RESUMEN – TRABAJO DE GRADO

AUTORES	**CLAUDIA ÁLVAREZ ROMERO** **JULIA BARBOSA LLAÍN** **LEONARDO ZAMBRANO ZAMBRANO**
FACULTAD	**FACULTAD DE INGENIERÍAS**
PLAN DE ESTUDIOS	**ESPECIALIZACION EN AUDITORIA DE SISTEMAS**
DIRECTOR	**ANTÓN GARCÍA BARRETO**
TÍTULO DE LA TESIS	**ANÁLISIS DE RIESGOS INFORMÁTICOS DE LA DEPENDENCIA DIVISIÓN DE SISTEMAS ADSCRITA A LA SUBDIRECCIÓN ACADÉMICA DE LA UFPSO, BASADA EN LA NORMA ISO/IEC 27005:2011**

RESUMEN

PARA LA DIVISIÓN DE SISTEMAS ES DE VITAL IMPORTANCIA GARANTIZAR LA PROTECCIÓN DE LA INFORMACIÓN Y DE TODA LA INFRAESTRUCTURA TECNOLÓGICA QUE LA SOPORTA POR LO QUE SE HACE NECESARIO REALIZAR UN ANÁLISIS DE RIESGOS QUE PERMITA ENCONTRAR AQUELLAS AMENAZAS A LAS QUE SE EXPONE CONTINUAMENTE, BASADO EN LA NORMA ISO/IEC 27005:2011, SE PRESENTA EL ANÁLISIS DE RIESGO DESARROLLADO TENIENDO EN CUENTA CADA UNO DE LOS CRITERIOS PROPUESTOS POR ESTA METODOLOGÍA, ESTABLECIENDO EL CONTEXTO, E IDENTIFICANDO Y VALORANDO CADA UNO DE LOS ACTIVOS ENCONTRADOS DONDE SE PLANTEA EL TRATAMIENTO QUE SE DEBE TENER EN CUENTA EN CADA RIESGO.

CARACTERÍSTICAS

PÁGINAS: 164	PLANOS:	ILUSTRACIONES:	CD-ROM: 1

ANÁLISIS DE RIESGOS INFORMÁTICOS DE LA DEPENDENCIA DIVISIÓN DE SISTEMAS ADSCRITA A LA SUBDIRECCIÓN ACADÉMICA DE LA UFPSO, BASADA EN LA NORMA ISO/IEC 27005:2011

AUTORES

CLAUDIA ÁLVAREZ ROMERO

JULIA BARBOSA LLAÍN

LEONARDO ZAMBRANO ZAMBRANO

Proyecto de grado presentado para optar al título de Especialistas en Auditoría de Sistemas

Director

MSC. ANTÓN GARCÍA BARRETO

UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA

FACULTAD DE INGENIERIAS

ESPECIALIZACIÓN EN AUDITORÍA DE SISTEMAS

Ocaña, Colombia **Octubre de 2016**

Índice

Lista de Tablas

Lista de Figuras

Introducción

Hoy en día es de vital importancia para las empresas contar con tecnología para apoyar sus procesos y estas a su vez están sujetas a una serie de factores o circunstancias que pueden afectar la operatividad de las mismas, como son la probabilidad de filtración de información sensible para fines delictivos, la posibilidad de que la información no sea confiable, el riesgo de no llegar a obtener disponibilidad de la información, perder el servicio por falla tecnológica entre otros. Es por esto que resulta pertinente para las empresas contar con un análisis de riesgos que les permita determinar el nivel de riesgo en que se encuentra cada uno de sus activos.

El presente análisis de riesgos desarrollado en la División de Sistemas de la Universidad Francisco de Paula Santander Ocaña, se basó en el estándar ISO/IEC 27005:2011, estableciendo las directrices que traza la norma para identificar los posibles riesgos sobre sus activos principales.

Este desarrollo permite identificar los activos del proceso, las vulnerabilidades a los que están expuestos, clasificándolos según su nivel de importancia y realizar una evaluación del riesgo según las amenazas y vulnerabilidades detectadas.

Realizando la evaluación del riesgo, se pasa al tratamiento del mismo donde se plasma las vulnerabilidades encontradas, los impactos y las posibles soluciones que deben tomarse para minimizar el nivel del riesgo garantizando aún más las funcionalidades de los procesos y servicios que presta la dependencia.

Capítulo 1. Análisis de riesgos informáticos de la dependencia División de Sistemas adscrita a la sub dirección académica de la UFPSO, basada en la norma ISO/IEC 27005:2011.

1.1 Planteamiento del problema

La seguridad dentro de una organización es una de las principales prioridades que se deben tener en cuenta para realizar seguimientos continuos y así reducir al mínimo la cantidad de fallas que se puedan generar, protegiendo toda la información que en su momento se encuentre vinculada a la División de Sistemas adscrita a la sub dirección académica de la UFPSO, ya que el uso de las tecnologías dentro de las organizaciones se ha ido incrementando para almacenar, mantener, transmitir y recuperar información, también ha aumentado las amenazas que pueden afectar la confidencialidad, disponibilidad e integridad de la misma.

Actualmente dentro del plan de contingencia creado en el año 2010 se contempla un análisis de riesgos el cual no se ha implementado completamente en la División de Sistemas, ya que se realizó de una forma muy general de las situaciones a presentarse, sin enfocarse en una metodología que permita contemplar todos los aspectos proactivos a tenerse en cuenta en dicho lugar, ya que su objetivo primordial es prestar el servicio de sistematización y procesamiento de datos a la UFPSO y con ello a la comunidad y en la que aún se evidencian falencias que ponen en riesgo el objetivo principal de la misma.

Es así que se hace necesario la elaboración de un análisis de riesgos en la División de Sistemas con la finalidad de establecer medidas preventivas y correctivas de seguridad para lograr maximizar las condiciones de disponibilidad e integridad física y lógica de los diferentes procesos que se llevan a cabo dentro de la misma, logrando así minimizar y garantizar el control de los riesgos existentes dentro de la dependencia División de Sistemas.

1.2 Formulación del problema

¿Elaborar un de análisis de riesgos basado en la norma ISO/IEC 27005:2011 a la división de sistemas a la UFPS Ocaña, identificando, valorando y tratando los riesgos, le permitirá minimizar al máximo la probabilidad de ocurrencia de falla y/o daño de sus activos?.

1.3 Objetivos

1.3.1 Objetivo General

Analizar los riesgos informáticos de la dependencia División de Sistemas adscrita a la sub dirección académica de la UFPSO, basada en la norma ISO/IEC 27005:2011.

1.3.2 Objetivos Específicos

Realizar un diagnóstico de la situación real de riesgos informáticos en la que se encuentra la División de Sistemas adscrita a la sub dirección académica de la UFPSO.

Establecer el contexto que permita formular los criterios para el análisis de riesgos correspondientes.

Realizar el análisis de riesgos identificando las amenazas, vulnerabilidades y hallar el nivel de riesgo.

Formular el tratamiento del riesgo basado en el análisis desarrollado.

1.4 Justificación

Hablar de gestión de riesgos se ha manejado desde diferentes concepciones y términos aplicados al tema, algunos desde una perspectiva tradicional y otros en búsqueda de planteamientos innovadores en base a metodologías y herramientas para reducir las vulnerabilidades y mitigación de los mismos.

Actualmente las organizaciones y en este caso la UFPSO se ve expuesta a riesgos informáticos afectando considerablemente la información vital que se aloje en la División de Sistemas, generando pérdidas, atentando contra la confidencialidad y credibilidad la Universidad ante la comunidad que depende de ella; ya que en dicha dependencia no existe un análisis de riesgos basado en una metodología, en este caso el uso de la norma ISO/IEC 27005:2011 permite identificarlos, analizarlos y mitigarlos de tal manera que se garantice una continuidad a los diferentes procesos que en esta área se llevan.

Este análisis pretende establecer aquellos procedimientos, normas y buenas prácticas que garanticen a todo el personal de la dependencia tener al alcance de su mano una herramienta que

les permita tomar aquellas medidas necesarias que minimicen los riesgos dentro de las actividades que realizan.

Siendo la seguridad, un proceso natural y propio del ser humano que vive en comunidad, es necesario actuar y animar las actividades humanas en todos los escenarios de la vida, buscando mitigar todos aquellos riesgos a los cuales se están expuestos; por consiguiente es estrictamente necesario realizar un análisis de riesgos informáticos en la División de Sistemas la cual maneja diariamente información vital; así mismo poder garantizar que las características de esta, como confidencialidad, integridad, disponibilidad, no se vulneren y garantizar la continuidad del funcionamiento de la UFPSO.

1.5 Hipótesis

La identificación por medio del análisis de riesgos informáticos, de la División de Sistemas adscrita a la sub dirección académica de la UFPSO, nos proporcionará resultados eficientes y sustentables, que permitan identificar, minimizar y eliminar los impactos de las amenazas a las que puede estar expuesta la dependencia.

1.6 Delimitaciones

1.6.1 Geográfica. Este estudio se llevará a cabo en la División de Sistemas adscrita a la sud dirección académica de la UFPSO.

1.6.2 Temporal. Este proyecto de investigación tendrá una duración de cuatro meses, desarrollando cada objetivo propuesto, desde Abril de 2016.

1.6.3 Conceptual. Los conceptos que se tendrán en cuenta en esta investigación se apoya en la norma ISO/IEC 27005:2011, y todos aquellos conceptos necesarios para manejar la seguridad de los sistemas informáticos.

1.6.4 Operativo. Esta investigación se realizará en la División de Sistemas adscrita a la sub dirección académica de la UFPSO, específicamente en los sistemas informáticos, existente en el momento y se fundamentará en las normas necesarias para soportar la prevención de todos los riesgos inminentes a los que está expuesta.

Capítulo 2. Marco Referencial

2.1 Antecedentes

Mediante el acuerdo “No. 126 del 9 de Diciembre de 1994, ARTICULO 177. La División de Sistemas es una dependencia adscrita a la Sub dirección académica cuyo objetivo es el de prestar el servicio de sistematización y procesamiento de datos primordialmente a la Universidad y adicionalmente a la comunidad. Tendrá adscritas las Unidades de Procesos Internos y Servicios Externos.

ARTICULO 179. Son funciones generales de la División de Sistemas.

a) Prestar el servicio de sistematización y procesamiento de datos en las áreas académicas, administrativas, financieras e investigativas de la Universidad, para agilización y efectividad de sus procesos internos.

b) Promover y suministrar el servicio de procesamiento de datos a otras entidades o empresas que así lo requieran, mediante el establecimiento de contratos o convenios interinstitucionales.

c) Definir un programa de trabajo en concordancia con las unidades de la Dependencia de tal manera que se garantice el establecimiento de prioridades y procedimientos integrados.

d) Presentar anualmente los requerimientos de reposición, renovación y actualización de equipos y software para la División.

e) Las demás que le señalen los reglamentos de la Universidad (Universidad Francisco de Paula Santander Ocaña, 2014)

2.2 Marco contextual

Este análisis de riesgos se realizará en la División de Sistemas adscrita a la sub dirección académica de la UFPSO, donde se analizará todos los procesos que en esta área se lleven, verificando la seguridad de la información y así identificar los riesgos informáticos a los que se expone.

2.3 Marco conceptual

El análisis de riesgos y su conocimiento contribuyen a los objetivos primordiales de la empresa, por tal motivo implica tener claro ciertos conceptos relacionados con el tema que permitirán tener las herramientas necesarias al vernos inmersos en cualquier situación, a continuación se define de manera clara y sencilla los términos relacionados con el tema.

2.3.1 Datos. "Es cualquier conjunto de caracteres (puede ser un único carácter). Existen tres tipos básicos de datos: Numéricos, alfabéticos y alfanuméricos; Considerando lo anterior, se puede definir la información como un conjunto de datos (numéricos, alfabéticos y alfanuméricos) ordenados con los que se representan convencionalmente hechos, objetos e ideas." (Universidad Nacional del Nordeste , s.f.)

2.3.2 Base de datos. "Las bases de datos son el método preferido para el almacenamiento estructurado de datos. Desde las grandes aplicaciones multiusuario, hasta los teléfonos móviles y las agendas electrónicas utilizan tecnología de bases de datos para asegurar la integridad de los

datos y facilitar la labor tanto de usuarios como de los programadores que las desarrollaron.” (Catalunya, 2008)

2.3.3 Información. “Consiste en la transmisión de los datos obtenidos sensorialmente, a través de un mensaje, desde un transmisor hacia un receptor, en un proceso comunicacional, utilizando el lenguaje oral, escrito o gestual, expuestos de manera sistemática para otorgarles significación, y generar conocimiento.” (De conceptos , s.f.)

2.3.4 Seguridad de la información. La seguridad de la información, según ISO 27001, “consiste en la preservación de su confidencialidad, integridad y disponibilidad, así como de los sistemas implicados en su tratamiento, dentro de una organización. Así pues, estos tres términos constituyen la base sobre la que se cimienta todo el edificio de la seguridad de la información: • Confidencialidad: la información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados.

• Integridad: mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.

• Disponibilidad: acceso y utilización de la información y los sistemas de tratamiento de la misma por parte de los individuos, entidades o procesos autorizados cuando lo requieran.” (NORMA ISO/IEC 27000)NORMA ISO/IEC 27000.

2.3.5 Riesgo. “Es la probabilidad de que suceda algún evento que tendrá un impacto sobre los objetivos de la organización.” (Departamento de la Funcion Publica, s.f.).

2.3.6 Gestión del riesgo. "Aplicación sistemática de políticas, procedimientos y prácticas de gestión para analiza, valorar y evaluar los riesgos." (Salas, 2006)

2.3.7 Valoración del riesgo. "Elemento de control que determina el nivel o grado de exposición de la organización al impacto del riesgo, permitiendo estimar prioridades para su tratamiento mediante la aplicación de acciones tendientes a evitar, reducir, compartir o asumir el riesgo residual." (Departamento Administrativo de Funcion Publica , 2011)

2.3.8 Identificación del riesgo. "Elemento de control que posibilita conocer los eventos potenciales que ponen en riesgo el logro de los objetivos, estableciendo su descripción, agentes generadoras, causas y los efectos de su ocurrencia." (Departamento de Funcion Publica, 2006)

2.3.9 Consecuencia. "Constituyen los efectos de la ocurrencia del riesgo sobre los objetivos de la empresa." (Departamento de Funcion Publica, 2006)

2.3.10 Vulnerabilidad. Son las debilidades que puede tenerse en la organización.

2.3.11 Amenaza. Son aquellos actos que permiten aprovechase de una vulnerabilidad.

2.3.12 Impacto. Consecuencias que puede ocasionar la materialización del riesgo.

2.3.13 Probabilidad. "Una medida (expresada como porcentaje o razón) para estimar la posibilidad de que ocurra un incidente o evento. Contando con registros, puede estimarse a partir

de su frecuencia histórica mediante modelos estadísticos de mayor o menor complejidad." (Copnia, 2012)COPNIA. (2012).

2.3.14 Nivel de riesgo. "Grado de exposición; es el resultado de relacionar la probabilidad con el impacto y con los actuales controles. Medida de la gravedad de riesgos y el proceso de clasificarlos en orden de prioridad. Permite establecer la importancia relativa del riesgo." (Departamento Administrativo de Funcion Publica , 2011)

2.3.15 Evaluación de riesgo. "Es la priorización de los riesgos de acuerdo con el nivel de riesgo asociado a cada uno, con el propósito de discriminar aquellos riesgos que de acuerdo con el nivel de riesgo definido por la Institución no requiere algún plan de acción inmediato." (Copnia, 2012)

2.3.16 Tratamiento de riesgo (Copnia, 2012)**.** "El tratamiento de los riesgos implica, identificar las diferentes opciones para manejar los riesgos. Algunas de esas opciones se representan a continuación:

- Evitar el riesgo
- Reducir la posibilidad de ocurrencia y las consecuencias
- Transferir los riesgos
- Asumir el riesgo"

2.3.17 Control. "Toda acción que tiende a minimizar los riesgos (Copnia, 2012)"

2.3.18 Monitoreo. “Es el proceso sistemático de recolectar, analizar y utilizar información para hacer seguimiento al progreso de un programa en pos de la consecución de sus objetivos, y para guiar las decisiones de gestión.” (Copnia, 2012)

2.3.19 Mitigación. “Planificación y ejecución de medidas dirigidas a reducir o minimizar las vulnerabilidades. (Copnia, 2012)”

2.3.20 Transferir riesgo. “Consiste en una técnica de planificación de la respuesta a los riesgos, con la cual se trasmite el impacto de una amenaza a un tercero, junto con la responsabilidad de la respuesta.” (Copnia, 2012)

2.4 Marco teórico

El hablar de riesgos infiere muchas definiciones que involucran a muchos actores, roles, procesos, etc., dentro de la organización, y es de gran importancia incorporar la gestión de riesgo en el gobierno corporativo, de tal manera que sean analizados y aporten su importancia dentro de las actividades de la empresa.

Es de resaltar que al contar con una o varias herramientas que garanticen una correcta evaluación de los riesgos, se podrán estudiar y analizar de tal manera que estos mismos sean mitigados. A continuación se mencionan aquellas teorías que serán tenidas en cuenta para realizar un correcto análisis de riesgos dentro de la dependencia de la división de Sistemas de la Universidad Francisco de Paula Santander Ocaña.

2.4.1 ISO/IEC 27005:2011 Tecnología de la información, técnicas de la seguridad. Gestión del riesgo de la seguridad de la información

"La norma ISO/IEC 27005:2011 forma parte de la familia ISO 27000 dedicada a la seguridad de la información. Sirve de complemento a las dos primeras normas de la familia (ISO/IEC 27001:2013 e ISO/IEC 27002:2013) que definen la necesidad de elaborar un análisis de riesgos pero no especifican directrices para ello" (27005:201, s.f.)

Esta norma describe los procesos y las actividades para realizar una adecuada gestión del riesgo en la seguridad de la información. Para realizar este procedimiento se contempla realizar lo siguiente:

1. El establecimiento del contexto, en el cual dé se define los objetivos, el alcance, hasta donde llegara el análisis y donde se establecen todos los criterios básicos que se consideran para el análisis de riesgos.
2. La evaluación del riesgo, que contempla la identificación del riesgo, la estimación del riesgo y la evaluación del riesgo. Dentro de la identificación del riesgo se realiza una clasificación de los activos, se estable el nivel de importancia de cada uno de ellos, se identifican las amenazas, se identifican los controles y se identifican las vulnerabilidades y las posibles consecuencias o impactos que se darían en caso de que una amenaza explote una vulnerabilidad. En la estimación del riesgo se define la metodología, los criterios para la valoración de las consecuencias y la valoración de los incidentes. Y en la evaluación del riesgo se analiza cada uno o grupo de activos relacionándolas con las posibles amenazas y vulnerabilidades que poseen

para posteriormente mediante una matriz hallar el nivel de riesgo en que se encuentran cada uno de ellos

3. El tratamiento del riesgo, donde se definen los riesgos encontrados y los controles y/o recomendaciones que deben darse a cada uno de ellos.

