9.2.2	Suministro de acceso de usuarios	**A**	**NC**
A.9.2.3	Gestión de derechos de acceso privilegiados	**A**	**Nc**
A.9.2.4	Gestión de información de autenticación Secreta de usuarios	**A**	**Nc**
A.9.2.5	Revisión de los derechos de acceso de usuarios	**A**	**Nc**
A.9.2.6	Retiro o ajuste de los derechos de acceso	**A**	**Nc**
A.9.3 RESPONSABILIDAD DE LOS USUARIOS			
A.9.3.1	Uso de la información de autenticación secreta	**A**	**C**
A.9.4 CONTROL DE ACCESO A SISTEMAS Y APLICACIONES			
A.9.4.1	Restricción de acceso a la información	**A**	**Nc**
A.9.4.2	Procedimiento de ingreso seguro	**A**	**C**
A.9.4.3	Sistema de gestión de contraseñas	**A**	**C**
A.9.4.4.	Uso de programas utilitarios privilegiados	**A**	**Nc**
A.9.4.5	Control de acceso a códigos fuente de programas	**A**	**C**

ELEMENTO/CRITERIO / ACTIVIDAD/		*1	*2
A.10.1 CONTROLES CRIPTOGRÁFICOS			
A.10.1.1	Políticas sobre el uso de controles criptográficos	**A**	**Nc**
A.10.1.2	Gestión de llaves	**A**	**Nc**
A.11.1 ÁREAS SEGURAS			
A.11.1.1	Perímetro de seguridad física	**A**	**Nc**
A.11.1.2	Controles de acceso físicos	**A**	**Nc**
A.11.1.3	Seguridad de oficinas, recintos e instalaciones	**A**	**Nc**
A.11.1.4	Protección contra amenazas externas y ambientales	**A**	**Nc**
A.11.1 5	Trabajo en áreas seguras	**A**	**Nc**
A.11.1.6	Áreas de despacho y carga	**Na**	**Na**
A.11.2 EQUIPOS			
A.11.2.1	Ubicación y protección de los equipos	**A**	**C**
A.11.2.2.	Servicios de suministro	**A**	**C**
A.11.2.3	Seguridad del cableado	**A**	**C**
A.11.2.4.	Mantenimiento de equipos	**A**	**C**
A.11.2.5	Retiro de activos	**A**	**C**
A.11.2.6	Seguridad de equipos y activos fuera de las instalaciones	**Na**	**Na**
A.11.2.7	Disposición segura o reutilización de los equipos	**A**	**C**
A.11.2.8	Equipos de usuarios desatendidos	**A**	**Nc**
A.11.2.9	Política de escritorio y pantalla limpia	**A**	**Nc**

ELEMENTO/CRITERIO / ACTIVIDAD/		*1	*2
A.12.1 PROCEDIMIENTOS OPERACIONES Y RESPONSABILIDADES			
A.12.1.1	Procedimientos de operación documentados	**A**	**C**
A.12.1.2	Gestión de cambios	**A**	**C**
A.12.1.3	Gestión de capacidad	**A**	**C**
A.12.1.4	Separación de los ambientes de desarrollo, pruebas y operación	**A**	**C**
A.12.2 PROTECCIÓN CONTRA CÓDIGOS MALICIOSOS			
A.12.2.1	Controles contra códigos maliciosos	**A**	**C**
A.12.3 COPIAS DE RESPALDO			
A.12.3.1	Respaldo de la información	**A**	**C**
A.12.4. REGISTRO Y SEGUIMIENTO			
A.12.4.1	Registro de eventos	**A**	**C**
A.12.4.2	Protección de la información	**A**	**NC**
A.12.4.3	Registros del administrador y del operador	**A**	**C**
A.12.4.4	Sincronización de Relojes	**A**	**C**
A.12.5 CONTROL DE SOFTWARE OPERACIONAL			
A.12.5.1	Instalación de software en sistemas operativos	**A**	**C**
A.12.6 GESTIÓN DE LA VULNERABILIDAD TÉCNICA			
A.12.6.1	Gestión de las vulnerabilidades técnicas	**A**	**C**
A.12.6.2	Restricción sobre la instalación de software	**A**	**C**
A.12.7 CONSIDERACIONES SOBRE AUDITORÍA DE INFORMACIÓN			
A.12.7.1	Controles de auditorías de sistemas de información.	**A**	**C**