4. La aceptación del riesgo, donde se determina si se aceptan o no los riesgos, y se definen las estrategias que deben darse a cada uno de ellos.

5. La comunicación y consulta del riesgo, en donde a partir del tratamiento que se les dé a los riesgos encontrados se comuniquen y consulten.

6. Monitoreo y revisión del riesgo, en donde a partir del tratamiento que se les dé a los riesgos encontrados se les haga el respectivo monitoreo y se revisen.

Esta norma nos proporciona un enfoque sistemático para realizar la gestión de riesgos y dependiendo de la naturaleza del entorno se establecen los criterios necesarios para realizar el análisis respectivo. La gestión de riesgos es una parte fundamental en las actividades de la seguridad de la información y a partir de esta se generan las estrategias para dar cumplimiento a los objetivos de la organización.

La gestión de riesgos en la seguridad de la información es un proceso continuo el cual nos proporciona las herramientas necesarias para revaluar la gestión realizada y garantizar así el estudio de nuevos riesgos y el establecimiento de nuevos criterios según sea el entono en el que se encuentre.

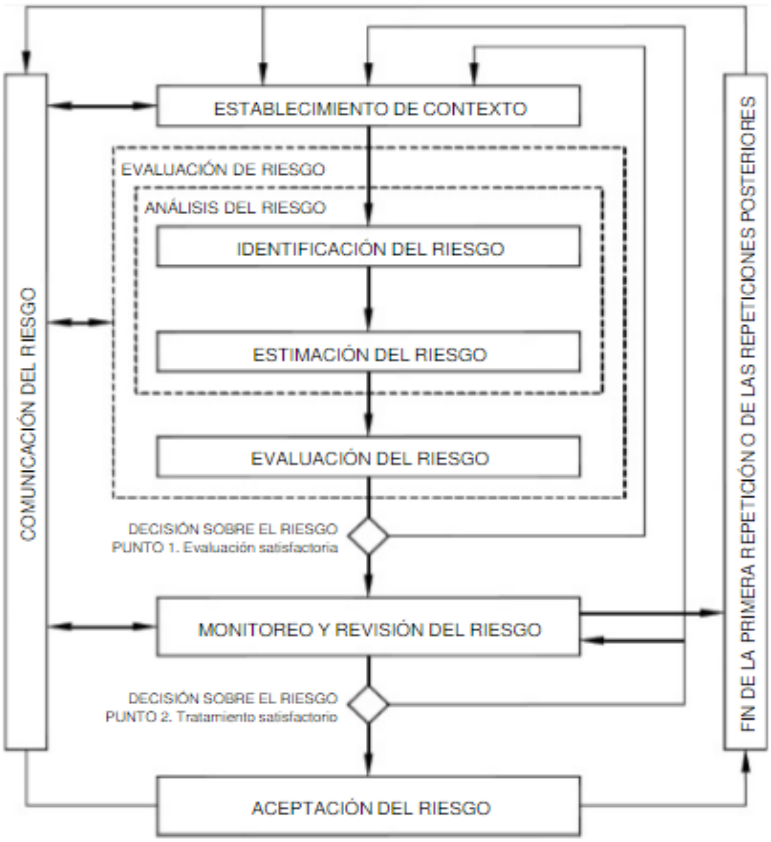


Figura 1: Proceso de gestión del riesgo en la seguridad de la información.

Fuente: http://nsa.wkall.se/litteratur/iso_iec_27005-2011.pdf

2.5 Marco histórico

La información es el activo primordial de una empresa por tal motivo es de gran importancia tener en cuenta aquellos factores que puedan poner en riesgo los objetivos de la organización y de igual manera darles la importancia que estos se merecen.

Para la elaboración de este documento se tomaron en cuenta diferentes proyectos de investigación que cuentan con información de gran relevancia para el análisis de riegos que se

desea llevar en la dependencia de la División de sistemas, a continuación se mencionan los de gran relevancia que fueron encontrados. (Yenis Piedad Osorio Rivero & Yesica Maria Perez Perez, 2014)

Teniendo en cuenta, que la presente propuesta está enfocada en la gestión de riesgos de la información, también se involucran conceptos relacionados con seguridad de la información que consisten en la preservación de la confidencialidad, la integridad y la disponibilidad de la información. (Sandra LIliana Ascanio Sanchez & Yuraima Karina Cardenas Estupiñan , 2013) (Indira del Valle Espinoza Rodriguez & Virginia Carolina Gomez Carvajal, 2009)

Con este análisis se logró identificar las posibles causas que pueden ocasionar lesiones o accidentes de trabajo, para así establecer medidas preventivas e implementar métodos que minimicen los riesgos dentro del departamento obteniendo beneficios como mayor eficacia por parte de los estudiantes y profesores.

2.6 Marco legal

En Colombia desde la expedición de la ley 87 de 1993, se gesta el concepto de riesgos, al establecer como uno de los objetivos del control interno en el artículo 2 literal a) “proteger los recursos de la organización, buscando su adecuada administración ante posibles riesgos que los afectan”. También el literal f) expresa: “definir y aplicar medidas para prevenir los riesgos, detectar y corregir las desviaciones que se presenten en la organización y que puedan afectar el logro de los objetivos”.

Los lineamientos del marco legal relacionados con la gestión del riesgo tienen como base un conjunto de leyes, decretos, resoluciones y normativas que definen y orientan su estudio y aplicación. El riesgo y su gestión se fundamentan en el siguiente marco legal.

El análisis de riesgos puede venir requerido por precepto legal. Tal es el caso de Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica. En el Capítulo II, Principios Básicos, se dice:

Artículo 6. Gestión de la seguridad basada en los riesgos.

1. El análisis y gestión de riesgos será parte esencial del proceso de seguridad y deberá mantenerse permanentemente actualizado.

2. La gestión de riesgos permitirá el mantenimiento de un entorno controlado, minimizando los riesgos hasta niveles aceptables. La reducción de estos niveles se realizará mediante el despliegue de medidas de seguridad, que establecerá un equilibrio entre la naturaleza de los datos y los tratamientos, los riesgos a los que estén expuestos y las medidas de seguridad.

El mismo Real Decreto 3/2010, en el Capítulo III, Requisitos Mínimos, se dice:

Artículo 13. Análisis y gestión de los riesgos.

1. Cada organización que desarrolle e implante sistemas para el tratamiento de la información y las comunicaciones realizará su propia gestión de riesgos.

2. Esta gestión se realizará por medio del análisis y tratamiento de los riesgos a los que está expuesto el sistema. Sin perjuicio de lo dispuesto en el Anexo II, se empleará alguna metodología reconocida internacionalmente.

3. Las medidas adoptadas para mitigar o suprimir los riesgos deberán estar justificadas y, en todo caso, existirá una proporcionalidad entre ellas y los riesgos.

La Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, en su artículo 9 (Seguridad de los datos) dice así:

El responsable del fichero, y, en su caso, el encargado del tratamiento, deberán adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los da-tos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural.

2.6.1 Ley 1273 del 5 de enero de 2009. Delitos informáticos

Por medio de la 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.

2.6.2 Decreto 4485 de 2009

Por el cual se adopta la actualización de la NTCGP a su versión 2009. Numeral 4.1 Requisitos generales literal g) “establecer controles sobre los riesgos identificados y valorados

que puedan afectar la satisfacción del cliente y el logro de los objetivos de la entidad; cuando un riesgo se materializa es necesario tomar acciones correctivas para evitar o disminuir la probabilidad de que vuelva a suceder". Este decreto aclara la importancia de la Administración del riesgo en el Sistema de Gestión de la Calidad en las entidades.

2.6.3 Norma Técnica Colombiana.

(Norma para la "Gestión de Riesgos" NTC 5254 de 2006)

Capítulo 3. Diseño Metodológico

3.1 Tipo de Investigación

El proyecto se fundamenta en una investigación descriptiva que permita según el análisis a realizar presentar las medidas de control y prevención que garanticen mitigar los riesgos que se tienen en la División de Sistemas de la UFPS Ocaña referentes a los sistemas de información.

3.2 Población

La población involucrada estará a cargo del jefe de división de sistemas, siendo éste análisis de riesgos de total interés para todos los funcionarios de la dependencia.

3.3 Muestra

Debido a que el jefe de la división de sistemas es el responsable de todos los procesos, activos, de la información, será a quien se le aplique cada uno de los instrumentos de recolección de información.

3.4 Análisis de la información

Las fuentes de información para este trabajo investigativo se hace a través de la recopilación y análisis de la información que reposan en la dependencia de división de sistemas

de la UFPSO como la documentación de los procesos, formatos, etc. Adicionalmente, acudiremos a la fuente de información, a través de entrevistas, las cuales estarán dirigidas al jefe de la dependencia.

En esta fase se tendrá en cuenta la observación directa sobre la dependencia de división de sistemas.

Capítulo 4. Análisis de riesgos basado en la norma ISO/IEC 27005:2011

4.1 Diagnóstico actual de la dependencia

4.1.1 Descripción de la dependencia división de sistemas

La División de Sistemas, es una dependencia administrativa encargada de la implementación de sistemas de información que estén acorde a solucionar los problemas de información académica y administrativa, soporte técnico del software y hardware de la Universidad, así mismo de la fijación de pautas de desarrollo e implementación de nuevas tecnologías.

4.1.1.1 Generalidades

La división de sistemas es un proceso de apoyo conocido como sistema de información, telecomunicaciones y tecnología (SITT).

4.1.1.2 Objetivo

Diseñar, desarrollar, implementar, administrar y mantener los sistemas de información, las telecomunicaciones y la infraestructura tecnológica; asesorar y gestionar la adquisición e implementación de nuevas tecnologías de información y comunicaciones, que brinden soluciones eficaces, efectivas y oportunas a las necesidades del cliente y partes interesadas, teniendo en

cuenta el uso eficiente de los recursos tecnológicos, minimizando el impacto ambiental y bajo un ambiente laboral propicio para los trabajadores.

4.1.1.3 Objetivos específicos

- Garantizar la permanente gestión de información bajo el uso de los diferentes sistemas de información que hacen parte de la UFPSO.
- Garantizar el correcto funcionamiento de la red de datos, de voz y red inalámbrica para la adecuada comunicación de los usuarios de la UFPSO.
- Mantener el apropiado funcionamiento de la salas de cómputo y demás equipos de oficina tanto de administrativos como de docentes.
- Asegurar el correcto funcionamiento de los servidores de red de la UFPSO.

4.1.1.4 Alcance

Desde la identificación de las necesidades de actualización, modernización y mantenimiento, hasta el aseguramiento en la prestación del servicio de sistemas de información, tecnología y telecomunicaciones.

La División de Sistemas es un proceso de apoyo perteneciente al Sistema de Información Telecomunicaciones y tecnología, de la Universidad Francisco de Paula Santander Ocaña.

4.1.1.5 Funciones

Son Funciones Generales de la División de Sistemas:

- Analizar las necesidades relacionas con las tecnologías de la información en las áreas institucionales (docencia, investigación y servicios administrativos). Contribuyendo con los objetivos, procesos y procedimientos de la Universidad.
- Elaborar planes estratégicos que contemplen las necesidades básicas, para alcanzar objetivos comunes, en beneficio de la Institución.
- Gestionar y mantener aplicaciones orientadas a proporcionar información a la comunidad universitaria.
- Llevar a cabo la función gerencial para el desarrollo de los sistemas de información y telecomunicaciones en la Universidad.
- Adecuar los procedimientos en el uso de los sistemas informáticos y las normas de seguridad vigentes e implantar los medios y las medidas necesarias para ello.
- Asesorar, estudiar e implementar soluciones de equipamiento e infraestructura para la red de voz y la red de datos de la Universidad.
- Responder consultas técnicas, de seguridad y documentar la configuración del sistema.
- Prestar asesoramiento a la comunidad universitaria en la adquisición de equipos y programas informáticos de uso común.
- Velar porque las operaciones efectuadas se apliquen correctamente en los sistemas diseñados para cumplir con las necesidades de la Institución.
- Ofrecer soporte a la institución en la adquisición y uso de tecnologías de informática y de telecomunicaciones como apoyo a la administración, la docencia y la investigación.

- Analizar, evaluar, planear y ejecutar los proyectos que favorecen el desarrollo de la informática y las telecomunicaciones en la universidad de acuerdo con las políticas institucionales establecidas.
- Crear y mantener un sistema de información institucional integral y consistente de apoyo a la toma de decisiones de la dirección Universitaria.
- Asesorar en la utilización de sistemas de información a las diferentes dependencias de la Institución.
- Brindar soporte y contratar el mantenimiento de la infraestructura de redes y servidores, equipo de cómputo, servicios de Internet, sistemas de información y sistemas de comunicaciones.
- Fomentar y velar por el buen funcionamiento de los recursos de servicios de información.
- Velar por el cumplimiento de estándares, normas y leyes de uso de servidores de información.
- Efectuar ajustes sobre los sistemas que están operando de acuerdo a las nuevas necesidades.
- Asesorar a la Universidad sobre aspectos de informática cuando así lo requiere.
- Responder ante el director por el cumplimiento de las actividades del personal de la división de sistemas de la Universidad.
- Responder por el inventario de todos los equipos existentes en la división de sistemas.
- Las demás que le asignen los reglamentos específicos y el director.

4.1.1.6 Roles

Existe un Manual de funciones establecido para la UFPS Ocaña, en la cual para el proceso SITT se evidencia las funciones del Jefe de la División de Sistemas, y de los Profesionales Universitarios; teniendo en cuenta que la mayoría de los funcionarios corresponde a Profesional Universitario pero que no todos realizan las mismas actividades, el proceso de Gestión Humana solicitó describir las funciones para cada uno de los roles que desempeñan dentro del proceso, dichas actualizaciones del documento no se encuentran hasta el momento aprobadas.

A continuación se relacionan las funciones de los cargos que se manejan en la División de sistemas.

Tabla 1:

Identificación del cargo (Jefe división de sistemas).

1. IDENTIFICACION DEL CARGO	
Nivel:	Directivo
Denominación del Empleo:	Jefe de la División de Sistemas
Grado:	Único
Dependencia:	División de Sistemas
Cargo del Jefe inmediato:	Subdirección Académica
Proceso:	Sistema de Información Telecomunicaciones y Tecnología
2. PROPOSITO PRINCIPAL	
Brindar apoyo y asesoría en forma óptima y oportuna a los diferentes sistemas de acuerdo a las políticas institucionales; Orientando los Procesos y recursos administrativos y tecnológicos de la Universidad.	
3. DESCRIPCION DE FUNCIONES	
➢ Analizar las necesidades relacionas con las tecnologías de la información en las áreas institucionales (docencia, investigación, servicios administrativos). Contribuyendo con los objetivos, procesos y procedimientos de la Universidad. ➢ Elaborar planes estratégicos que contemplen las necesidades básicas, para alcanzar objetivos comunes, en	

beneficio de la Institución.

- Asignar objetivos a las distintas divisiones, seguir el desarrollo de proyecto y actividades, controlar los resultados en materia informática y de telecomunicaciones.
- Gestionar y mantener aplicaciones orientadas a proporcionar información a la comunidad universitaria
- Llevar a cabo la función gerencial para el desarrollo de los sistemas de información y telecomunicaciones en la Universidad.
- Adecuar los procedimientos en el uso de los sistemas informáticos y las normas de seguridad vigentes e implantar los medios y las medidas necesarias para ello.
- Asesorar, estudiar e implementar soluciones de equipamiento e infraestructura para la red de voz de datos de la Universidad.
- Responder consultas técnicas, de seguridad y documentar la configuración del sistema.
- Prestar asesoramiento a la comunidad universitaria en la adquisición de equipos y programas informáticos de uso común.
- Velar porque las operaciones efectuadas se apliquen correctamente en los sistemas diseñados para cumplir con las necesidades de la Institución.
- Ofrecer soporte a la institución en la adquisición y uso de tecnologías de informática y de telecomunicaciones como apoyo a la administración, la docencia y la investigación
- Analizar, evaluar, planear y ejecutar los proyectos que favorecen el desarrollo de la informática y las telecomunicaciones en la universidad de acuerdo con las políticas institucionales establecidas.
- Crear y mantener un sistema de información institucional integral y consistente de apoyo a la toma de decisiones de la dirección Universitaria.
- Asesorar en la utilización de sistemas de información a las diferentes dependencias de la Institución.
- Socializar y capacitar a los usuarios en el uso de los servidores de información.
- Brindar soporte y contratar el mantenimiento de la infraestructura de redes y servidores, equipo de cómputo, servicios de Internet, sistemas de información y sistemas de comunicaciones.
- Fomentar y velar por el buen funcionamiento de los recursos de servicios de información.
- Velar por el cumplimiento de estándares, normas y leyes de uso de servidores de información.
- Efectuar ajustes sobre los sistemas que están operando de acuerdo a las nuevas necesidades.
- Asesorar a la Universidad sobre aspectos de informática cuando así lo requiere.
- Responder por el inventario de todos los equipos existentes en la división de sistemas.
- Las demás que le asignen los reglamentos específicos y el director.

Nota Fuente: https://ufpso.edu.co/ftp/pdf/manuales/gh/M-GH-DRH-001BII.pdf

Tabla 2:

Identificación del cargo (profesional universitario).

1. IDENTIFICACION DEL CARGO	
Nivel:	Profesional
Denominación del Empleo:	Profesional Universitario
Grado:	Único
Dependencia:	División de Sistemas
Cargo del Jefe inmediato:	Jefe de la División de Sistemas
Proceso:	Sistema de Información Telecomunicaciones y Tecnología
2. PROPOSITO PRINCIPAL	
Coordinar, apoyar y asesorar la gestión institucional aplicando los conocimientos propios de cualquier carrera profesional reconocida por la Ley, que requieren capacidad de análisis y de proyección, para preparar, elaborar y desarrollar Planes, Programas y Proyectos.	
3. DESCRIPCION DE FUNCIONES	
➢ Aplicar conocimientos, principios y técnicas de la formación profesional, para generar nuevos programas y/o servicios. ➢ Analizar, proyectar, perfeccionar y recomendar las acciones que deban adoptarse para el logro de los objetivos y las metas de la Universidad a través de la dependencia asignada. ➢ Participar en el diseño, la organización, la coordinación, la ejecución y el control de Planes, programas y proyectos o actividades de la oficina: y garantizar la correcta aplicación de las normas y de los procedimientos vigentes. ➢ Realizar estudios y análisis con el fin de elaborar, perfeccionar, controlar y/o desarrollar procedimientos. ➢ Proponer el diseño y la formulación de procedimientos y sistemas atinentes a las áreas de desempeño, con miras a optimizar la utilización de los recursos disponibles. ➢ Brindar asesoría en el área de desempeño, de acuerdo con las políticas y las disposiciones vigentes sobre la materia y vigilar el cumplimiento de las mismas por parte de los usuarios. ➢ Promover y tramitar asuntos de diferente índole en representación de la Universidad, por delegación de autoridad competente; realizar los estudios y preparar los informes respectivos de acuerdo con las instrucciones recibidas. ➢ Analizar, revisar, controlar y evaluar los sistemas y los procedimientos, para garantizar su efectividad. ➢ Absolver consultas sobre la materia competencia de la oficina, de acuerdo con las disposiciones y las políticas institucionales. ➢ Preparar y presentar los informes sobre las actividades desarrolladas, con la oportunidad y la periodicidad requeridas.	

➢ Planear, organizar, dirigir, ejecutar, controlar y evaluar con eficiencia el desarrollo de los proyectos y las actividades propias de su trabajo. ➢ Participar con su labor diaria en la misión, visión, objetivos, políticas, propósitos y principios de la Universidad. ➢ Coordinar y participar directamente en actividades referentes a sus responsabilidades y desempeño de sus funciones, con el desempeño y funciones de los otros cargos o entidades internas y/o externas, relacionadas con el desarrollo de su labor de manera efectiva. ➢ Desempeñar las demás funciones asignadas por la autoridad competente de acuerdo con el nivel, la naturaleza y el área de desempeño.

Nota Fuente: https://ufpso.edu.co/ftp/pdf/manuales/gh/M-GH-DRH-001BII.pdf.

4.1.1.7 Revisión documental

Mediante la exploración, observación e investigación documental, se pudo constatar que la división de sistemas cuenta con una serie de instrumentos los cuales se enunciarán a continuación:

- **Política.** Política de seguridad de la información (Aprobadas, según resolución No. 0118 de Abril 22 de 2015).
- **Procedimientos**

R-TT-DSS-001 – Procedimiento soporte y atención al usuario.

R-TT-DSS-002 – Procedimiento administración de los recursos informáticos.

R-TT-DSS-001 – Procedimiento gestión de los sistemas de TI.

- **Instructivos**

I-TT-DSS-001 – Instructivo servicio técnico y tecnológico.

I-TT-DSS-002 – Instructivo gestión de la configuración.

I-TT-DSS-001 – Instructivo parametrización de los sistemas informáticos.

- **Manuales**

M-TT-DSS-001 – Manual de usuario (SIF) – módulo contabilidad cxp.

M-TT-DSS-002 – Manual de usuario (SIF) – módulo almacén cxp.

M-TT-DSS-009 – Manual de usuario (SIB) – administración módulo de circulación .

M-TT-DSS-010 – Manual de usuario (SIB) – módulo jefe.

M-TT-DSS-028 – Manual especifico proceso de sistemas de información, telecomunicaciones y tecnología.

- **Formatos**

F-TT-DSS-004 - Formato administración de usuarios de los sistemas de información.

F-TT-DSS-005 - Formato administración de usuarios en la bd.

F-TT-DSS-006 - Formato ficha técnica de cámaras.

F-TT-DSS-007 - Formato control de préstamo de salas.

F-TT-DSS-008 - Formato bitácora manejo de errores sitt.

F-TT-DSS-010 - Formato entrega de carnés.

F-TT-DSS-012 - Formato ficha técnica de servidores.

F-TT-DSS-013 - Formato ficha técnica de redes.

F-TT-DSS-014 - Formato bitácora de monitoreo a servidores.

F-TT-DSS-017 - Formato ficha técnica de software.

F-TT-DSS-018 - Formato inventario de telecomunicaciones.

F-TT-DSS-019 - Formato infraestructura de red.

F-TT-DSS-021 - Formato levantamiento de información.

F-TT-DSS-022 - Formato diagrama de flujo.

F-TT-DSS-023 - Formato modelo de datos.

F-TT-DSS-024 - Formato diseño preliminar de software.

F-TT-DSS-025 - Formato ficha técnica de SI.

F-TT-DSS-026 - Formato control de capacitación al usuario.

F-TT-DSS-027 - Formato registro de creación de diplomados, talleres, cursos o seminarios de programa de educación continuada.

F-TT-DSS-035 - Formato bitácora de monitoreo de cámaras.

F-TT-DSS-039 - Formato inscripción para capacitación.

F-TT-DSS-040 - Formato mantenimiento correctivo de servidores.

F-TT-DSS-042 - Formato de registro acceso a sala de servidores.

- **Otros**

L-TT-DSS-001 – Plan de mantenimiento preventivo y correctivo de equipos tecnológicos.

L-TT-DSS-002 – Plan de contingencia de TI.

Documento borrador del Plan de Continuidad.

4.1.2 Infraestructura física de la división de sistemas

La división de sistemas es el nodo principal de la infraestructura que soporta los diferentes servicios de la universidad. La división de sistemas tiene un área de 24 m^2 aproximadamente, tiene un área de servidores, un área de desarrollo y un cuarto de telecomunicaciones donde se encuentran 2 rack uno para la parte telefónica y otro para la red de datos, también se encuentran 5 UPS como respaldo a las fallas eléctricas que se presentan, cuenta con un cableado estructurado en categoría 5e, 4 aires acondicionados, iluminación adecuada y la cubierta del techo en eternit y machimbre.

4.1.3 Infraestructura tecnológica

La infraestructura tecnológica es la base primordial de cualquier empresa y permite la optimización de sus recursos, el aumento del valor de su empresa y una respuesta más rápida a los requerimientos existentes en el día a día.

4.1.3.1 Tipo y topología de red

La Universidad Francisco de Paula Santander Ocaña en su Campus Universitario localizado en la sede el algodonal vía la granja, cuenta con una red LAN, en la cual se extiende un Backbone (Cableado principal de transporte de datos) en fibra óptica con topología estrella extendida, que interconecta el centro de cableado principal ubicado en el edificio División de Sistemas con los demás edificios localmente dispersos mediante Switches.

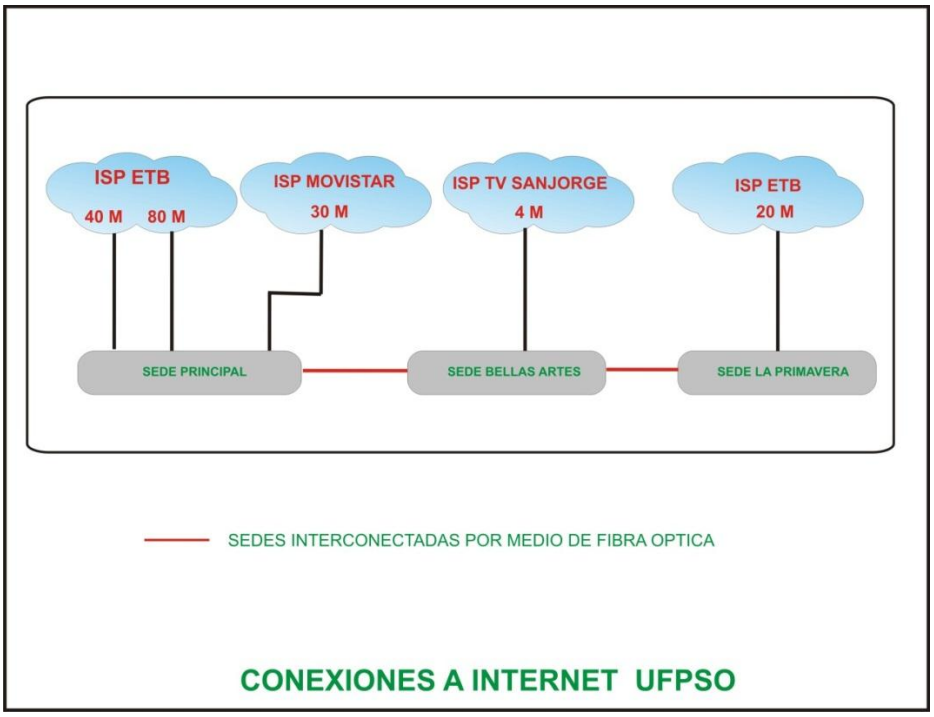


Figura 2: Conexiones a Internet UFPSO.

Fuente: División de sistemas - UFPSO.

La Universidad cuenta con cuatro canales de Internet dedicados, distribuido tal como se muestra en la figura 2. 60 E1 (120 Mbps), en la sede principal; 15 E1 (30Mbps), en la sede principal; 2 E1 (4 Mbps), en la escuela de bellas artes y 10 E1 (20Mbps), en la sede la primavera. Para la sede principal la Universidad adquirió una antena para recibir y transmitir vía microondas, la cual tiene línea de vista con las antenas de propiedad del grupo ISA (a través de su filian INTERNEXA), que permite conectarse a la fibra óptica nacional y a su vez a través del cable submarino arcos.

Las sedes de la primavera y escuela bellas artes se encuentran intercomunicadas con la sede algodonal por medio de fibra óptica.

- Edificio de la sede primavera (conectado por medio de fibra óptica).
- Edificio escuela de bellas artes (conectado por medio de fibra óptica).
- Edificio de división de sistemas (nodo principal).
- Edificio sala de cómputo (conectado por medio de fibra óptica).
- Edificio anexos académicos (conectado por medio de fibra óptica).
- Edificio la granja (conectado por vía inalámbrica).
- Edificio de aulas (conectado por medio de fibra óptica).

En cada una de las sedes y edificios se encuentran conectadas todas las dependencias, las cuales cuentan con características técnicas que permiten una fácil conexión al medio de transmisión, como son los Switch, Access Point, Fibra Óptica y Cableado Estructurado UTP categoría 7A. Para la interconexión de las dependencias y puestos de trabajo cuentan con 1600 puntos de red cableados (intranet), 155 puntos telefónicos analógicos y 120 teléfonos IP.

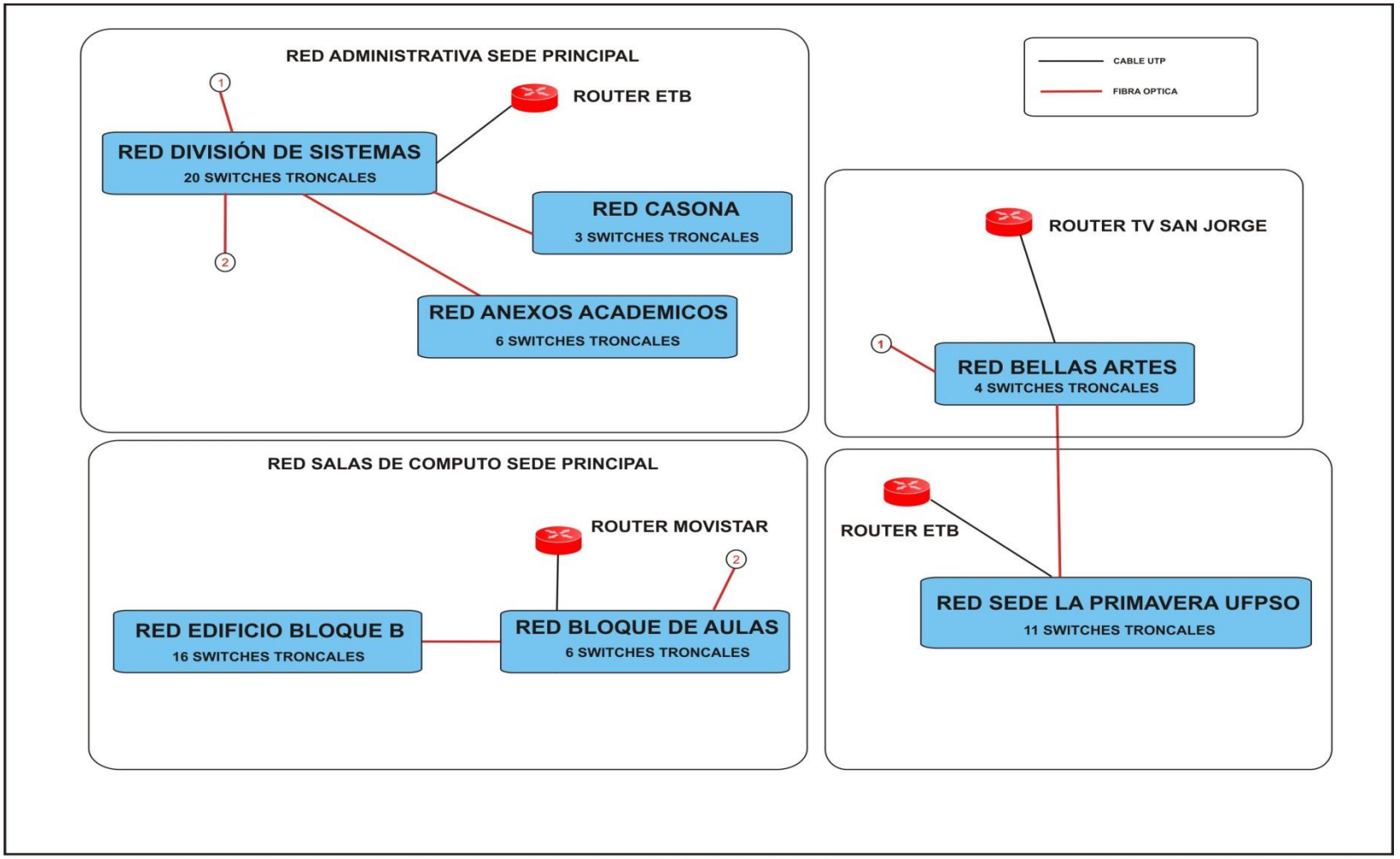


Figura 3: Diagrama de interconectividad de las sedes.

Fuente: División de sistemas – UFPSO.

Como se muestra en la figura 3, la red de la UFPSO, está conformada por la conexión de las tres sedes, todas estas con tecnologías de Switches HP de última generación con capacidad de trabajo y funcionalidades de capa 2; el Switch CORE, de la red es un Switch HP V1910 de 24 puertos que está ubicado en la división de sistemas, la interconexión con las sedes se hace a través de Transceivers de fibra óptica de 1 Gbps. Se cuenta con un CORE de Switch de 66 en su totalidad, los cuales configurados por medio de Vlans se distribuye los diferentes tráficos que se generan por los servidores que se alojan en la división de sistemas.

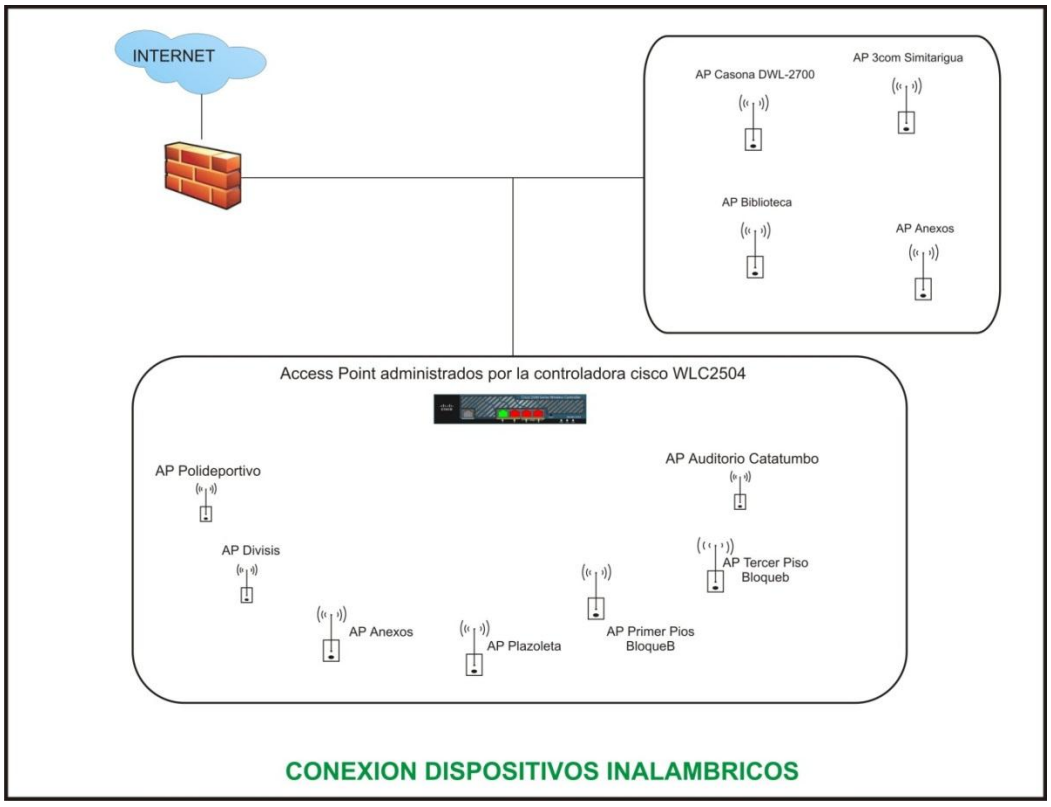


Figura 4: Diagrama de conexión de dispositivos inalámbricos.

Fuente: División de sistemas – UFPSO.

La red inalámbrica de la Universidad como se muestra en la figura 4, está soportada por nuevas tecnologías que permiten dar disponibilidad de conexión a los diferentes usuarios que la utilicen. Actualmente una parte de esta red está administrada por una controladora CISCO y los demás son puntos de acceso están independientes; a continuación se muestra los dispositivos con que esta red cuenta.

Tabla 3:

Dispositivos inalámbricos.