A.13.1 GESTIÓN DE LA SEGURIDAD DE LAS REDES			
A.13.1.1	Controles de redes	**A**	**NC**
A.13.1.2	Seguridad de los servicios de la red	**A**	**C**
A.13.1.3	Separación de las redes	**A**	**C**
A.13.2 TRANSFERENCIA DE INFORMACIÓN			
A.13.2.1	Políticas y procedimientos de la transferencia de la información	**A**	**C**
A.13.2.2	Acuerdos sobre transferencia de información	**A**	**C**
A.13.2.3	Mensajería electrónica	**A**	**C**
A.13.2.4	Acuerdos de confidencialidad o de no divulgación.	**A**	**C**
A.14.1 REQUISITOS DE SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN			
A.14.1.1	Análisis y especificación de requisitos de seguridad de la información	**A**	**C**
A.14.1.2	Seguridad de servicios de las aplicaciones en redes públicas	**A**	**C**
A.14.1.3	Protección de transacciones de los servicios de las aplicaciones	**A**	**C**
A.14.2 SEGURIDAD EN LOS PROCESOS DE DESARROLLO Y SOPORTE			
A.14.2.1	Política de desarrollo seguro	**A**	**C**
A.14.2.2	Procedimientos de control de cambios de sistema	**A**	**C**
A.14.2.3	Revisión técnica de las aplicaciones después de cambios en la plataforma de operación	**A**	**C**
A.14.2.4	Restricciones en los cambios a los paquetes de software	**A**	**NC**

A.14.2.5	Principios de construcción de los sistemas seguros	**A**	**NC**
A.14.2.6	Ambiente de desarrollo seguro	**A**	**C**
A.14.2.7	Desarrollo contratado externamente	**A**	**C**
A.14.2.8	Pruebas de seguridad de los sistemas	**A**	**C**
A.14.2.9	Prueba de aceptación de los sistemas	**A**	**NC**
A.14.3 DATOS DE PRUEBA			
A.14.3.1	Protección de datos de prueba		**NC**
A.15.1 SEGURIDAD DE LA INFORMACIÓN EN LAS RELACIONES CON LOS PROVEEDORES			
A.15.1.1	Política de seguridad de la información para las relaciones con los proveedores	**A**	**C**
A.15.1.2	Tratamiento de la seguridad dentro de los acuerdos con los proveedores	**A**	**C**
A.15.1.3	Cadena de suministro de tecnología de información y comunicación	**A**	**Nc**
A.15.2 GESTIÓN DE LA PRESTACIÓN DE SERVICIO A PROVEEDORES			
A.15.2.1	Seguimiento y revisión de los servicios de los proveedores	**A**	**Nc**
A.15.2.2	Gestión de cambios en los servicios de los proveedores	**A**	**C**
A.16.1 GESTIÓN DE INCIDENTES Y MEJORAS EN LA SEGURIDAD DE LA INFORMACIÓN			
A16.1.1	Responsabilidades y procedimientos	**A**	**C**
A.16.1.2	Reporte de eventos de seguridad de la información	**A**	**C**
A.16.1.3	Reporte de debilidades de seguridad de la información	**A**	**NC**

A.16.1.4	Evaluación de eventos de seguridad de la información y decisiones sobre ellos	**A**	**C**
A.16.1.5	Respuesta de incidentes de seguridad de la información	**A**	**C**
A.16.1.6	Aprendizaje obtenido de los incidentes de seguridad de la información	**A**	**NC**
A.16.1.7	Recolección de evidencia	**A**	**C**
A.17.1 CONTINUIDAD DE SEGURIDAD DE LA INFORMACIÓN			
A.17.1.1	Planificación de la continuidad de la seguridad de la información	**A**	**NC**
A.17.1.2	Implementación de la continuidad de la seguridad de la información	**A**	**C**
A.17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	**A**	**C**
A.17.2 REDUNDANCIAS			
A17.2.1	Disponibilidad de instalaciones de procesamiento de información	**A**	**C**
A.18.1 CUMPLIMIENTO DE REQUISITOS LEGALES Y CONTRACTUALES			
A.18.1.1	Identificación de la legislación aplicable y de requisitos contractuales	**A**	**C**
A.18.1.2	Derechos de propiedad intelectual	**A**	**Nc**
A.18.1.3	Protección de registros	**A**	**Nc**
A.18.1.4	Privacidad y protección de información de datos personales	**A**	**Nc**
A.18.1.5	Reglamentación de controles criptográficos	**A**	**Nc**
A.18.2 REVISIÓN DE SEGURIDAD DE LA INFORMACIÓN			
A.18.2.1	Revisión independiente de la seguridad de la información	**A**	**Nc**

A.18.2.2	Cumplimiento de las políticas y normas de seguridad	**A**	**Nc**
A.18.2.3	Revisión del cumplimiento técnico	**A**	**Nc**

Columna 1 revisión: elementos que aplica del documento de referencia que son adecuados e implementados.