Núm.	CARACTERÍSTICA	CANTIDAD	OBSERVACIÓN
1	Controladora cisco WLC2504	1	Dispositivo para la gestión de los Access Point AIR-CAP1702I-A-K9
2	Access Point AIR-CAP1702I-A-K9	7	Dispositivos administrador por la controladora WLC2504
3	Access Point TP-Link WR743DN	1	Dispositivo en la división de sistemas
4	Access Point cisco WAP4410N	6	Dispositivo en los anexos académicos, auditorio casona, plan de estudios de comunicación social, auditorio simitarigua, ventanilla única y observatorio
5	Access Point Dlink DWL-2700	1	Casona
6	Access Point Nano loco 2	1	Biblioteca
7	Access Point Cisco RV110W	1	Catedráticos

Nota Fuente: División de sistemas – UFPSO.

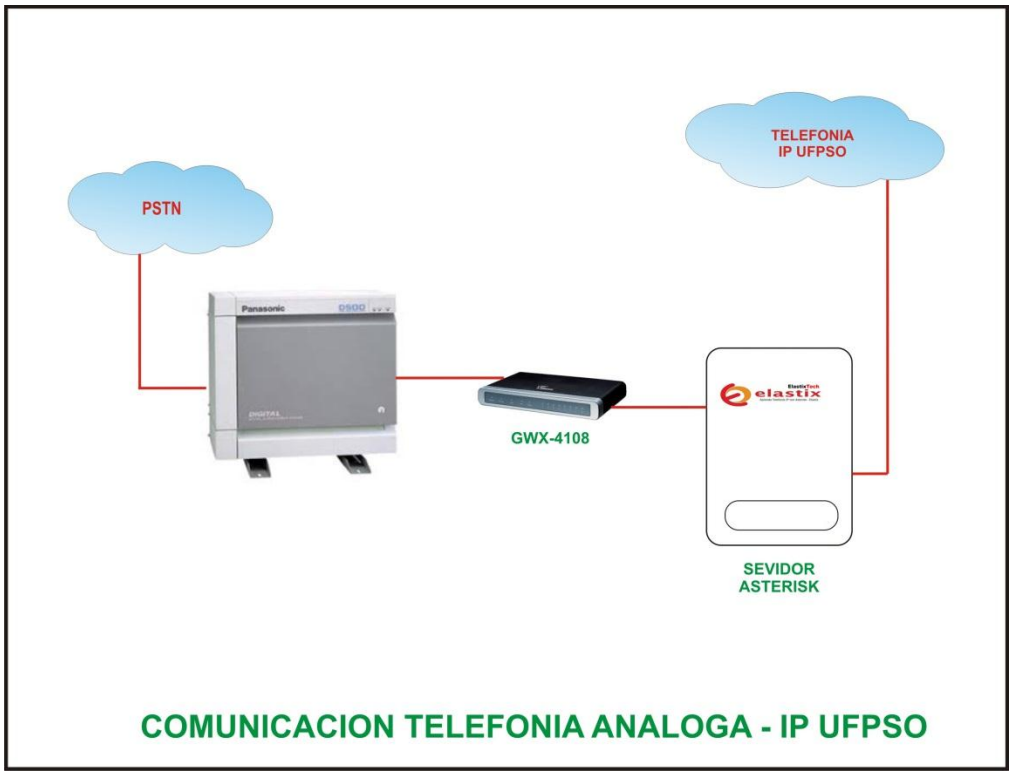


Figura 5: Comunicación telefonía análoga IP UFPSO.

Fuente: Autores del proyecto.

La Universidad actualmente cuenta con un módulo de la central telefónica KX-TD500 Panasonic de la cual se tienen 155 teléfonos análogos. A esta central convergen las 11 líneas troncales que nos provee telefónica Movistar, de las cuales 6 de estas están en un PBX y las restantes se distribuyen a las dependencias principales (dos en dirección, subdirección académica, sub dirección administrativa y división de sistemas). Viendo la limitación de esta planta se desarrolló la implementación de una central IP, como se muestra en la figura 5. Este desarrollo buscó integrar la telefonía análoga con la telefonía IP por medio de un Gateway GWX-4108, utilizando como troncales 4 extensiones análogas hasta el momento y haciendo las configuraciones respectivas para lograr esta comunicación.

- Infraestructura de video vigilancia por IP.

La división de sistemas en busca de salvaguardar la seguridad en las áreas principales ha implementado la video vigilancia por IP, utilizando dispositivos DNR 322L DLINK, distribuyendo las cámaras de la siguiente manera. 28 cámaras IP dos por cada sala de cómputo, 2 cámaras IP de exteriores en la Universidad, 10 cámaras IP en la biblioteca, 7 cámaras IP en el restaurante universitario, 2 cámaras IP en la emisora UFM, 4 cámaras IP en el laboratorio de física, 7 cámaras IP en el consultorio jurídico y sala de audiencias, 2 cámaras IP en el centro de idiomas, 3 cámaras IP en la escuela de bellas artes, 1 cámara IP en la división de sistemas y 1 cámara IP en la sala de catedráticos.

4.1.3.2 Inventario de Hardware

4.1.3.2.1 Equipos de trabajo de división de sistemas

Tabla 4:

Equipos de trabajo de división de sistemas.

Equipo de Trabajo División de Sistemas	
Sistema operativo	Windows 7 64 bits
Procesador	Intel(R) Core(TM) i3 540 @ 3.07GHz,
Memoria	4Gigas
Disco Duro	500 Gigas
Cantidad	14

Nota Fuente: División de sistemas – UFPSO.

4.1.3.2.2 Equipos servidores

Tabla 5:

Servidor físico 01.

Servidor Físico – SF01	
Característica	HP ProLiant DL380G5
Sistema operativo	GNU - Linux
Procesador	Intel® Xeon® CPU E5430 @ 2.66GHz, 4 cores
Memoria	4Gigas
Disco Duro	4 DD c/u de 146 GB – SAS
Cantidad	1

Nota Fuente: División de sistemas – UFPSO.

Tabla 6:

Servidor físico 02.

Servidor Físico – SF02	
Característica	HP ProLiant DL380e G8
Sistema operativo	VMware ESXi – 6.0
Procesador	Intel(R) Xeon(R) CPU E5-24070 @ 2.20GHz,
Memoria	24 Gigas
Disco Duro	6 DD c/u de 1 TB – SATA
Cantidad	1

Nota Fuente: División de sistemas – UFPSO.

Tabla 7:

Servidor físico 03.

Servidor Físico – SF03	
Característica	HP ProLiant DL380e G8
Sistema operativo	VMware ESXi – 5.0
Procesador	Intel(R) Xeon(R) CPU E5-24070 @ 2.20GHz,
Memoria	24 Gigas
Disco Duro	8 DD c/u de 500 GB – SATA
Cantidad	1

Nota Fuente: División de sistemas – UFPSO.

Tabla 8:

Servidores físicos 04 y 05.

Servidor Físico – SF04 y SF05	
Característica	HP ProLiant DL380p G8
Sistema operativo	VMware ESXi – 6.0
Procesador	Intel(R) Xeon(R) CPU E5-2630 @ 2.30 GHz,
Memoria	64 Gigas
Disco Duro	8 DD c/u de 1 TB – SATA
Cantidad	2

Nota Fuente: División de sistemas – UFPSO.

Tabla 9:

Servidor físico 06.

Servidor Físico – SF06	
Característica	HP ProLiant DL380 G9
Sistema operativo	VMware ESXi – 6.0
Procesador	Intel™ Xeon™ CPU E5-2640 v3 @ 2.60GHz,
Memoria	64 Gigas
Disco Duro	2 DD c/u de 1 TB – SATA
Cantidad	1

Nota Fuente: División de sistemas – UFPSO.

Tabla 10:

Servidor físico 07.

Servidor Físico – SF07	
Característica	HP ProLiant DL385 G7
Sistema operativo	GNU - Linux
Procesador	AMD Opteron™ Processor 6172, 12 cores
Memoria	16 Gigas
Disco Duro	4 DD c/u de 600 GB – SAS
Cantidad	1

Nota Fuente: División de sistemas – UFPSO.

Tabla 11:

Servidor físico 08.

Servidor Físico – SF08	
Característica	HP ProLiant DL385 G7
Sistema operativo	GNU - Linux
Procesador	AMD Opteron™ Processor 6172, 12 cores
Memoria	16 Gigas
Disco Duro	4 DD c/u de 600 GB – SAS
Cantidad	1

Nota Fuente: División de sistemas – UFPSO.

Tabla 12:

Servidor físico 09.

Servidor Físico – SF09	
Característica	Equipo Clon
Sistema operativo	GNU - Linux
Procesador	Intel™ Core™2 Duo CPU E7500 @ 2.93GHz, 2 cores
Memoria	8 Gigas
Disco Duro	1 DD c/u de 320 GB – SATA
Cantidad	1

Nota Fuente: División de sistemas – UFPSO.

Tabla 13:

Servidores físicos 10, 11 y 12.

Servidores Físicos SF10 – SF11 y SF12	
Característica	Equipos Clones
Sistema operativo	GNU - Linux
Procesador	Intel™ Core™ i3 CPU 540 @ 3.07GHz, 4 cores
Memoria	4 Gigas
Disco Duro	1 DD c/u de 500 GB – SATA
Cantidad	3

Nota Fuente: División de sistemas – UFPSO.

Tabla 14:

Servidor físico 13.

Servidor Físico – SF13	
Característica	Equipo Clon
Sistema operativo	GNU - Linux
Procesador	Intel™ Core™ i3 CPU 540 @ 3.07GHz, 4 cores
Memoria	4 Gigas
Disco Duro	1 DD c/u de 500 GB – SATA
Cantidad	1

Nota Fuente: División de sistemas – UFPSO.

Tabla 15:

Servidor físico 14.

Servidor Físico – SF14	
Característica	Equipo Clon
Sistema operativo	GNU - Linux
Procesador	Intel™ Core™ i3 CPU 540 @ 3.07GHz, 4 cores
Memoria	4 Gigas
Disco Duro	1 DD c/u de 200 GB – SATA
Cantidad	1

Nota Fuente: División de sistemas – UFPSO.

Tabla 16:

Servidor físico 15.

Equipo Servidores – SF15	
Característica	Sistema de cómputo unificado - UCS Cisco Mini 5108
Blades	3 Blades UCS B200 M4
Memoria	64 Gigas por Cada Blade
Cantidad	1

Nota Fuente: División de sistemas – UFPSO.

4.1.3.2.3 Equipos de almacenamiento

Tabla 17:

Equipo para almacenamiento SAN 1.

Equipo de Almacenamiento Para servidores # 1	
Característica	SAN HP 2000
Disco Duro	16 DD c/u de 600 GB – SAS y 6 DD SAS-MDL 1TB
Cantidad	1

Nota Fuente: División de sistemas – UFPSO.

Tabla 18:

Equipo para almacenamiento SAN 2.

Equipo de Almacenamiento Para servidores # 2	
Característica	SAN HP MSA 2040
Disco Duro	18 Discos duros de 900 GB SAS 6 Discos duros de 2TB SAS MDL
Cantidad	1

Nota Fuente: División de sistemas – UFPSO.

Tabla 19:

Equipo de almacenamiento de imágenes.

Equipo de Almacenamiento de Imágenes	
Característica	DNR 322L DLINK
Cantidad	6
Cámaras	DCS-7010L

Nota Fuente: División de sistemas – UFPSO.

4.1.3.2.4 Equipos de comunicación red de datos

Tabla 20:

Switches de servidores.

Equipo de Comunicación Switch de Fibra Para servidores	
Característica	HP StorasWork 8/8 SAN Switch
Cantidad	2

Nota Fuente: División de sistemas – UFPSO.

Tabla 21:

Core de Switches de acceso.

Equipo de Comunicación Switch de Acceso			
Característica	Switch HP V1910 de 24 puertos.	**Cantidad**	66

Nota Fuente: División de sistemas – UFPSO.

4.1.3.2.5 Equipos de comunicación red de voz

Tabla 22:

Equipos de comunicación de telefonía.

Equipo de Comunicación Voz	
Característica	Central Panasonic KX-TD500
Cantidad	1 módulo.
Característica	Gateway GXW 4108 GrandStream
Función Gateway	Interconectar la telefonía análoga con la telefonía IP Servidor No

Nota Fuente: División de sistemas – UFPSO.

4.1.3.2.6 Equipos de respaldo de energía

Tabla 23:

Equipos de respaldo de energía.

Equipo de respaldo de energía	
Característica	UPS TITAN 10 K
Cantidad	1
Característica	UPS TITAN 6 K
Cantidad	1
Característica	UPS APC 1 K
Cantidad	2
Característica	UPS TRIPP-LITE
Cantidad	1

Nota Fuente: División de sistemas – UFPSO.

4.1.4 Plataforma tecnológica división de sistemas

4.1.4.1 Sistema de alta disponibilidad SAD 1

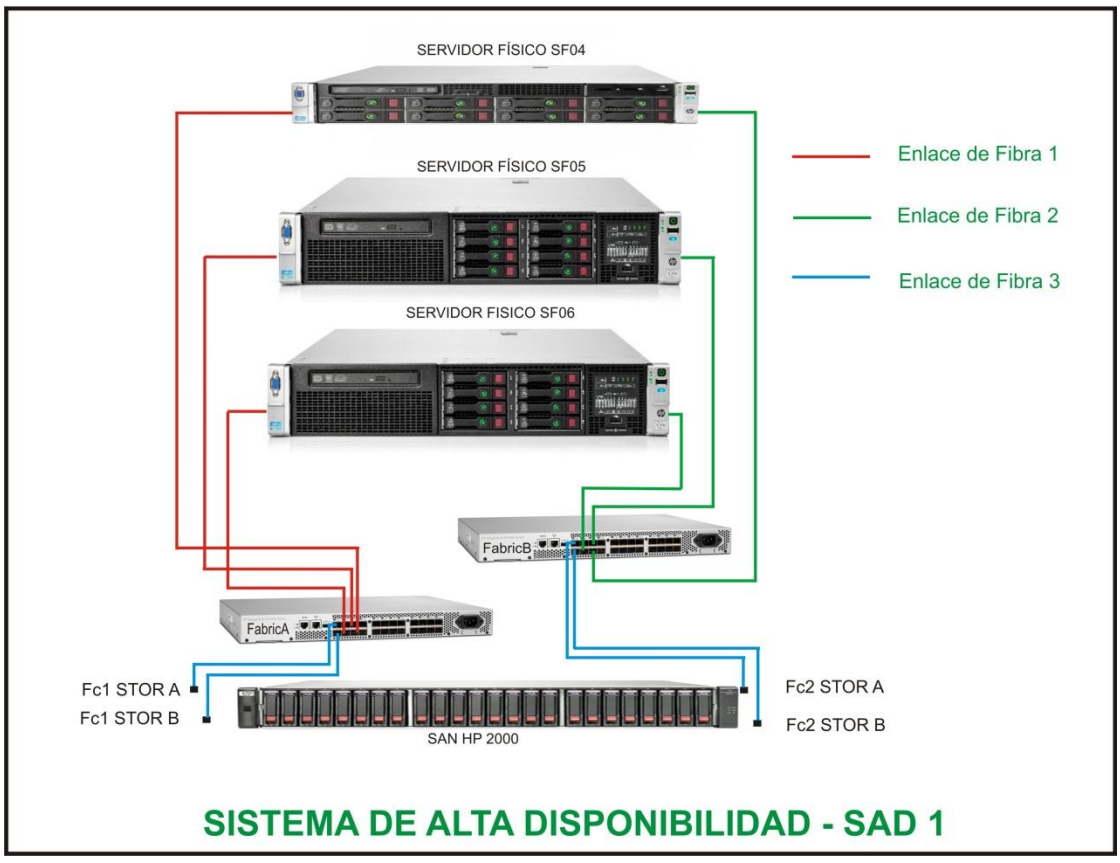


Figura 6: Sistema de alta disponibilidad SAD 1.

Fuente: División de sistemas – UFPSO.

En la figura 6, se observa la interconectividad de los servidores administrados por vCenter, software que permite gestionar cada una de las máquinas virtuales que se encuentran configuradas.

"VMware vCenter, suministra una plataforma centralizada para administrar los entornos de VMware vSphere para automatizar y suministrar una infraestructura virtual de confianza" (VMware, s.f.)

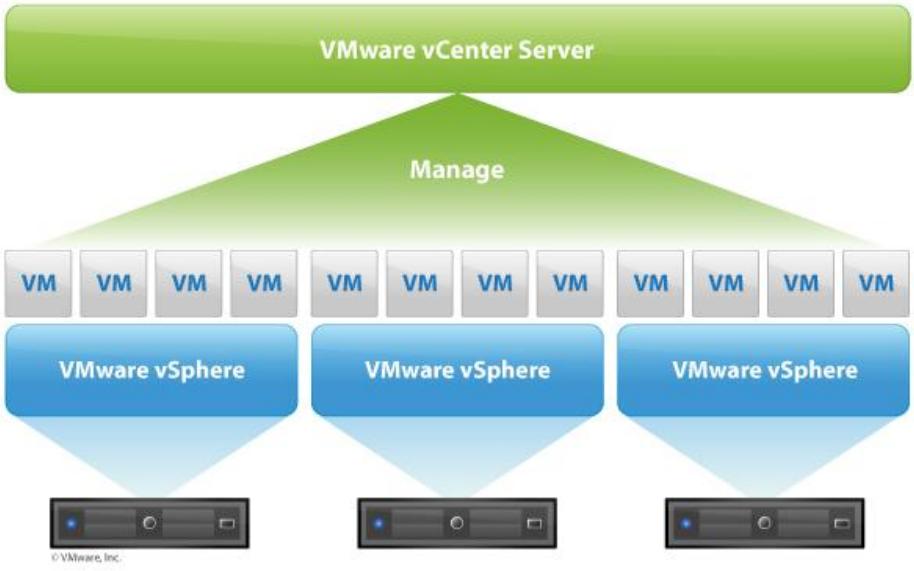


Figura 7: Plataforma VMware vCenter.

Fuente: http://www.vmware.com/co/products/vcenter-server/features.html

4.1.4.2 Sistema de alta disponibilidad SAD 2

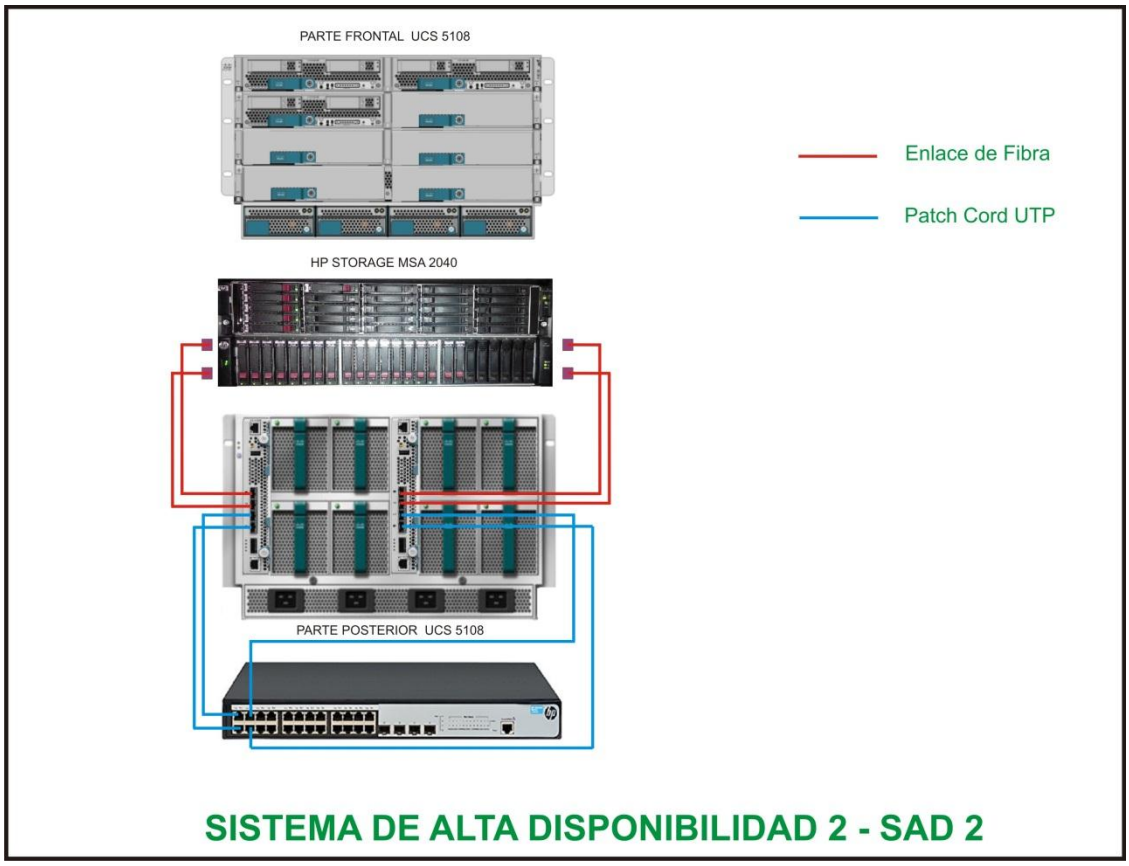


Figura 8: Sistema de alta disponibilidad SAD 2.

Fuente: División de sistemas – UFPSO.

En la figura 8, se ilustra una UCS Mini 5108 (Sistema de Computo Unificada) con almacenamiento HP. Esta solución está basada en tecnología Cisco Data Center de las familias USC Mini. Servidores blade y redes de 10 Gigabit Ethernet (10GE) y fábrica de 8G FC SAN integrado, capacidad de expansión máxima hasta 15 servidores de rack o blade y accesible por la administración unificada.

4.1.4.3 Sistema de alta disponibilidad, replicación y backup

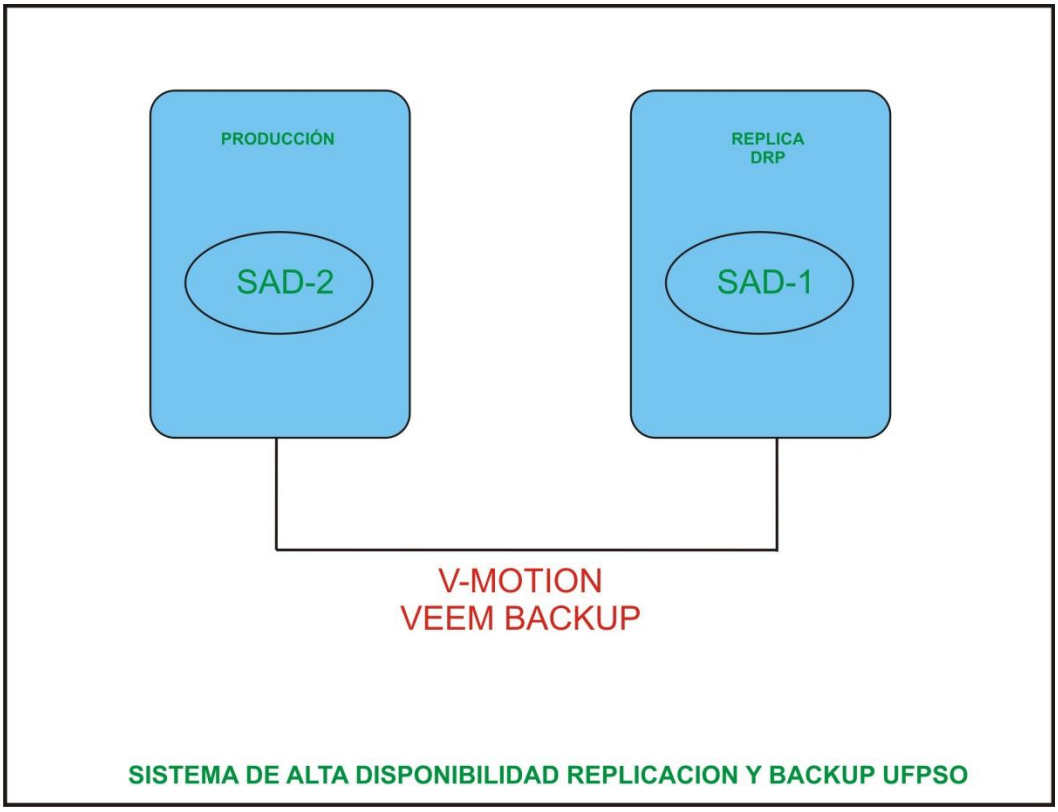


Figura 9: Sistema de alta disponibilidad, replicación y backup.

Fuente: División de sistemas – UFPSO.

En la figura 9, se describe el sistema de alta disponibilidad, replicación y backup implementado en la división de sistemas como respaldo a cada una de las máquinas virtuales configuradas en el sistema de producción (figura 8). Este sistema de alta disponibilidad implica tener un sistema de réplica o DRP (Plan de Recuperación de Desastres), que para nuestro caso sería la infraestructura que se muestra en la figura 6.

Esta configuración está dada por VeemBackup el cual ofrece la posibilidad tanto de copias de seguridad como de replicación de nuestro entorno virtual VMware. Permite realizar copias de seguridad de las máquinas virtualizadas del sistema de producción (figura 8) al sistema de réplica (figura 6) y se mantienen actualmente 14 copias de cada una de las máquinas y están configuradas para que se realicen de forma incremental.

4.1.4.4 Estado actual de la plataforma tecnológica división de sistemas

Tabla 24:

Estado actual de la plataforma tecnológica.

SV = Servidor Virtualizado SF = Servidor Físico

CARACTERÍSTICA	SOFTWARE / CARACTERISTICA		APLICACIÓN	SOPORTADO EN ADMINISTRACIÓN Y/O DESARROLLO POR
SV01	• Windows • BioStar 1.8	• No Licenciado • Licenciado	Software para el registro de ingreso de los empleados a la UFPS Ocaña	División de Sistemas División de Personal
SV02	• GNU - Linux • Asigra	• Software Libre • Software Libre	Aplicación para desarrollar las copias de seguridad externas	División de Sistemas
SV03	• GNU - Linux	• Software Libre	Aplicación para realizar pruebas de configuración de las plataformas de virtualización (uvirtual – univirtual)	División de Sistemas Unidad Virtual
SV04	• GNU - Linux	• Software Libre	Servidor de nombre de dominio	División de Sistemas
SV05	• Apliance Antivirus	• Licenciado	Eset Enpoint Security, Antivirus	División de Sistemas
SV06	GNU - Linux	• Software Libre	Aplicación para ejercicio de clase	División de Sistemas
SV07	• FreeBSD	• Software Libre	Firewall - Proxy red Salas de Computo	División de Sistemas

SV08	• FreeBSD	• Software Libre	Firewall - Proxy red Inalámbrica	División de Sistemas
SV09	• FreeBSD	• Software Libre	Firewall - Proxy red Idiomas	División de Sistemas
SV10	• Windows • LABSAG	• No licenciado • Licenciado	Aplicativo utilizado por la carrea de administración de empresas	División de sistemas
SV11	GNU - Linux	• Software Libre	Aplicativo base de datos	División de sistemas
SV12	GNU - Linux	• Software Libre	Aplicación para realizar las pruebas de inglés para los estudiantes de la UFPS Ocaña	División de Sistemas Centro de Idiomas
SV13	• FreeBSD	• Software Libre	Firewall - Proxy red administrativa	División de Sistemas
SV14	• GNU - Linux	• Software Libre	Servidor para realizar las pruebas de los aplicativos web que son desarrollados por la división de sistemas	División de sistemas
SV15	• GNU - Linux	• Software Libre	Aplicación para aplicar pruebas saber a los estudiantes de los últimos semestres	División de Sistemas
SV16	• Windows • Deep Freeze	• No licenciado • Licenciado	Aplicativo para controlar la instalación de software no autorizado en los equipo del área administrativa	División de Sistemas
SV17	• GNU - Linux	• Software Libre	Aplicativo para los procesos del restaurante universitario	División de sistemas Proyecto de Interconectividad

SV18	• GNU - Linux	• Software Libre	Aplicativos sistema de información documental, y peticiones quejas y reclamos.	División de Sistemas
SV19	• GNU - Linux	• Software Libre	Aplicativo sitio de inscripción para los estudiantes que desean ingresar a la UFPSO.	División de sistemas
SV20	• GNU - Linux	• Software Libre	Aplicativos soportados y desarrollados por la división de sistemas.	División de Sistemas
SV21	• GNU - Linux	• Software Libre	Aplicativos desarrollados por otras dependencias.	Laboratorio de Cisco División de sistemas - DIE DIE Cedit Proyecto de Interconectividad
SV22	• GNU - Linux	• Software Libre	página principal Institucional.	Webmaster
SV23	• GNU - Linux	• Software Libre	Respaldo de información.	División de sistemas
SV24	GNU - Linux	• Software Libre	Directorio activo, UFPS Ocaña.	División de sistemas
SV25	• Vmware - Vcenter	• Licenciado	Sistema de alta disponibilidad.	División de sistemas

SV26	• Windows • Veeam Backup and Replicaction	• Licenciado • Licenciado	Sistema de copia y replicación	División de sistemas
SF01	• GNU - Linux	• Software Libre	Emisora institucional	División de Sistemas
SF02	• VMware ESXi – 6.0 • Sistema operativo Linux	• Licenciado • Software Libre	Respaldo de información	División de Sistemas
SF03	• VMware ESXi – 6.0	• Licenciado	Servidor con disponibilidad para la realización de pruebas respectivas en las configuraciones que se llevan a cabo por la dependencia.	División de Sistemas
SF07	• GNU - Linux	• Software Libre	Aplicativos plataforma virtual	División de Sistemas Unidad virtual
SF08	• GNU - Linux	• Software Libre	Servidor base de datos	División de Sistemas
SF09	GNU - Linux	• Software Libre	Aplicativos de inscripción	División de Sistemas
SF10	• GNU - Linux	• Software Libre	Aplicativo emisora institucioanl	Proyecto de Interconectividad
SF11	• GNU - Linux	• Software Libre	Aplicativos soportados por otras dependencias	Proyecto de Interconectividad
SF12	GNU - Linux	• Software Libre	Aplicativo informacion institucional	División de Sistemas Planeación

SF13	• GNU - Linux	• Software Libre	Aplicativo informacion institucional	División de Sistemas Biblioteca
SF14	• GNU - Linux	• Software Libre	Central telefónica para la gestión de telefonía IP en la Institución	División de sistemas

Nota Fuente: División de sistemas – UFPSO.

La división de sistemas cuenta con una granja de servidores que en su mayoría están bajo una plataforma Linux y algunos de estos en Windows como se muestra en la tabla 24, que dan soporte a las diferentes aplicaciones y servicios de red para los usuarios brindando capacidad de almacenamiento y conectividad. Esta plataforma es robusta, estable y actualizada.

4.1.5 Sistemas de información

La Universidad Francisco de Paula Santander Ocaña encaminada a brindar los mejores servicios a la comunidad universitaria, decide implementar una serie de proyectos que se iniciaron en el año 2001 y que inició con el Sistema de Información Académico SIA, para continuar con el Sistema de Información Bibliográfico SIB, luego el Sistema de Información Financiero SIF, y actualmente se encuentran en implementación los Sistemas de Información Documental SID y el Sistema de Información de la Escuela de Bellas Artes SIABE, siendo herramientas que permiten de una manera óptima manejar la información, logrando así un mejor aprovechamiento del recurso humano y físico de la institución.

"Los Sistemas de Información están desarrollados con el sistema manejador de base de datos relacional RDBMS ORACLE y orientados a la web (Cliente/Servidor), el cual permitió diseñar un eficiente modelo relacional que garantiza la integridad y seguridad de la información, permitiendo la definición de diferentes políticas para su administración." (Sistema de información institucional., 2014)

- Sistema de información académico SIA.

Es una aplicación elaborada para la administración de los diferentes procesos académicos que se llevan a cabo en la Universidad, el cual contiene los siguientes desarrollos:

- Sistema vía Web inscripción a aspirantes.
- Sistema de información académico vía Web.
- Sistema vía Web matrícula de alumnos en línea.
- Sistema vía Web inclusiones y/o cancelaciones.
- Sistema vía Web digitación de notas.
- Sistema vía Web solicitud de becas trabajos y/o monitorias.
- Sistema vía Web solicitud de financiación de la matrícula.
- Sistema vía Web solicitud de vacacionales.
- Sistema vía Web evaluación docente.
- Sistema vía Web registro de examen de serología.
- Sistema vía Web de registro de cátedra de los docentes.
- Sistema vía Web de académicos para cursos y pruebas de inglés (inscripción, matrícula, gestión de grupo).

- Sistema de información bibliográfico SIB.

Es una aplicación que permite manejar la información cualquier tipo de material bibliográfico como son libros, tesis, publicaciones seriadas. Incluye los siguientes módulos:

- Sistema de circulación y préstamo.

- Sistema vía Web de consulta bibliográfica.
- Repositorio digital – Dspace (consulta de trabajo de grado en línea).

➢ Sistema de información documental.

El Sistema de Información Documental (SID) es una herramienta tecnológica desarrollada por la UFPSO bajos los más altos estándares de la Web, siguiendo los lineamientos de la oficina de Archivo y Correspondencia para el servicio de cada una de sus dependencias productoras de documentos.

El (SID), permite al usuario crear, actualizar e imprimir documentos como: Actas, Certificados, Circulares, Citaciones, Constancias, Memorandos, Resoluciones y Oficios. Además de soportar los tipos de documentos ya mencionados, cuenta con un módulo de ventanilla única para la recepción y control de documentos provenientes de instituciones o entidades externas a la Universidad.

El sistema (SID) actual mente cuenta con varios módulos en los cuales se destacan:

- Módulo de Registro de convenio.
- Módulo de sugerencia.
- Módulo de contenido de resolución.
- Módulo de solicitud.
- Módulo de registros de normogramas.
- Módulo de radicación (Entrada y Salida de documentos).

- Módulo de encuesta de satisfacción de los clientes de ventanilla única.
- Módulo de producción de documentos.
- Módulo de consulta de documentos.
- Módulo de distribución de documentos.

➢ Sistema de información financiero.

Es una aplicación elaborada para facilitar la administración de los diferentes procesos contables y presupuestales que se llevan a cabo en la intranet de la Universidad.

Módulos desarrollados:

- Módulo de solicitudes de servicios y compras.
- Módulo de subdirección administrativa (ordenes, autorizaciones de pago, etc).
- Módulo de tesorería (comprobantes de egresos, ingresos, etc).
- Módulo de presupuesto (CDP, obligaciones, etc).
- Módulo de contabilidad (cuentas por pagar, cuentas por cobrar etc).
- Módulo de recursos humanos (nómina y personal).
- Módulo de almacén (entrada y salida de elementos).
- Módulo de inventario institucional.

➢ Sistema de información académico SIABE (Escuela de Artes).

Es una aplicación web que tiene como finalidad dar soporte a los procesos académicos beneficiando a toda la comunidad en especial a estudiantes, docentes y administradores, quienes

podrán consultar toda su información académica en cualquier momento y desde cualquier lugar de forma rápida y segura.

Módulos desarrollados:

- Sistema vía Web de inscripciones.
- Sistema vía Web de matrículas.
- Digitación de notas.
- Registro hora cátedra.
- Evaluación docente.

➢ Sistema de información de bienestar universitario SIBU.

Es una aplicación orientada a la web, con el fin de almacenar información de acuerdo a la actividad que se esté ejecutando por parte del profesional idóneo contratado. Corresponde al área de salud, cultura y deportes.

Módulos desarrollados:

- Módulo administrador de bienestar universitario.
- Módulo de enfermería.
- Módulo de odontología.
- Módulo de psicología.
- Módulo de medicina general.
- Módulo de trabajo social.
- Módulo de asesoría espiritual.
- Módulo de deportes.

- Módulo de cultura.

4.2 Establecimiento del contexto

4.2.1 Consideraciones generales

A partir del numeral 4.1 del capítulo 4 se describe las principales características de las funciones procedimientos, infraestructura y servicios que soporta la dependencia División de Sistemas de la UFPSO. El propósito de este análisis contempla organizar y agrupar los activos con el fin de minimizar los riesgos a los que estos se enfrentan.

Para el caso de este análisis solamente se contempla llegar al tratamiento de los riesgos, por que depende de la dirección de la universidad abordar las etapas de aceptación de los riesgos que se encuentren y el posterior monitoreo de los mismos para dar seguimiento a la toma de las medidas necesarias que permitan mitigar las fallas encontradas, con el fin de conservar y garantizar la seguridad de la información de todos los activos con que cuenta la división de sistemas.

4.2.2 Criterios básicos

El enfoque que presenta el análisis contempla la evaluación de los activos y el impacto que podría presentarse en caso de que uno de estos se viera afectado. Considerando la naturaleza del entorno y de la información previamente seleccionada. Para esto se utilizará un enfoque

cualitativo, acompañado de una valoración numérica; y usando una matriz que se formará de combinar la probabilidad que ocurra una amenaza con la magnitud del daño de dicha amenaza, asignándole su valor correspondiente para obtener resultados más apropiados para su interpretación, además se utilizará colores para diferenciar cada uno de los resultados obtenidos de acuerdo a la gravedad del riesgo. Los criterios a utilizar para realizar esta etapa del análisis contempla:

- Criterios para la clasificación de activos.
- Criterios de probabilidad de ocurrencia de las amenazas.
- Criterios de impacto.
- Criterios de evaluación del riesgo.
- Criterios de aceptación del riesgo.