COLUMNA	**CALIFICACIÓN**				
2**	A-Aplica	Na-No Aplica			
1*	C-Cumple	Nr-No Revisado	Nm-Necesita Mejorar	Nc-No Conformidad	Na-No Aplica

1. CONFORMIDADES

A continuación, se detallan las conformidades identificadas durante el proceso de auditoría a la Coordinación Tecnológica, basados en los dominios contemplados en el Anexo A, del estándar NTC-ISO/IEC 27001:2013:

CONTROL Estándar ISO 27001:2013	DESCRIPCIÓN
A.6.1 ORGANIZACIÓN INTERNA	
A.6.1.2	Se evidencia que en la coordinación tecnológica de la Unidad Académica Virtual y a Distancia – UNIVIDA, existe un encargado que vela por la seguridad de la información.
A.6.1.3	En la Unidad Académica Virtual y a Distancia – UNIVIDA, existen roles establecidos para cada una de las actividades que se deben desarrollar dentro de las áreas, con el fin de proteger los activos y el uso de la información.
A.6.2 DISPOSITIVOS MÓVILES Y TELETRABAJO	
A.6.2.2	Con relación al uso de dispositivos móviles y teletrabajo, esta modalidad se cumple plenamente, dado que varios de los integrantes de la unidad académica virtual - UNIVIDA, en ocasiones pueden ejercer su trabajo desde su casa haciendo uso de sus dispositivos móviles, lo anterior reglamentado a las políticas internas de la entidad.
A.7.1 ANTES DE ASUMIR EL EMPLEO	
A.7.1.1	Antes de realizar la contratación de personal el director de la Unidad Académica Virtual y a Distancia – UNIVIDA se cerciora de que todos los antecedentes del candidato estén en óptimas condiciones para ejercer el cargo.
A.7.1.2	Al momento de la aceptación del empleo por parte del

	candidato se realiza el contrato laboral con términos y condiciones definidos por la Unidad Académica Virtual y a Distancia – UNIVIDA.
A.7.2 DURANTE LA EJECUCIÓN DEL EMPLEO	
A.7.2.3	Se ejecuta un proceso formal que tiene la Unidad Académica Virtual y a Distancia – UNIVIDA, para sancionar al empleado que cometa una violación a la seguridad de la información.
A.7.3 TERMINACIÓN Y CAMBIO DE EMPLEO	
A.7.3.1	En la Unidad Académica Virtual y a Distancia – UNIVIDA, se realiza un acuerdo de confidencialidad al momento de la firma del contrato mediante una cláusula contenida en ésta, de este modo se toma las responsabilidades que debe asumir el exempleado para la protección de la información.
A.8.1 RESPONSABILIDAD DE LOS ACTIVOS	
A.8.1.1	Se mantiene por parte del departamento de GTI (Gestión Tecnológica de la Información), un control sobre el inventario de los equipos existentes de la Unidad Académica Virtual y a Distancia – UNIVIDA, para su posterior modificación en caso que se requiera.
A.8.1.2	Cada equipo que se encuentra en la Unidad Académica Virtual y a Distancia – UNIVIDA, es asignado al empleado encargado que lo requiera y este debe responder por su conservación en buen estado, destacando que su uso debe ser de estricto cumplimiento para su labor.
A.8.2 CLASIFICACIÓN DE LA INFORMACIÓN	
A.8.2.3	Se ha implementado un procedimiento de clasificación de información, para el manejo de los activos de acuerdo a la organización de la Unidad Académica Virtual y a Distancia – UNIVIDA.
A.9.3 RESPONSABILIDAD DE LOS USUARIOS	

A.9.3.1	A cada funcionario se le asigna por medio del gestor de contraseñas una clave personal, el cual se encuentra alineada a los parámetros de una contraseña segura, a su vez se le entrega de manera formal vía correo.
A.9.4 CONTROL DE ACCESO A SISTEMAS Y APLICACIONES	
A.9.4.2	Con respecto al control de acceso al sistema y aplicaciones se encuentra un cumplimiento satisfactorio, dado que mantienen el ingreso a éstos por medio de un sistema de autenticación empleando un login y contraseña.
A.9.4.3	Se cuenta con un sistema de gestión de contraseñas, el cual es generado desde la Coordinación Tecnológica.
A.9.4.5	El acceso a los códigos fuentes de los programas se mantienen restringidos es solo para el personal debidamente autorizado por el departamento encargado.
A.11.2 EQUIPOS	
A.11.2.1	Los equipos se encuentran ubicados de manera adecuada, de manera que permiten salvaguardar la información.
A.11.2.2	Con relación a la protección y regulación de energía en los equipos en la Unidad Académica Virtual y a Distancia – UNIVIDA, cada equipo está asociado a la Ups para la protección en caso de apagones de energía.
A.11.2.3	En lo relacionado al cableado, éste se encuentra debidamente protegido y salvaguardado por canaletas y con las debidas medidas de seguridad pertinente.
A.11.2.4	Se programan revisiones de mantenimiento preventivo y/o correctivo a los equipos de cómputo al finalizar cada semestre.
A.11.2.5	Para cada procedimiento de retiro de equipos se da aviso a la dirección, para que se realice éste de manera formal y se tenga la debida autorización.
A.11.2.6	En la actualidad los equipos de propiedad de la Unidad Académica Virtual y a Distancia – UNIVIDA, no son retirados

	fuera de las instalaciones, pero de hacerlo estos siguen un procedimiento formal y de esta manera se le brinda lineamientos de seguridad para salvaguardar la información contenida en ellos.
A.12.1 PROCEDIMIENTOS OPERACIONALES Y RESPONSABILIDADES	
A.12.1.1.	Los procedimientos operacionales y las responsabilidades se encuentran condensados en el documento del Modelo tecnológico y orientado por la Coordinación Tecnológica.
A.12.1.2	Cuentan con un gestor de cambios en los procesos que se llevan a cabo en los desarrollos de los aplicativos y éstos son almacenados en un repositorio, permitiendo darles un seguimiento a éstos.
A.12.1.3	El seguimiento y las actualizaciones se realizan por el equipo de Gestión de las Tecnologías de la información; así como las actualizaciones y reposiciones de los recursos que se le asignan a los empleados.
A.12.1.4	Las pruebas que se le realizan a los productos software se llevan a cabo bajo entornos controlados por medio del gestor de tareas que se tiene de manera local antes de subirlo a producción.
A.12.2 PROTECCIÓN CONTRA CÓDIGO	
A.12.2.1	La protección contra el código del Campus virtual se maneja de manera regulada mediante la asignación de permisos de acceso a éste por parte de la Coordinación Tecnológica.
A.12.3 COPIAS DE RESPALDO	
A.12.3.1	En lo relacionado a las copias de seguridad son realizadas por el proveedor Good-Daddy, el cual es el encargado de brindar seguridad a la información, lo que se puede decir que es un riesgo que han tercerizado.

A.12.4 REGISTRO Y SEGUIMIENTO	
A.12.4.3	Las actividades del administrador del sistema se encuentran definidas en el gestor de tareas orientado por el Modelo Tecnológico, las cuales son revisadas periódicamente.
A.12.4.4	Se encuentran sincronizados los relojes del sistema y de los equipos como única fuente de referencia de tiempo, frente algún incidente de seguridad.
A.12.5 CONTROL DE SOFTWARE OPERACIONAL	
A.12.5.1	Los controles de instalación de software son monitoreados por el equipo de Gestión de las Tecnologías de la información.
A.12.7 CONSIDERACIONES SOBRE AUDITORÍAS DE SISTEMAS DE INFORMACIÓN	
A.12.7.1	Diariamente se revisan los registros del sistema para evaluar las estrategias que minimicen el riesgo de interrupción y/o instrucción, por parte del departamento de Gestión Tecnológica.
A.13.1. GESTIÓN DE LA SEGURIDAD DE LAS REDES	
A.13.1.2	Se han identificado e implementado mecanismos de seguridad para los servicios de red internos.
A.13.1.3	Se evidencia la separación de las redes, implementados por parte del departamento Gestión Tecnológica, por medio de los diferentes grupos de acceso asignados al personal.
A.13.2 TRANSFERENCIA DE INFORMACIÓN	
A.13.2.1	Se cuenta con controles para la transferencia de información solamente en los equipos internos en lo referente a los protocolos de comunicación.
A.13.2.2	Con relación a los acuerdos de transferencia de información se destaca que existen acuerdos de confidencialidad con el personal externo e interno, para darle tratamiento seguro de la información.
A.13.2.3	El servicio de mensajería se encuentra protegido, por medio

	de las medidas de seguridad que implementa Google, por lo que es un servicio que se ha tercerizado.
A.13.2.4	De manera periódica y de acuerdo a las necesidades de la organización se revisan y se actualizan los acuerdos de confidencialidad que tiene la institución.
A.14.1 REQUISITOS DE SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN	
A.14.1.1	Dentro del proceso de construcción en la etapa del análisis y especificación de los requisitos del desarrollo de una aplicación se tienen en cuenta los requisitos de seguridad, destacando que estos se encuentran concertados por el gestor de tareas.
A.14.1.2	Las aplicaciones se encuentran protegidas por contraseñas para protegerlas de actividades fraudulentas, por lo que se determina que cada aplicación y servicio se encuentran protegidos.
A.14.1.3	Las transacciones de información sobre las aplicaciones se encuentran protegidas por accesos restringidos o no autorizados
A.14.2 SEGURIDAD EN LOS PROCESOS DE DESARROLLO Y DE SOPORTE	
A.14.2.1	Se cuenta con un repositorio de código fuente que su uso lo determinan con política para el desarrollo seguro de las aplicaciones
A.14.2.2	Se cuenta con el sistema de gestión de versiones que les permite realizar un procedimiento formal para realizar los cambios en los sistemas o en desarrollos
A.14.2.3	Antes de salir a producción el coordinador tecnológico se encarga de realizar las pruebas a las aplicaciones para implementarlas al negocio
A.14.2.7	La unidad virtual realiza un seguimiento a las actividades o los productos que son contratados y ejecutados por externos