4.2.2.1 Criterio para la clasificación de activos

Teniendo en cuenta el análisis llevado en la división de sistemas y analizando cada uno de sus objetivos se hace la clasificación de los activos de la siguiente manera: activos primarios (activos de información) y activos de soporte (activos físicos, activos de software y activos de servicios). La valoración de los activos busca establecer la importancia de los mismos tomando como criterios su disponibilidad, integridad y confidencialidad.

Tabla 25:

Criterios de disponibilidad de los activos.

VALOR	PARAMETRO	DESCRIPCION
1	Bajo	La falta del activo no afecta los procesos o actividades soportadas por la división de sistemas
2	Medio	La falta del activo afecta medianamente los procesos o actividades soportadas por la división de sistemas
3	Alto	La falta del activo afecta considerablemente los procesos o actividades soportadas por la división de sistemas
4	Muy alto	La falta del activo es crítico para los procesos o actividades soportadas por la división de sistemas

Nota Fuente: Autores del proyecto.

Tabla 26:

Criterios de confidencialidad de los activos.

VALOR	PARAMETRO	DESCRIPCION
1	Bajo	El conocimiento de la información propia del proceso (archivos de configuración, datos de acceso, entre otros) no afecta la ejecución de las actividades soportadas por la división de sistemas
2	Medio	El conocimiento de la información propia del proceso (archivos de configuración, datos de acceso, entre otros) afecta medianamente la ejecución de las actividades soportadas por la división de sistemas
3	Alto	El conocimiento de la información propia del proceso (archivos de configuración, datos de acceso, entre otros) afecta considerablemente la ejecución de las actividades soportadas por la división de sistemas
4	Muy alto	El conocimiento de la información propia del proceso (archivos de configuración, datos de acceso, entre otros) es crítico para la ejecución de las actividades soportadas por la división de sistemas

Nota Fuente: Autores del proyecto.

Tabla 27:

Criterios de integridad de los activos.

VALOR	PARAMETRO	DESCRIPCION
1	Bajo	La pérdida de veracidad y/o funcionalidad de los activos, impacta levemente a todas las actividades soportadas por la división de sistemas
2	Medio	La pérdida de veracidad y/o funcionalidad de los activos, impacta medianamente a todas las actividades soportadas por la división de sistemas
3	Alto	La pérdida de veracidad y/o funcionalidad de los activos, impacta considerablemente a todas las actividades soportadas por la división de sistemas
4	Muy alto	La pérdida de veracidad y/o funcionalidad de los activos, impacta críticamente a todas las actividades soportadas por la división de sistemas

Nota Fuente: Autores del proyecto.

Para establecer el nivel de importancia (NI) del activo se debe tener encueta los niveles establecidos en los criterios de disponibilidad, integridad y confidencialidad, tal como se indican en las tablas 25, 26 y 27 respectivamente. Para calcular el nivel del riesgo se realiza la siguiente operación:

NI = (integridad).(disponibilidad).(confidencialidad)

De la fórmula anterior se obtienen los valores respectivos y se establecen los rangos para valorar el activo como se muestra en la tabla 28.

Tabla 28:

Valores para determinar el nivel de importancia de los activos.

VALOR	PARAMETRO	DESCRIPCION
1 – 4	No es importante	El activo es de muy baja importancia para los procesos que soporta la división de sistemas.
6 – 12	Poco importante	El activo tiene poca importancia para los procesos que soporta la división de sistemas
16 – 27	Importante	El activo es importante para los procesos que soporta la división de sistemas
32 – 64	Muy importante	El activo es de vital importancia para el buen funcionamiento de los procesos que soporta la división de sistemas.

Nota Fuente: Autores del proyecto.

4.2.2.2 Criterios para la probabilidad de ocurrencia de amenazas

Los criterios de probabilidad de ocurrencia, serán analizados teniendo en cuenta que tan probable se presente una vulnerabilidad para que sea aprovechada por una amenaza estos valores se exponen en la tabla 29. La norma establece varios criterios pero para el desarrollo de este análisis se estipularon 4 valores.

Tabla 29:

Probabilidad de ocurrencia de amenazas.

VALOR	GRADO DE IMPACTO	DESCRIPCIÓN
1	PC = Poco Probable	Amenazas cuya probabilidad de explotar vulnerabilidades es poco probable
2	P =Probable	Amenazas que con poca frecuencia exploten vulnerabilidades
3	MP = Muy Probable	Amenazas que frecuentemente explotan vulnerabilidades
4	AP = Altamente probable	Amenazas que en la mayoría de los casos explotan vulnerabilidades

Nota **Fuente:** Autores del proyecto

4.2.2.3 Criterios de impacto

Para la división de sistemas es de vital importancia mantener la operatividad en todos los servicios que presta, y de presentarse alguna falla en sus activos y procesos causaría un gran impacto que afectaría a todos los usuarios que hacen uso de las plataformas que brinda la división de sistemas. Para estos criterios se consideran los siguientes aspectos.

- Tiempo que el servicio se encuentra sin funcionamiento.
- Pérdidas de confidencialidad integridad y/o disponibilidad de los activos.

De acuerdo a la información recolectada en la división de sistemas se establece un valor cualitativo cuando se presentan problemas en los diferentes servicios, estableciendo escalas de tiempo sin funcionamiento de un servicio y se asignará un valor de 1 a 4 como se describe en la tabla 30.

Tabla 30:

Impacto de acuerdo al tiempo sin funcionamiento del servicio.

VALOR	GRADO DE IMPACTO	DESCRIPCIÓN
1	P = Pequeño	Tiempo de caída mínimo de 1 a 14 minutos
2	M =Medio	Tiempo de caída moderado de 15 a 30 minutos
3	G = Grave	Tiempo de caída del servicio alto de 30 minutos a una hora
4	MG = Muy Grave	Tiempo de caída muy alto de más de 1 horas

Nota Fuente: Autores del proyecto.

En la tabla 31. Se establecen los criterios para valorar el impacto desde el punto de vista que pueda presentarse una pérdida de confidencialidad, integridad y disponibilidad de los activos que soporta la infraestructura de la dependencia de la División de sistemas.

Tabla 31:

Impacto de acuerdo a la pérdida de confidencialidad, integridad y disponibilidad del activo

VALOR	GRADO DE IMPACTO	DESCRIPCIÓN
1	P = Pequeño	Pérdida de confidencialidad, integridad y disponibilidad del activo mínimo.
2	M =Medio	Pérdida de confidencialidad, integridad y disponibilidad del activo moderado.
3	G = Grave	Pérdida de confidencialidad, integridad y disponibilidad del activo grave
4	MG = Muy Grave	Pérdida de confidencialidad, integridad y disponibilidad del activo muy grave

Nota Fuente: Autores del Proyecto.

4.2.2.4 Criterios de evaluación del riesgo

Para obtener un valor de riesgo aproximado a la realidad de acuerdo a los servicios prestados por la división de sistemas se trabajará con el valor obtenido del producto de la probabilidad de ocurrencia de una amenaza por el valor del impacto debido al tiempo sin funcionamiento del servicio y la pérdida de integridad, confidencialidad y disponibilidad del activo. Por lo tanto:

Nivel de evaluación de riesgo = (probabilidad de ocurrencia de una amenaza) * (tiempo sin funcionamiento del servicio)*(pérdida de integridad, confidencialidad disponibilidad del activo)

Estableciendo las diferentes combinaciones de acuerdo a la expresión anterior se obtienen los rangos cualitativos para la evaluación del riesgo como se muestra en la tabla 32.

Tabla 32:

Nivel de evaluación del riesgo.

VALOR	NIVEL	DESCRIPCION
1 – 4	Bajo	El nivel de riesgo es bajo, cuando el tiempo sin funcionamiento del servicio es mínimo, la pérdida de integridad, disponibilidad y confidencialidad es mínima y tiene pocas probabilidades de la ocurrencia de una amenaza.
6 – 12	Moderado	El nivel de riesgo es moderado, cuando el tiempo sin funcionamiento del servicio es medio, la pérdida de integridad, disponibilidad y confidencialidad es pequeña y con ciertas probabilidades de la ocurrencia de una amenaza.
16 – 27	Alto	El nivel de riesgo es alto, cuando el tiempo sin funcionamiento del servicio es grave, la pérdida de integridad, disponibilidad y confidencialidad es alta y con altas probabilidades de la ocurrencia de una amenaza.
32 – 64	Muy alto	El nivel de riesgo es muy alto, cuando el tiempo sin funcionamiento del servicio es muy alta, la pérdida de integridad, disponibilidad y confidencialidad es considerable y con altísimas probabilidades de la ocurrencia de una amenaza.

Nota Fuente: Autores del proyecto.

4.2.2.5 Criterios de aceptación del riesgo

Los criterios de aceptación del riesgo por lo general dependen de las políticas y objetivos establecidos por la división de sistemas, siendo así que la evaluación del riesgo se realiza de la comparación de los niveles de riesgo con los criterios para la evaluación del mismo.

Tabla 33:

Criterios de aceptación y tratamiento del riesgo.

NIVEL DEL RIESGO	TRATAMIENTO
Bajo	REDUCCION DEL RIESGO
Moderado	
Alto	
Muy Alto	

Nota Fuente: Autores del Proyecto.

Teniendo en cuenta que la norma 27005:2011, presenta para el tratamiento del riesgo las opciones de retener, reducir, evitar o transferir, se considera la reducción para todos los niveles de riesgos ya mencionados.

Se puede realizar la transferencia del riesgo, en el caso de que un servicio de la división de sistemas pase a formar parte de otra área, en tal caso, el manejo de la gestión será transferido con todas las recomendaciones para minimizar el riesgo. De igual manera aquellos factores que involucren la dirección o gestión de terceros garantizando así la funcionalidad de los servicios.

4.2.3 Alcance y límites

La división de sistemas es la encargada de dar soporte a las telecomunicaciones, infraestructura y los diferentes servicios que esta ofrece, para toda la universidad. Es por eso que es de gran importancia realizar una análisis de riesgos que permitan identificar las fallas encontradas y a partir de estas seguir los lineamiento necesarios que con lleven a garantizar la funcionalidad y continuidad de los mismos.

De acuerdo a la información descrita en la primera parte de este capítulo en el cual se describe la infraestructura tecnológica de la división de sistemas; este análisis contempla los activos primarios (El proceso, y las bases de datos) y lo activos de soporte (equipos servidores, equipos del área de trabajo UPS, el sistema de alta disponibilidad, los servicios, las aplicaciones la infraestructura de red, el personal y el sitio).

Los activos a describir son los que permiten el correcto funcionamiento y operatividad de los servicios que presta la división de sistemas, por lo tanto esta gestión de riesgos busca identificar aquellas amenazas a los que estas expuestos y a partir de esta identificación, realizar el tratamiento de los mismos, según los criterios que fueron establecidos en el desarrollo del proyecto.

4.3 Valoración del riesgo en la Seguridad de la Información

Un riesgo es una combinación de las consecuencias que se presentarían después de la ocurrencia de un evento indeseado y de su probabilidad de ocurrencia. La valoración del riesgo cuantifica o describe cualitativamente el riesgo y permite a los directores priorizarlos riesgos de acuerdo con su gravedad percibida u otros criterios establecidos.

La valoración del riesgo consta de las siguientes actividades

- Identificación del riesgo
- Estimación del riesgo
- Evaluación del Riesgo

"La valoración del riesgo determina el valor de los activos de información, identifica las amenazas y vulnerabilidades aplicables que existen (o que podrían existir), identifica los controles existentes y sus efectos en el riesgo identificado, determina las consecuencias potenciales y, finalmente, prioriza los riesgos derivados y los clasifica frente a los criterios de evaluación del riesgo determinados en el contexto establecido." (INTERNATIONAL STANDARD ISO/IEC 27005:2011, 2011)

4.3.1 Análisis de riegos

4.3.1.1 Identificación del riesgo

El propósito de la identificación de riesgo es determinar los activos que soportan los diferentes servicios que brinda la división de sistemas, las amenazas a las que están expuesto dichos activos y las vulnerabilidades que podrían ser explotadas por las amenazas.

4.3.1.1.1 Identificación de los activos

Tabla 34:

Activos primarios.

Información

Activo:	Proceso de apoyo SITT
Descripción técnica	Sistema de información telecomunicaciones y tecnología, es el nombre del proceso dado a la dependencia, como uno de los procesos de apoyo de la UFPSO, ya que la universidad cuenta con un SIG (Sistema Integrado de Gestión) en el cumplimiento de la norma ISO 9001:2015. Este proceso contempla lo descrito en el inciso 4.1.1.7 revisión documental, donde se establecen todos los procedimientos y caracterización del proceso que contempla esta norma y son de vital importancia para la universidad para garantizar el cumplimiento de la misma.
Responsable	Como responsable del proceso está a cargo el jefe de la división de sistemas, y los profesionales de apoyo, dependiendo de sus funciones se asignan los formatos respectivos.

Activo	Base de datos Oracle 10G
Descripción técnica	Base de datos principal de la UFPS Ocaña, y de los cuales se alimentan diferentes sistemas de información.
Responsable	Jefe División de sistemas

Activo	Base de datos Mysql
Descripción técnica	Base de datos Utilizada para diferentes aplicativos dentro de la institución.
Responsable	Profesional de apoyo (área de servidores)

Activo	Base de datos Postgres
Descripción técnica	Base de datos Utilizada para diferentes aplicativos dentro de la institución
Responsable	Profesional de apoyo (área de servidores)

Nota Fuente: Autores del proyecto.

Tabla 35:

Activos de soporte.

Equipos fijos - Servidores

Activo	Servidor Físico SF01, servidor físico SF02, servidor físico SF03, servidor físico SF04, servidor físico SF05, servidor físico SF06, servidor físico SF07, servidor físico SF08, servidor físico SF09, servidor físico SF10, servidor físico SF11, servidor físico SF12, servidor físico SF13, servidor físico SF14, servidor físico SF15.
Descripción técnica	Características de estos activos en la tabla 24, y en el inciso 4.1.3.2.2.
Responsable	Profesional de apoyo (área de servidores)

Equipos fijos - Computadores de trabajo

Activo	Computadores de escritorio
Descripción técnica	Características de estos activos en la tabla 4, hace referencia a los equipos utilizados por los funcionarios en la división de sistemas para las realizar sus labores diarias
Responsable	Jefe división de sistemas y profesionales de apoyo

Equipos de respaldo de energía

Activo	UPS
Descripción técnica	Características de estos activos en la tabla 23, estas UPS respaldan los equipos del área de servidores y los rack de comunicaciones ubicados en la división de sistemas
Responsable	Jefe división de sistemas y profesionales de apoyo

Solución de alta disponibilidad replicación y Backup

Activo	SAD 1 y SAD 2
Descripción técnica	Las características de las soluciones SAD 1 y SAD 2 se encuentran en las figuras 6 y figura 8 respectivamente, la solución SAD 1 fue la primera solución adquirida por la universidad, la cual está conformada por los switches de fibra (Características tabla 20) y por la SAN 1 (Características tabla 17). Esta solución de alta disponibilidad utiliza un enlace y un switch de fibra de respaldo en caso tal switch y enlace principal fallen, garantizando así la disponibilidad de la solución. La solución SAD 2 (figura 8) fue la última solución de alta disponibilidad adquirida por la universidad, un sistema de cómputo unificado (Características Tabla 16) la cual está conformada por la SAN 2 (Características tabla 18). Estas dos soluciones conforman la solución de alta disponibilidad replicación y backup implementados por la división de sistemas; donde la última solución soporta el desarrollo de todos los servicios en producción y la primera solución adquirida se configuró como un DRP (Plan de recuperación de desastre) la cual está configurada para replicar las máquinas configuradas en el sistema de producción y guardar réplicas de las mismas de manera incremental por 14 días.
Responsable	Profesional de apoyo (área de servidores)

Equipos de comunicaciones

Activo	Switches de acceso
Descripción técnica	El core de switches permite la interconexión de todos los equipos dispersos en el campus universitario (Características Tabla 21), descripción de la conexión figura 3.
Responsable	Profesional de apoyo (área de redes)

Servicios

Activo	Directorio activo
Descripción técnica	El servicio de OpenLdap, se encarga del almacenamiento de usuarios y las credenciales respectivas, funciona como el primer nivel de seguridad para la autenticación de los usuarios ante los diferentes sistemas que presta la división de sistemas.
Responsable	Profesional de apoyo (área de servidores)

Activo	Antivirus
Descripción técnica	Servidor de protección de antivirus para las estaciones de trabajo de los diferentes equipos del área administrativa de la UFPSO
Responsable	Profesional de apoyo (área de servidores)

Activo	Servicio DNS
Descripción técnica	Este servidor es el encargado de la resolución de nombres para todos los sitios que son configurados y soportados por la división de sistemas. Descripción en la tabla 24.
Responsable	Profesional de apoyo (área de servidores)

Activo	Servicio Proxy – Firewall - DHCP
Descripción técnica	Estos servidores son los encargados de prestar el servicio de Internet para las estaciones de trabajo. De igual forma asignan los parámetros de red para los equipos de las salas de cómputo y la red inalámbrica, en el caso de la red administrativa el direccionamiento es estático. A través de estos se configuran las reglas de control de acceso y los bloqueos a los sitios no permitidos.
Responsable	Profesional de apoyo (área de servidores)

Activo	Backup
Descripción técnica	El proceso de backup de cada uno de las aplicaciones alojadas en los servidores se realiza diariamente al servidor de backup (Tabla 24. SV02). Las copias generadas se almacenan en este servidor y el aplicativo DS-Client toma la información y la envía completa al equipo destinado en el Datacenter, de forma incremental para actualizar los datos que hayan cambiado.
Responsable	Profesional de apoyo (área de servidores)