A.14.2.8	Durante la etapa de desarrollo el coordinador tecnológico se encarga de realizar las pruebas de funcionalidad sobre la seguridad del producto
A.15.1 SEGURIDAD DE LA INFORMACIÓN EN LAS RELACIONES CON LOS PROVEEDORES	
A.15.1.2	A pesar de no tener establecido una política documentada, se cuenta con requisitos de seguridad para los proveedores, aunque estos no tengan acceso a la información de manera directa.
A.15.2 GESTIÓN DE LA PRESTACIÓN DE SERVICIOS DE PROVEEDORES	
A.15.2.2	La unidad académica virtual realiza ajustes- cambios a las cláusulas de los contratos de suministros de servicio teniendo en cuenta la criticidad de la información con el propósito de mitigar los riesgos asociados a ésta.
A.16.1 GESTIÓN DE INCIDENTES Y MEJORAS EN LA SEGURIDAD DE LA INFORMACIÓN	
A.16.1.1	La dirección de unidad establece las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida ante los incidentes que puedan ocurrir de seguridad de la información
A.16.1.2	Los posibles eventos que puedan ocurrir con la seguridad de la información son informados al director rápidamente, mediante un canal de comunicación que es el correo electrónico del mismo.
A.16.1.4	Se evalúan los eventos de seguridad de la información y se clasifican según el riesgo.
A.16.1.5	Se da respuesta oportuna a los incidentes de la seguridad de la información de acuerdo a los procedimientos de la unidad
A.16.1.7	La unidad académica virtual - UNIVIDA, define y aplica procedimientos para identificar, recolectar, adquirir y preservar evidencia que pueda servirles frente a procesos que se

	determinen.
A.17.1 CONTINUIDAD DE LA SEGURIDAD DE LA INFORMACIÓN	
A.17.1.2	La unidad mantiene documentados los procesos y procedimientos para asegurar el nivel de la continuidad que se necesita para la seguridad de la información en una situación adversa
A.17.1.3	La unidad verifica regularmente que se cumplan los controles de continuidad de la seguridad de la información con el fin de asegurarse que son válidos y adecuados.
A.17.2 REDUNDANCIAS	
A.17.2.1	Las instalaciones del procesamiento de información están debidamente implementadas las medidas de redundancia de información para cumplir con los requisitos de disponibilidad.
A.18.1 CUMPLIMIENTO	
A.18.1.1	La documentación legal de la unidad académica virtual - UNIVIDA, se encuentran alineados a los parámetros legales, reglamentarios y contractuales vigentes.

2. NO CONFORMIDADES

No conformidades coordinación tecnológica.

CONTROL **Estándar ISO 27001:2013**	**DESCRIPCIÓN**
A.5.1 ORIENTACIÓN DE LA DIRECCIÓN PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	
A.5.1.1	La oficina de coordinación tecnológica de la Unidad académica Virtual, no cumple con una política definida para la seguridad de la información, la cual debe ser aprobada por la dirección, publicada y comunicada a los empleados y a las personas tanto del sector externo, como a las que

	hacen parte del proceso.
A.5.1.2	Al no tener una política para la seguridad de la información evidentemente no existe la revisión de manera periódica que se debe hacer, por lo cual el dominio en mención no se cumple.
A.6.1 ORGANIZACIÓN INTERNA	
A.6.1.1	Actualmente no hay de manera organizada y definida la asignación de las responsabilidades de la seguridad de la información, dentro de la unidad académica virtual - UNIVIDA.
A.6.1.4	No se mantienen contactos apropiados con grupos, asociaciones o foros de interés especial o asociaciones profesionales especializadas en seguridad.
A.6.1.5	No se establece un equipo de proyectos que haga la gestión y vigilancia independiente de la seguridad de la información.
A.6.2 DISPOSITIVOS MÓVILES Y TELETRABAJO	
A.6.2.1	No se ha implementado una política y/o medidas de seguridad que de soporte para gestionar los riesgos que se puedan presentar al manipular los dispositivos móviles.
A.7.2 DURANTE LA EJECUCIÓN DEL EMPLEO	
A.7.2.1	Con respecto a las responsabilidades que la dirección debe exigir a sus empleados y contratistas en la aplicación de medidas de seguridad de la información No cumplen con esta condición, dado que no cuentan con la política de seguridad de la información.
A.7.2.2	Esta actividad no se ejecuta en su totalidad en la unidad académica virtual - UNIVIDA, de modo que no cumple con la especificación requerida, dado que no se realizan jornadas que permitan tomar conciencia con relación a manejo seguro de la información.

A.8.1 RESPONSABILIDAD DE LOS ACTIVOS	
A.8.1.3	No se ha diseñado un plan de manejo para la información y los activos asociados con información, dado a esto tampoco cuentan con un documento que especifique el uso aceptable de los activos que comprende la unidad académica virtual - UNIVIDA.
A.8.2 CLASIFICACIÓN DE LA INFORMACIÓN	
A.8.2.1	No se clasifica la información de manera adecuada, por legalidad, valores, criticidad y susceptibilidad dentro de la unidad académica virtual - UNIVIDA.
A8.2.2	No se ha desarrollado un procedimiento de manejo de activos que permita el correcto etiquetado de la información dentro de la unidad académica virtual - UNIVIDA.
A.8.3 MANEJO DE MEDIOS	
A.8.3.1	No se mantiene una implementación de gestión de medios removibles para evitar la divulgación, la modificación, el retiro o la destrucción de información almacenada.
A.8.3.2	No existe un procedimiento formal para la disposición final de los diferentes medios de almacenamiento cuando ya no se requieren.
A.8.3.3	Este proceso se encuentra fuera de la aplicabilidad del dominio, ya que los medios de información que se manejan no son transportados para su aseguramiento.
A.9.1 REQUISITOS DEL NEGOCIO PARA EL CONTROL DE ACCESO	
A.9.1.1	No existe una política que controle el acceso en base a los requisitos del negocio y de la seguridad de la información, en la unidad académica virtual - UNIVIDA.
A.9.1.2	Se permite el acceso constante a las redes y a los servicios con autorización general para todo el personal que tiene dicho acceso a la plataforma de la unidad académica

	virtual - UNIVIDA
A.9.2 GESTIÓN DE ACCESO DE USUARIOS	
A.9.2.1	No hay formalizado un procedimiento que registre y/o cancele los registro de los usuarios para posibilitar la nuevas asignaciones con accesos controlados.
A.9.2.2	No se ha implementado un sistema que formalice el proceso de acceso formal de usuarios para asignar o revocar derechos de acceso a los servicios y sistemas.
A.9.2.3	No se controla la asignación y uso de derechos a usuarios con acceso privilegiado al sistema.
A.9.2.4	No se ha formalizado un procedimiento que cumpla con el control de la asignación de información de autenticación secreta.
A.9.2.5	No se revisa en tiempos regulados los activos de información por parte del departamento encargado.
A.9.2.6	No se controla el acceso de los empleados a la información y a las instalaciones del procesamiento de información una vez terminado el empleo.
A.9.4 CONTROL DE ACCESO A SISTEMAS Y APLICACIONES	
A.9.4.1	Al no contar con una política de control de acceso no cumple con el dominio en mención, ya que se basa en restringir el acceso a la información de acuerdo a esta política.
A.9.4.4.	No se restringe el uso de programas utilitarios dentro de la unidad, el cual tienen acceso a proceder a instalar herramientas de manera independiente y sin previa autorización.
A.10.1 CONTROLES CRIPTOGRÁFICOS	
A.10.1.1	No se ha considerado la posibilidad de desarrollar una

	política de uso de controles criptográficos.
A.10.1.2	Al no establecer una política de controles criptográficos no hay manera de desarrollar una misma política para el uso, la protección y tiempo de vida de las llaves criptográficas.
A.11.1 SEGURIDAD FÍSICA Y DEL ENTORNO	
A.11.1.1	No se han establecido las medidas de seguridad física en el perímetro que abarca la unidad académica virtual - UNIVIDA.
A.11.1.2	No se cuenta con un sistema de ingreso de personal apropiado y seguro a las oficinas de la unidad académica virtual y a distancia - UNIVIDA.
A.11.1.3	En este control sólo se establece la seguridad física para el ingreso general a las instalaciones de FUP, pero la unidad virtual se encuentra desprotegida totalmente.
A.11.1.4	No se tienen implementadas las medidas apropiadas para la atención de un desastre natural, ataque o incidentes.
A.11.1.5	No se lleva a cabo un procedimiento para usar en las áreas de trabajo en caso de cualquier incidente relacionado con la seguridad física.
A.11.2 EQUIPOS	
A.11.2.8	Los equipos no cuentan con ninguna medida que pueda permitirle garantizar una seguridad a la información cuando éstos se encuentran desatendidos, como el cierre total de la aplicación cuando ya no se esté utilizando o cuando no se esté trabajando con el equipo.
A.11.2.9	No se ha adoptado una política de escritorios y pantallas limpias, dado a esto la mayoría de los escritorios de los pc cuentan con una gran cantidad de carpetas visibles, así mismo en lo que respecta a los escritorios físicos

	mantienen documentos sobre esto, dejando vulnerable y fácil acceso a la información por parte de una amenaza.
A.12.4 REGISTRO Y SEGUIMIENTO	
A.12.4.1	A pesar de que realizan auditorías a la Unidad Académica Virtual y a distancia – UNIVIDA, éstas no se llevan cabo con criterios enmarcados a la seguridad de la información, dado que solo se realizan es basados con lineamientos de la norma de calidad NTC-ISO 9001
A.12.4.2	No se evidencia una seguridad de las instalaciones ni tampoco de la información estos no se encuentran correctamente protegidos frente alteraciones y/o acceso no autorizados.
A.12.6 GESTIÓN DE LA VULNERABILIDAD TÉCNICA	
A.12.6.1	Esta es una tarea que no se desarrolla propiamente por la coordinación tecnológica, está la lleva a cabo el proveedor y el reporte es alojado en el aplicativo Apache, evidenciándose que no se toman medidas al respecto.
A.12.6.2	No se han implementado medidas que restrinja la instalación de software por parte de los usuarios.
A.13.1 GESTIÓN DE LA SEGURIDAD DE LAS REDES	
A.13.1.1	No se cuenta con una política que establezca que se debe administrar y controlar las redes para proteger la información en sistemas y aplicaciones
A.14.2 REQUISITOS DE SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN	
A.14.2.4	Antes de salir a producción no cuentan con una persona que se encargue de realizar las pruebas a las aplicaciones de manera adecuada.
A.14.2.5	No se cuenta con un documento donde se establezcan los principios para realizar una construcción de sistemas