Aplicaciones

Activo	Aplicaciones desarrolladas y soportadas por la división de sistemas
Descripción técnica	Estas aplicaciones son: ➢ Sistema de información académico ➢ Sistema de información financiero ➢ sid.ufpso.edu.co ➢ pqrs.ufpso.edu.co ➢ aspirante.ufpso.edu.co ➢ biblioteca.ufpso.edu.co ➢ artes.ufpso.edu.co ➢ bienestar.ufpso.edu.co ➢ controli.ufpso.edu.co ➢ egresado.ufpso.edu.co ➢ serología.ufpso.edu.co ➢ ingles.ufpso.edu.co ➢ divisis.ufpso.edu.co ➢ siadmon.ufpso.edu.co ➢ planeación.ufpso.edu.co ➢ encuesta.ufpso.edu.co ➢ respaldo.ufpso.edu.co ➢ ofniametsis.ufpso.edu.co ➢ snies.ufpso.edu.co ➢ repositorio.ufpso.edu.co
Responsable	Profesional de apoyo (área de desarrollo)

Activo	Aplicaciones a las cuales la división de sistemas les presta servicio de alojamiento del sitio y de la base de datos respectiva al igual que las copias de seguridad de las mismas
Descripción técnica	Estas aplicaciones son: ➢ virtualidad.ufpso.edu.co ➢ idiomas.ufpso.edu.co ➢ saberpro.ufpso.edu.co ➢ restaurante.ufpso.edu.co ➢ lryt.ufpso.edu.co ➢ campusvirtual.ufpso.edu.co ➢ revistas.ufpso.edu.co ➢ die.ufpso.edu.co ➢ cedit.ufpso.edu.co ➢ coninge.ufpsoe.du.co ➢ www.ufpso.edu.co ➢ laufm.ufpso.edu.co ➢ uvirtual.ufpso.edu.co ➢ univirtual.ufpso.edu.co ➢ web.ufpso.edu.co ➢ eventos.ufpso.edu.co ➢ portalbienestar.ufpso.edu.co
Responsable	Personal externo a cargo del desarrollo de las mismas

Red

Activo	Telefonía análoga e IP
Descripción técnica	El sistema de telefonía de la UFPSO se describe en la figura 5, es responsabilidad de la división de sistemas garantizar la funcionalidad del servicio de voz |para toda la universidad.
Responsable	Profesional de apoyo (área de servidores)

Activo	Red de datos
Descripción técnica	La red de datos de la UFPSO está conformada por 2 sedes externas, la sede de la primavera y la sede de bellas artes. Como se muestra en la figura 3. La conexión de fibra converge al nodo principal ubicado de la división de sistemas y a través de esta se distribuyen los diferentes tráficos que se originan en la red para prestar los servicios respectivos.
Responsable	Profesional de apoyo (área de redes)

Activo	Red de Inalámbrica
Descripción técnica	La red inalámbrica hace referencia a la descripción realizada en la figura 4. Este servicio de conexión a Internet es ofrecido por zonas para los diferentes estudiantes, profesores y administrativos dentro de la sede principal.
Responsable	Profesional de apoyo (área de servidores)

Sitio

Activo	Centro de cómputo
Descripción técnica	La división de sistemas aloja todos los equipos que dan soporte a la infraestructura de red y a los servicios para toda la universidad, es de vital importancia para la organización mantener estos activos a salvo y seguros de cualquier incidente.
Responsable	Profesional de apoyo (área de servidores)

Activo	Personal
Descripción técnica	Hace referencia a todas las personas que laboran en el proceso de sistemas de información telecomunicaciones y tecnología
Responsable	Jefe división de sistemas y Profesional de apoyo

Nota Fuente: Autores del proyecto

4.3.1.1.2 Valoración de los activos

Para determinar el valor del activo se utilizan los valores de disponibilidad, integridad y confidencialidad descritos en las tablas 25, 26, 27 respectivamente; de igual forma dependiendo de la operación para hallar el nivel de importancia (NI), se establecerá el valor del activo para la división de sistemas (Tabla28).

Tabla 36:

Valoración de los activos.

ACTIVO	CRITERIOS DE VALORACIÓN DE LOS ACTIVOS			VALOR DEL ACTIVO
	Disponibilidad	Confidencialidad	Integridad	
Proceso de apoyo SITT	4	3	4	48
Base de datos Oracle 10g	4	4	4	64
Base de datos Mysql	4	4	4	64
Base de datos Postgres	4	4	4	64
Servidores	4	4	4	64
Computadores de escritorio	3	3	2	18

UPS	4	3	4	48
SAD 1 y SAD 2	4	4	4	64
Switches de acceso	4	3	4	48
Directorio activo	4	4	4	64
Antivirus	4	3	3	36
Servicio DNS	4	3	3	36
Servidor Proxy – Firewall DHCP	4	3	3	36
Backup	4	4	4	64
Aplicaciones desarrolladas y soportadas por la división de sistemas	4	4	4	64
Aplicaciones a las cuales la división de sistemas se les presta servicio de alojamiento del sitio y de la base de datos respectiva al igual que las copias de seguridad de las mismas	4	4	4	64
Telefonía análoga e IP	3	3	3	27
Red de datos	4	4	4	64
Red Inalámbrica	2	3	3	18
Centro de computo	4	4	4	64
Personal	4	4	4	64

Nota Fuente: Autores del proyecto.

Los valores establecidos corresponden a los criterios que considera la división de sistemas para cada uno de sus activos, es de vital importancia realizar detalladamente este análisis para determinar la importancia de los mismos.

4.3.1.1.3 Identificación de las amenazas

Para la identificación de las amenazas sobre los activos identificados por la división de sistemas, se toma en consideración la naturaleza del origen de las mismas, las cuales pueden ser deliberadas (D), accidentales (A) o ambientales (naturales – (E)) y pueden dar como resultado el daño o la pérdida de uno o varios activos que son de vital importancia para las diferentes actividades y procesos que ejecuta la dependencia. La letra D se utiliza para todas la acciones deliberadas o mal intencionadas que tienen como objetivo causar daño a los activos, A se utiliza para las acciones humanas que puedan dañar accidentalmente los activos y E se utiliza para todos los incidentes que no se basa en las acciones humanas sino más bien son producto de eventos naturales.

Tabla 37:

Identificación de las amenazas.

Tipo	Amenaza	Origen
Daño físico	Fuego	A, D, E
	Daño por agua	A, D ,E
	Destrucción del equipo o los medios	A, D
	Polvo, corrosión, altas temperaturas	E
Eventos naturales	Fenómenos climáticos	E
	Fenómenos sísmicos	E
Pérdida de los servicios esenciales	Falla en el sistema de suministro de aire acondicionado	D
	Pérdidas de suministro de energía	A, D, E
	Falla en el equipo de telecomunicaciones	D, E
Perturbación debido a la radiación	Radiación electromagnética	D
Compromiso de la información	Interceptación de señales de interferencia comprometedoras	D
	Espionaje remoto	D
	Hurto de medios, EQUIPOS documentos	D
	Recuperación de medios reciclados o desechados	D
	Manipulación con hardware	D
	Manipulación con software	D
Fallas técnicas	Falla de equipo	A, E
	Mal funcionamiento del software e incumplimiento en el mantenimiento del mismo	A

Acciones no autorizadas	Uso no autorizado del equipo	D
	Copia fraudulenta del software	D
	Uso del software falso o copiado	D
	Corrupción de datos	D
Compromisos de las funciones	Error en el uso inadecuado de la información	A
	Incumplimiento en la disponibilidad del personal	A, D, E

Nota Fuente: Autores del Proyecto.

4.3.1.1.4 Identificación de los controles existentes

Como medidas de control la división de sistemas cuenta con un documento de políticas de seguridad de la información, aprobadas según resolución No. 0118 de Abril 22 de 2015, pendiente de socialización y divulgación para conocimiento de los funcionarios de la dependencia y comunidad en general. A continuación se mencionan los controles existentes encontrados e implementados por la dependencia.

Tabla 38:

Controles Existentes.

TIPO DE AMENAZA	CONTOLES EXISTENTES	OBSERVACIONES
Daño Físico	Extintores	Se cuentan con tres extintores en la dependencia, para mitigar cualquier conflagración. Pero estos no se encuentran presentes en los cuartos de telecomunicaciones donde están ubicados los demás racks. El mantenimiento es periódico. No se cuenta con personal capacitado dentro del área de sistemas para su manipulación.
	Aire acondicionado	Se cuenta con 4 aires acondicionados para evitar las altas temperaturas y evitar el recalentamiento de los equipos, 2 para el cuarto de servidores, uno para el área de administración y otro para el área de desarrollo.
Eventos naturales	Copias de seguridad	Se tiene contratado un servicio de copias de seguridad con un proveedor externo el cual se encarga de salvaguardar la información que

		se aloja en el servidor de copias de seguridad interno a sus servidores.
Pérdida de los servicios esenciales	SAI o en inglés UPS (sistema de alimentación ininterrumpida)	Se cuentan con 5 UPS, las cuales se encuentran descritas en el numeral 4.1.3.2.6 Equipos de respaldo de energía, la de 10 K se encarga de dar respaldo a los servidores (Equipos servidores y Solución de alta disponibilidad) la de 6 K al rack de comunicaciones, las de 1K instaladas como soporte a la de 10K y la TRIPP – LITE como respaldo a los equipos de desarrollo y de administración de la red. El tiempo máximo de estas UPS es de 30 minutos.
	Canales de Internet	Se cuenta con canales para dar respaldo de conexión, en caso de que el internet de la sede principal falle por algún evento ajeno de la universidad. No se cuenta con balanceo de carga, y el procedimiento de configuración se hace manualmente.
Compromiso de la información	Cámaras de seguridad	La seguridad física al cuarto de servidores está monitoreada por una cámara de seguridad, y puertas de acceso con llave a las diferentes áreas. La seguridad física no es la adecuada ya que no se cuentan con áreas seguras para el acceso al cuarto de servidores, ni al cuarto de telecomunicaciones, y el techo no es adecuado para albergar estos equipos.
	Hardening	Consiste en realizar el endurecimiento de la máquina antes de ser expuesta a Internet, Consiste en la actualización de la paquetería, el cambio de puertos y la utilización de contraseñas robustas.
	Políticas de seguridad • Controles de acceso • Uso y caducidad de contraseñas • Navegación y uso del correo electrónico • Entre otros.	Las políticas de seguridad establecidas por la división de sistemas se acoge a los controles y sanciones establecidas en la ley 1273 del 5 de enero del 2009.
Fallas técnicas	Personal	La división de sistemas cuenta con personal capacitado para dar soporte a las diferentes actividad y procesos que esta dependencia Tiene.

	Antivirus	Se cuenta con un antivirus licenciado, Eset Enpoint Security. El cual se encuentra implementado para los equipos del área administrativa de la Universidad
	Firewall	Se tienen instalados 4 firewall para las redes existentes en la universidad, en ellos hay configuradas reglas de acceso, restricciones a páginas web entre otros; todos estos bajo software.
	Congelamiento de Particiones	En el proceso de mantenimiento de los equipos se cuenta con licencia del software Deep Freeze, en este mantenimiento se congela la partición en donde se instala el sistema operativo (Generalmente C) con el fin de evitar la instalación permanente de software no autorizado.
Acciones no autorizadas	Sistema de autenticación	El servicio de directorio activo mediante OpenLdap se encarga de almacenar los usuarios y las credenciales de autenticación de los mismos ante los diferentes servicios. Es el primer nivel de seguridad.
	Manejo de privilegios	A nivel de base de datos se crea el usuario y la contraseña respectiva y solo ese usuario tiene privilegios a la base de datos que se le asigne. A nivel de acceso al sitio los usuarios se les restringe el escalamiento en el árbol de directorios, solo tienen acceso a la carpeta asignada.
	Extensiones telefónicas	Se restringe el acceso de llamadas externas a las extensiones telefónicas de la Universidad por límite de tiempo y con código de acceso a las líneas troncales según sea el caso.
Compromiso de las funciones	Mantenimiento preventivos	Existe un plan de mantenimiento preventivo y correctivo de equipos de cómputo (L-TT-DSS-001). Se cumple en su totalidad.
	Certificado digital https	Uso del protocolo HTTPS como mecanismo de seguridad de los sitios. Se encuentra implementado en la mayoría de ellos.
	Controles de tráfico	Las redes de la Universidad se encuentran segmentadas por medio de Vlans y el acceso y configuración a cada una de ellas seda por el administrador de la red.

Nota Fuente: Autores del proyecto.

4.3.1.1.5 Identificación de vulnerabilidades

Mediante la realización de visitas al sitio y realizando las entrevistas respectivas al jefe del área, se identificaron las vulnerabilidades que pueden presentare en todos los servicios que presta la división de sistemas, considerando el tipo de amenazas a los cuales se exponen. Ver tabla 39.

4.3.1.1.6 Identificación de las consecuencias

Se describen las consecuencias o impactos que son detectados en los servicios que ofrece la división de sistemas, causadas por las vulnerabilidades encontradas, ver tabla 39.

Tabla 39:

Identificación de vulnerabilidades y consecuencias.

TIPO	AMENAZAS	VULNERABILIDAD	IMPACTO	DESCRIPCIÓN
Daño físico	Fuego	• No existen sensores de humo o alarma contra incendios en el área de sistemas. • Desconocimiento del procedimiento de emergencia ante un incendio. • Desconocimiento en el manejo de extintores • Existencia de materiales inflamables como escritorios caja de cartón, cubierta de machimbre etc., dentro del cuarto de servidores.	Pérdida de información y daño material en los equipos que se alojan en la dependencia en caso de producirse un incendio.	De llegarse a materializar dicha amenaza existiría la pérdida de la edificación y de todos los equipos servidores y de red que en esta se alojan. En este momento la solución de alta disponibilidad no sería efectiva ya está ubicada en la división de sistemas y esta debería estar en la sede de bellas artes.
	Daños por agua	• Posibilidad de ocurrencia de filtraciones de agua en época de invierno, en toda la dependencia de sistemas. • Ubicación inapropiada de los aires acondicionados dentro del cuarto de servidores, esto genera probabilidad de que en caso de falla de dichos aires afecten los equipos del área de servidores ubicados bajo ellos.	Daño en los equipos, ya que existe la posibilidad que el agua los afecte.	Los equipos de toda la dependencia y en especial los equipos servidores serían afectados por esta amenaza, afectando la disponibilidad de los servicios.
	Falla en los aires acondicionados	• Mal mantenimiento en los aires acondicionados • Condiciones inadecuadas de temperatura.	Recalentamiento de los equipos en especial en el área de servidores y cuarto de telecomunicaciones.	Al no existir un clima adecuado para los servidores y cuarto de telecomunicación están expuestos a altas temperaturas y podría afectar el funcionamiento interno de los mismos.

Perdida de los servicios esenciales	Corte de suministro de energía	• No se cuenta con una planta eléctrica para este tipo de incidentes. • Las UPS solo brindan energía en caso de emergencia por un lapso de 20 minutos. • La falta de mantenimiento de las puestas a tierra en los sistemas eléctricos podrían ser susceptibles a un corto circuito que podrían provocar la interrupción total o parcial de los servicios.	Los equipos sensibles a variaciones de voltaje serian afectados. No se garantizaría la disponibilidad de los servicios ante un corte de energía prologando.	Ante un corte de energía corto los SAI implementados en la división de sistemas darían respaldo a los servicios, pero si el tiempo del corte de energía se extiende más de 30 minutos no se podría garantizar la disponibilidad de los mismos y el personal del área no podría realizar las actividades asignadas.
	Destrucción de los equipos	• El control de acceso a las áreas críticas en la división de sistemas (sala de servidores), carece de medidas efectivas.	Disponibilidad de los equipos	Los controles de acceso a la división de sistemas son muy simples, al darse el caso de que alguien ingresara podría tener acceso a cualquier dispositivo.
Eventos naturales	Fenómenos climáticos	• Filtraciones de agua en la estructura de la dependencia.	Daño en los equipos de toda la dependencia	Los equipos se verían seria mente afectados al entra en contacto con el agua, afectando la disponibilidad de los mismos.
	Fenómenos sísmicos	• Falta de capacitación del personal sobre cómo actuar ante un evento de esta clase. • Carencia de salidas de emergencia y/o en su defecto las puertas empleadas en la división de sistemas pueden ocasionar atrapamiento del personal.	Accidentes de los funcionarios ante un evento de este tipo	Los funcionarios de la dependencia podrían sufrir accidentes ante un evento de alta magnitud, al no saber actuar ante dicha situación.
Perturbación debido a la radiación	Radiación	• Equipos UPS no cuentan con un cuarto o espacio adecuado para los mismos.	Personal expuesto a este tipo de campos.	La dependencia no cuenta con un cuarto especial para las UPS, el personal del área que labora diariamente en el cuarto de telecomunicaciones está expuesto a este tipo de campos, ya que las UPS están ubicadas en el mismo espacio

				de trabajo.
Compromiso de la información	Espionaje	• No existe un registro del monitoreo de los accesos SFTP desde afuera de la Universidad.	Acceso no autorizado, puede haber hurto o manipulación de la información a las cuales tienen acceso.	A los usuarios que tienen acceso SFTP de forma remota, no se lleva un monitoreo o registro sobre estos accesos.
	Hurto de equipos o documentos	• El área de servidores es utilizado como bodega para almacenar todo tipo de dispositivos (switches, Access Point, Patch paneles, etc.) siendo de fácil acceso para cualquier persona que ingrese a esta área. • Existe documentación en los escritorios de fácil acceso. • Seguridad física insuficiente. • El conocimiento de la información que se lleva en los formatos del proceso podría utilizarse para fines dañinos.	Robo, pérdida de dispositivos activos y pasivos.	Hay facilidad de acceso a todos los tipos de dispositivos que se encuentran en el área de servidores ya que no están alojados bajo llave, pueden ser hurtados por cualquier persona mal intencionado.
	Recuperación de medios reciclados o desechados	• No existe una política para la destrucción de material no utilizado (Discos duros), con información importante.	Robo de información	Actualmente el procedimiento para los equipos no utilizados es darlos de baja, y se traslada a la unidad de almacén, la información contenida en esos equipos no se destruye.
	Manipulación por Hardware	• Falta de seguridad en el rack del nodos de la emisora, los switches pueden ser manipulados • Protección física de equipos inadecuada • No se realiza filtrado por MAC para los equipos de la red. • Cuartos de telecomunicaciones principales como casona y anexos utilizados como bodegas.	Manipulación no autorizada de los equipos	En el nodo de la emisora el rack abarca los equipos transmisores de la estación de la misma y a su vez aloja el cableado estructurado del edificio siendo de fácil acceso para la manipulación.
	Manipulación por Software	• No existe un sistema de control de versiones para el desarrollo de las aplicaciones que se llevan a	Pérdidas de los archivos de configuración y/o desarrollo	Las aplicaciones no cuentan con un sistema de control de versiones que permita a los

		cabo en la dependencia. • Desconocimiento de los usuarios de las responsabilidades adquiridas al tener acceso a los sistemas de información		desarrolladores resarcir alguna modificación mal realizada.
Fallas técnicas	Falla de equipo	• Las altas temperaturas en el cuarto de servidores y telecomunicaciones pueden afectar el funcionamiento de los equipos. • No se tiene definido un procedimiento de respuesta a eventos e incidentes de seguridad • No existe switches de respaldo en caso de que uno de estos falle	Mal funcionamiento de los equipos. Disponibilidad de la conexión para uno o varios usuarios	Falta de mantenimiento a los aires acondicionados. Pérdida de comunicaciones en caso de daño de un swicth.
	Desconexión de puertos de los equipos	• Personal de limpieza y mantenimiento puede desconectar cables accidentalmente. • Protección física de equipos inadecuada	Los servicios se verían interrumpidos	Hay lugares en donde el cableado está expuesto y puede presentarse la desconexión del mismo de manera involuntaria.
Acciones no autorizadas	Uso no autorizado del equipo	• No se cuenta con sistemas IDS o IPS ataque informático	Denegación de servicios, hurto de información. No se dispone de un plan de contingencia ante un ataque informático.	El funcionamiento de los servicios se vería altamente afectado.
Compromisos de las funciones	Incumplimiento en la disponibilidad del personal Erro en el uso	• No existe documentación de la configuración de los servidores en caso que estos fallen. • Falta de conocimiento acerca de las políticas de seguridad de la información.	Falta de documentación afecta la operatividad de los servicios El usuario podría ejecutar acciones que comprometan la información.	Los servicios pueden verse afectados por falta de ausencia de personal en el área. El desconocimiento de las políticas y responsabilidades podría comprometer la información

Nota Fuente: Autores del Proyecto.