	seguros.
A.14.2.9	No se cuenta con pruebas de aceptación ante la adquisición de un nuevo sistema de información.
A.14.3 DATOS DE PRUEBA	
A.14.3.1	Los datos de prueba no son seleccionados y tampoco se les brindan la protección en caso que sea necesario, cuando se implementa una nueva plataforma o cambios sobre esta.
A.15.1 SEGURIDAD DE LA INFORMACIÓN EN LAS RELACIONES CON LOS PROVEEDORES	
A.15.1.1	No se cuenta con una política de seguridad de la información que permita mitigar los riesgos asociados a la información guardada en la unidad académica virtual y a distancia UNIVIDA.
A.15.2 GESTIÓN DE LA PRESTACIÓN DE SERVICIOS DE PROVEEDORES	
A.15.2.1	La unidad académica virtual - UNIVIDA, no realiza un seguimiento de forma periódica sobre los servicios prestados por los proveedores
A.16.1 GESTIÓN DE INCIDENTES Y MEJORAS EN LA SEGURIDAD DE LA INFORMACIÓN	
A.16.1.3	En la unidad académica virtual - UNIVIDA, no se exige a los empleados que reporten cualquier novedad o debilidad de la seguridad de la información que detecten.
A.16.1.6	Al no tener gran cantidad de incidentes y el análisis de éstos, no se genera un conocimiento práctico que les brinde mayor capacidad de impacto de incidentes para el futuro.
A.17.1 CONTINUIDAD DE LA SEGURIDAD DE LA INFORMACIÓN	
A.17.1.1	No se tienen claros los requisitos para la seguridad de la información, por ello no cuentan con un plan de

	contingencia y/o continuidad del negocio frente alguna eventualidad.
A.18.1 CUMPLIMIENTO	
A.18.1.2	La unidad no es una productora de software por lo tanto este dominio no tiene aplicabilidad, más sin embargo se producen contenidos asociados con las asignaturas de los programas, de los cuales no se le da el debido proceso con respecto a la propiedad intelectual de éstos.
A.18.1.3	La unidad académica virtual - UNIVIDA, no cuenta con medidas de protección a los registros que se generan, ya que la mayoría de estas medidas lo realizan por medio del proveedor de servicios tercerizado.
A.18.1.4	No se cuenta con una política de protección de datos que permita conocer el tratamiento de éstos, por tanto, en la actualidad no le han dado el debido tratamiento de acuerdo a la legislación vigente establecida en la ley 1581 de 2012.
A.18.1.5	En la unidad académica virtual - UNIVIDA no se han implementados lineamientos con respecto a la utilización de controles criptográficos para el manejo seguro de la información.
A.18.2 REVISIÓN DE SEGURIDAD DE LA INFORMACIÓN	
A.18.2.1	No se ha elaborado un documento donde se establezca revisar independientemente los procesos y procedimientos cuando ocurran cambios significativos en los sistemas de información que contempla la unidad académica virtual - UNIVIDA.
A.18.2.2	Al no haber un documento elaborado como políticas de protección de datos personales se evidencia su incumplimiento con la legislación 1581 de 2012.
A.18.2.3	Al no existir políticas de seguridad de la información no se puede realizar la revisión de manera periódica del mismo.

3. SUGERENCIAS Y/O RECOMENDACIONES

OBSERVACIONES GENERALES

A continuación, se detallan unas sugerencias y/o recomendaciones para la Unidad Virtual Académica y a distancia – UNIVIDA, que podría empezar a implementar como acciones de mejora dentro de sus procesos:

- En lo que respecta a no tener una política de seguridad de la información se le sugiere implementar la herramienta que ofrece SANS a través de sus guías y plantilla, el cual podrían tomarlo como referencia para construir la política de seguridad de la información.

- Se sugiere tener una guía donde establezcan las responsabilidades y funciones con relación a la seguridad de la información, dado a esto pueden tomar como parámetros la guía CCN, así mismo el documento Ernst & Young, quien plantea un enfoque práctico y basado en riesgos del cumplimiento con la segregación de funciones.

Del mismo modo la guía NIST SP800-100 de seguridad de la información para gerentes, permitiendo hacer una mejor gestión en la organización interna de los activos y poder entregar lineamiento que permitan un trabajo seguro aquellos que ejercen el teletrabajo o un acceso remoto a la información de la unidad virtual académica y a distancia- UNIVIDA.

Por otro lado, se recomienda implementar la herramienta Patriot, para la monitorización en tiempo real de cambios en sistemas Windows o ataques de red y monitorizar el uso y acceso de escritorio remoto.

- En cuanto a la seguridad de los recursos humanos se recomienda realizar actividades de capacitación y concientización acerca de manejo seguro de la información, así como también involucrar a la alta dirección para que de esta manera ellos identifiquen la necesidad que se tiene en proteger los activos que

condensan información y por ende tener los recursos para proceder a implementar los controles que determinó el diagnóstico.

- Se requiere que establezcan mediante una metodología de evaluación del riesgo la identificación y clasificación de los activos, para poder darle el tratamiento adecuado a los mismos, por otra parte, en lo que concierne a la gestión de dispositivos removibles se propone que pueden utilizar la herramienta Hardwipe para que realicen un borrado seguro aquellos dispositivos que se vayan a reutilizar.

- Como medida de protección de acceso se recomienda emplear la herramienta User Lock, para proteger el acceso a las redes de Windows, impidiendo las conexiones simultáneas, al dar la posibilidad de limitar las conexiones de los usuarios y proporcionando a los administradores el control remoto de las sesiones, así mismo la solución de código abierta OpenNac, para el control de acceso de red en entornos LAN/WAN, basados en políticas de red.

Por otro lado, para verificar la fortaleza de las contraseñas que utilizan está Jhon de Ripper y/o Password generator, para la generación de contraseñas seguras.

- Se recomienda utilizar la guía de Sans como modelo ejemplo para la redacción de las políticas en cuanto al uso del cifrado, como también la aplicación de la norma OpenPGP como se define en RFC 4880. GnuPG que permite cifrar y firmar datos y comunicación.

- En vista de que la Unidad Académica Virtual y a distancia – UNIVIDA, no cuenta con políticas de seguridad física se recomienda emplear como modelo guía la de SISTESEG, de esta manera empezar a construir la propia, y así poder contar con lineamientos claros con relación a la seguridad de la información, del mismo modo implementar barreras de seguridad física en los pasillos como al interior de las oficinas por ejemplo: sistemas biométricos, circuitos cerrados de televisión , alarmas, que permitan garantizar un trabajo seguro en estos recintos.

En cuanto a la protección de los equipos portátiles se sugiere la herramienta Kensington security slot.

- Como medida de protección en cuanto a las copias de seguridad se sugiere la herramienta Cobian backup, de esta manera minimizan el riesgo de pérdida de la información este se caracteriza por ser un software freeware.

Para la recolección de información de las operaciones realizadas y monitorización la herramienta Snare, podría ser de gran ayuda para la Unidad académica.

La herramienta Insecurity Research, puede ser una solución que podrían implementar para el testeo de software para mitigar, monitorear y gestionar las últimas vulnerabilidades presentadas en seguridad.

- En cuanto a la seguridad en las redes se recomienda revisar el estándar ISO/IEC 18028 y 27033 que está enfocado a la seguridad en las redes, de este modo proteger los canales de comunicación de la Unidad académica virtual y a distancia.

- Teniendo en cuenta que la Unidad académica y a distancia UNIVIDA, brinda servicios online, se propone que implementen la guía de desarrollo de OWASP, el cual les permitirá crear aplicaciones web seguras, y manejando el riesgo de los incidentes posibles a ocurrir.

Por otro lado, se sugiere tener una base de dato y entornos de pruebas, para realizar las diferentes comprobaciones y/o cambios antes que del sistema salga a su entorno de producción.

- Se recomienda incluir dentro de la política de seguridad de la información las responsabilidades que deben tener los terceros en cuanto a la seguridad y buen tratamiento de la información, de esta manera se reducirá los riesgos que estos pueden tener asociado en cuanto a filtración, alteración, eliminación o pérdida de la información.

-Para la gestión de incidencias de seguridad se recomienda el estándar ISO/IEC 27037, quien otorga los lineamientos para la identificación, recopilación, consolidación y preservación de evidencias digitales y para que puedan ser utilizadas con valor probatorio, dado el caso que se requieran.

- En cuanto a los planes de continuidad del negocio en el ámbito de la seguridad se sugieren revisar dos estándares el ISO/IEC 22313:2012, guía para la implantación de sistemas de gestión para la continuidad del negocio e ISO/IEC 27031 quien entrega las directrices para la elaboración del plan.

- Se recomienda revisar las legislaciones relacionadas con la seguridad de la información como la ley 1581 de 2012, quien entrega los lineamientos para construir la política de protección de datos y el decreto 1377 de 2013, que reglamenta la directriz anterior, así mismo establecer una clasificación en cuanto a la información como por ejemplo datos sensibles, secreto, de dominio público en interno condensado en directrices claras y documentadas.

FIRMAS DE RECEPCIÓN DE ESTE INFORME

_____	_____	_____
DIRECTOR	REPRESENTANTE DEL ÁREA	FECHA