4.3.2 Estimación del riesgo

4.3.2.1 Metodologías para la estimación del riesgo

Como se describe en la norma, la metodología para la estimación del riesgo pueden ser cuantitativas, cualitativas o una combinación de las dos.

Para este análisis se empleó una metodología cuantitativa, que a través de esta se permita obtener un valor e identificar el nivel del riesgo y sea de fácil interpretación para el personal encargado de analizar los valores obtenidos.

4.3.2.2 Valoración de las consecuencias

La valoración de las consecuencias se refiere a la valoración de los impactos que se tienen como resultado del aprovechamiento de una vulnerabilidad, es decir la ocurrencia de una amenaza.

Esta valoración para cada grupo de activo se presenta en las tablas descritas en la evaluación del riesgo utilizando los criterios de valoración de impacto establecidos respectivamente en las tablas 30 y 31.

4.3.2.3 Valoración de los incidentes

Consiste en valorar la probabilidad de ocurrencia de alguna amenaza, teniendo en cuenta los acontecimientos de incidentes, los controles existentes, las experiencias adquiridas y lo que se pudo observar durante la visita a la dependencia. Para esto se utiliza los criterios de probabilidad de ocurrencia de una amenaza estipulados en la tabla 29.

4.3.2.4 Nivel de estimación del riesgo

Para realizar la estimación del riesgo se han definido los valores para probabilidad de ocurrencia de una amenaza y los impactos de acuerdo al tiempo sin funcionamiento del servicio y el impacto de acuerdo a la pérdida de confidencialidad, integridad y disponibilidad del activo. La valoración se hace teniendo en cuenta los criterios establecidos en el ítem 4.2.2 (Criterios básicos).

Luego de hacer la valoración de los criterios se procede hallar el nivel de evaluación del riesgo como se menciona en el ítem 4.2.2.4 (Criterios de evaluación del riesgo).

4.3.3 Evaluación del riesgo

Para desarrollar la evaluación del riesgo, se analiza en cada grupo de activos las vulnerabilidades que posee y las amenazas que puedan explotar dichas vulnerabilidades con el

fin de valorar la probabilidad de ocurrencia de las amenazas y el impacto que pudieran ocasionar en caso de materializarse y así obtener la evaluación del riesgo para dicho activo.

A continuación se presenta la evaluación del riesgo para cada grupo de activos que son de vital importancia para la dependencia de la división de sistemas. Este análisis servirá de base para realizar la evaluación del riesgo de cualquier servicio dentro de cada activo.

Para realizar esta evaluación de riesgos, se muestra a continuación un ejemplo del proceso que se llevó a cabo para la identificación de los mismos, teniendo en cuenta los criterios de probabilidad de ocurrencia de una amenaza (tabla 29) y los criterios de impacto (tablas 30 y 31) para luego obtener así el nivel del riesgo (tabla 32).

Activo. Bases de datos

Vulnerabilidad. No existe un sistema contra incendios dentro del área de servidores.

Impacto. Pérdida de los servidores que alojan estos sistemas, y pérdida de información.

Criterio de Probabilidad de ocurrencia. 3 (MP Muy Probable).

Impacto de acuerdo a que el activo se encuentre sin servicio. 2 (M medio).

Impacto de acuerdo a la perdida de confidencialidad, integridad y disponibilidad del activo. 4 (MG Muy grave).

Nivel de evaluación del riesgo. [(3*2*4) = 24] = Alto

Tabla 40:

Valoración del riesgo servicios de base de datos (Oracle, Mysql, Postgres).

Tipo de amenaza	Amenaza	Vulnerabilidad	Impacto	Probabilidad de ocurrencia de amenazas	Tiempo que el servicio se encuentra sin funcionamiento	Pérdidas de confidencialidad, integridad y/o disponibilidad de los activos	Nivel de riesgo
Daño físico	fuego	No existen sensores de humo o alarma contra incendios en el área de servidores.	Pérdida de información y daño material en los equipos que se alojan en la dependencia en caso de producirse un incendio.	1	4	4	16
	Daños por agua	Posibilidad de ocurrencia de filtraciones de agua en época de invierno, en toda la dependencia de sistemas	Daño en los equipos, ya que existe la posibilidad que el agua los afecte.	2	4	4	32
Perdida de los servicios esenciales	Falla en los aires acondicionados	Mal mantenimiento en los aires acondicionados	Recalentamiento de los equipos en especial en el área de servidores y cuarto de telecomunicaciones	3	1	1	3
	Corte de suministro de energía	No se cuenta con una planta eléctrica para este tipo de incidentes	No se garantizaría la disponibilidad de los servicios ante un corte de energía prologando.	3	4	1	12
	Destrucción de los equipos	El control de acceso a las áreas críticas en la división de sistemas (sala de servidores), carece de medidas efectivas.	Disponibilidad de los equipos	1	3	4	12
Eventos naturales	Fenómenos climáticos	Filtraciones de agua en la estructura de la dependencia.	Daño en los equipos de toda la dependencia	2	4	4	32

Compromiso de la información	Espionaje	No existe un registró del monitoreo de los accesos SFTP desde afuera de la Universidad.	Acceso no autorizado, puede haber hurto o manipulación de la información a las cuales tienen acceso	1	4	4	16
	Recuperación de medios reciclados o desechados	No existe una política para la destrucción de material no utilizado (Discos duros). Con información importante.	Robo de información	2	1	3	6
	Manipulación por Hardware	Cuartos de telecomunicaciones principales como casona y anexos utilizados como bodegas.	Manipulación no autorizada de los equipos	1	2	4	8
	Manipulación por Software	No existe un sistema de control de versiones para el desarrollo de las aplicaciones que se llevan a cabo en la dependencia	Pérdidas de los archivos de configuración y/o desarrollo	1	2	4	8
Fallas técnicas	Falla de equipo	Las altas temperaturas en el cuarto de servidores y telecomunicaciones pueden afectar el funcionamiento de los equipos.	Mal funcionamiento de los equipos	1	2	2	4
	Desconexión de puertos de los equipos	Protección física de equipos inadecuada	Los servicios se verían interrumpidos	1	4	2	8
Acciones no autorizadas	Uso no autorizado del equipo	No se cuenta con sistemas IDS o IPS	Denegación de servicios, hurto de información	2	4	4	32
		Ataque informático	Denegación de servicios, hurto de información	2	4	4	32
Compromisos de las funciones	Incumplimiento en la disponibilidad del personal	No existe documentación de la configuración de los servidores en caso que estos fallen.	Falta de documentación afecta la operatividad de los servicios	2	3	1	6
	Error en el uso	Falta de conocimiento	El usuario podría	4	1	1	4

		acerca de las políticas seguridad	ejecutar acciones que comprometan la información.				

Nota Fuente: Autores del proyecto.

En la tabla 40, valoración de riesgos en base de datos, se puede evidenciar que se cuenta con riesgos altos en las amenazas por agua y fenómenos climáticos, ya que se considera que la infraestructura con la que cuenta la dependencia tiene altas vulnerabilidades en el material con el cual está construido sus techos, el cual no es apto, presentando una alta probabilidad de un riesgo para la dependencia, afectando considerablemente las características de información, así mismo se pueden detectar otros riesgos altos como son las denegación en los servicios ya que no se cuenta con un sistema de detección ni prevención de intrusos que contrarrestar algún ataque informático. Por lo contrario se puede evidenciar un nivel de riesgo bajo como son los mantenimiento en los aires acondicionados y sus posibles fallas, ya que en el inicio del estudio realizado se encontró que uno de ellos no estaba en funcionamiento por daño, a pesar de dicha vulnerabilidad, no afecto el funcionamiento de las bases de datos, ni se afectó la información que se maneja la dependencia.

Tabla 41:

Valoración del riesgo servidores, UPS, computadores de escritorio, SAD1 y SAD2.

Tipo de amenaza	Amenaza	Vulnerabilidad	Impacto	Probabilidad de ocurrencia de amenazas	Tiempo que el servicio se encuentra sin funcionamiento	Pérdidas de confidencialidad, integridad y/o disponibilidad de los activos	Nivel de riesgo
Daño físico	fuego	No existen sensores de humo o alarma contra incendios en el área de servidores.	Perdida de información y daño material en los equipos que se alojan en la dependencia en caso de producirse un incendio.	1	4	4	16
		Existencia de materiales inflamables como escritorios caja de cartón, cubierta de machimbre etc. Dentro del cuarto de servidores.	Perdida de equipos	2	4	4	32
	Daños por agua	Posibilidad de ocurrencia de filtraciones de agua en época de invierno, en toda la dependencia de sistemas	Daño en los equipos, ya que existe la posibilidad que el agua los afecte.	2	4	4	32
		Ubicación inapropiada de los aires acondicionados dentro del cuarto de servidores, esto genera probabilidad de que en caso de falla de dichos aires afecten los equipos del área de servidores ubicados bajo ellos.	Daño en los equipos	3	4	4	48
Perdida de los servicios esenciales	Falla en los aires acondicionados	Mal mantenimiento en los aires acondicionados	Recalentamiento de los equipos en especial en el área de servidores y	3	2	2	12

			cuarto de telecomunicaciones				
	Corte de suministro de energía	No se cuenta con una planta eléctrica para este tipo de incidentes	No se garantizaría la disponibilidad de los servicios ante un corte de energía prologando.	3	4	4	48
		Las UPS solo brindan energía en caso de emergencia por un lapso de 20 minutos.	Servicios interrumpidos	2	4	2	16
		La falta de mantenimiento de las puestas a tierra en los sistemas eléctricos podría ser susceptible a un corto circuito que podría provocar la interrupción total o parcial de los servicios.	Equipos físicos expuestos ante un sistema a tierra sin revisión, daño en los equipos.	3	4	4	48
	Destrucción del equipos	El control de acceso a las áreas críticas en la división de sistemas (sala de servidores), carece de medidas efectivas.	Disponibilidad de los equipos	1	3	3	9
Eventos naturales	Fenómenos climáticos	Filtraciones de agua en la estructura de la dependencia.	Daño en los equipos de toda la dependencia	2	4	4	32
	Fenómenos sísmicos	No asegurar correctamente la ubicación de los equipos	Daño físico	2	3	3	18
Perturbación debido a la radiación	Radiación	Equipos UPS no cuentan con un cuarto o espacio adecuado para los mismos	Equipos del área de servidores y cuarto de telecomunicaciones expuestos a estos campos magnéticos.	3	2	1	6
Compromiso de la información	Hurto de equipos o documentos	El área de servidores es utilizado como bodega para almacenar todo tipo	Robo, pérdida de dispositivos activos y pasivos.	3	4	4	48

		de dispositivos (switches, Access Point, Patch paneles, etc.) siendo de fácil acceso para cualquier persona que ingrese a esta área.					
	Recuperación de medios reciclados o desechados	No existe una política para la destrucción de material no utilizado (Discos duros). Con información importante.	Robo de información	2	1	3	6
	Manipulación por Hardware	Cuartos de telecomunicaciones principales como casona y anexos utilizados como bodegas.	Manipulación no autorizada de los equipos	2	3	4	24
		Falta de seguridad en el rack del nodos de la emisora, los switches pueden ser manipulados	Acceso a los dispositivos	3	3	3	27
	Manipulación por Software	Desconocimiento de los usuarios de las responsabilidades adquiridas al tener acceso a los sistemas de información	Manipulación inadecuada	2	3	3	18
Fallas técnicas	Falla de equipo	Las altas temperaturas en el cuarto de servidores y telecomunicaciones pueden afectar el funcionamiento de los equipos.	Mal funcionamiento de los equipos	3	1	1	3
	Desconexión de puertos de los equipos	Protección física de equipos inadecuada	Los servicios se verían interrumpidos	2	3	3	18
Acciones no autorizadas	Uso no autorizado del equipo	No se cuenta con sistemas IDS o IPS (ataque informático)	Denegación de servicios, hurto de información	2	1	3	6
Compromisos de las	Incumplimiento en la	No existe documentación de la configuración de	Falta de documentación afecta la operatividad de	2	2	1	4

funciones	disponibilidad del personal	los servidores en caso que estos fallen.	los servicios				
	Error en el uso	Falta de conocimiento acerca de las políticas seguridad	El usuario podría ejecutar acciones que comprometan la información.	3	1	2	6

Nota Fuente: Autores del proyecto.

En la tabla 41, en la Valoración del riesgo servidores, UPS, computadores de escritorio, SAD1 y SAD2, se evidencia un alto riesgo de los activos, por su inadecuada ubicación dentro la infraestructura que actualmente los soporta, detectando mediante los instrumentos de análisis y recolección de información empleados, que la dependencia cuenta con un área muy reducida, razón por la cual la sala de servidores hace las veces también de bodega, almacenando equipos de comunicaciones (switches, Access Point, canaletas, etc.), así mismo se puede observar gran cantidad de material inflamable (cartón, plásticos, mesa de madera, etc.), que en caso de que ocurra un incendio afectaría gravemente los activos que se encuentran en el área y las características de la información se vieran comprometidas.

De igual manera se detecta grandes amenazas en la perdida de los servicios esenciales, debido a que la universidad a pesar que cuenta una ups de alta tecnología, no es suficiente para mantener los servicios en caso de un incidente general por un periodo de tiempo indeterminado, a pesar de que la dependencia ha gestionado la adquisición de una planta como se encontró en los oficios que se evidenciaron en la dependencia al inicio de la investigación, no ha sido satisfactorio la solución dada.

En dicha valoración se mantiene como riesgo moderado la ubicación de la UPS, dentro del cuarto de comunicación, manteniendo la vulnerabilidad que se evidencia en la infraestructura en el cual permanecen los activos de comunicación, que a pesar de que no es un riesgo alto, si se podría presentar fallas en los equipos a largo plazo, tanto por las radiaciones como por las altas temperaturas a las cuales se exponen en los momentos que se presentan fallas en los aires acondicionados por falta de mantenimiento periódico.

Tabla 42:

Valoración del riesgo Directorio activo, antivirus, backups, dns, servidor proxy-firewall dhcp.

Tipo de amenaza	Amenaza	Vulnerabilidad	Impacto	Probabilidad de ocurrencia de amenazas	Tiempo que el servicio se encuentra sin funcionamiento	Perdidas de confidencialidad, integridad y/o disponibilidad de los activos	Nivel de riesgo
Daño físico	fuego	No existen sensores de humo o alarma contra incendios en el área de servidores.	Perdida de información y daño material en los equipos que se alojan en la dependencia en caso de producirse un incendio.	1	4	4	16
	Daños por agua	Posibilidad de ocurrencia de filtraciones de agua en época de invierno, en toda la dependencia de sistemas	Daño en los equipos, ya que existe la posibilidad que el agua los afecte.	2	4	4	32
Perdida de los servicios esenciales	Falla en los aires acondicionados	Mal mantenimiento en los aires acondicionados	Recalentamiento de los equipos en especial en el área de servidores y cuarto de telecomunicaciones	3	1	1	3
	Corte de suministro de	No se cuenta con una planta eléctrica para este	No se garantizaría la disponibilidad de los	3	3	1	9

	energía	tipo de incidentes	servicios ante un corte de energía prologando.				
	Destrucción del equipos	El control de acceso a las áreas críticas en la división de sistemas (sala de servidores), carece de medidas efectivas.	Disponibilidad de los equipos	2	3	4	24
Eventos naturales	Fenómenos climáticos	Filtraciones de agua en la estructura de la dependencia.	Daño en los equipos de toda la dependencia	2	4	4	32
	Fenómenos sísmicos	Falta de capacitación del personal sobre cómo actuar ante un evento de esta clase.	Accidentes de los funcionarios ante un evento de este tipo	1	3	2	6
Compromiso de la información	Espionaje	No existe un registró del monitoreo de los accesos SFTP desde afuera de la Universidad.	Acceso no autorizado, puede haber hurto o manipulación de la información a las cuales tienen acceso	3	4	4	48
	Recuperación de medios reciclados o desechados	No existe una política para la destrucción de material no utilizado (Discos duros). Con información importante.	Robo de información	2	1	3	6
	Manipulación por Hardware	Control de acceso a la división de sistemas deficiente	Manipulación no autorizada de los equipos	2	3	4	24
	Manipulación por Software	Asignación errada de políticas y derechos de acceso para los clientes	Acceso no autorizada Abuso de privilegios	2	3	4	24
Fallas técnicas	Falla de equipo	Las altas temperaturas en el cuarto de servidores y telecomunicaciones pueden afectar el funcionamiento de los equipos.	Mal funcionamiento de los equipos	1	2	2	4

	Mal funcionamiento del software	No haber planificado una renovación oportuna de licencias (antivirus)	No se contaría con las actualizaciones respectivas	4	1	3	12
	Desconexión de puertos de los equipos	Protección física de equipos inadecuada	Los servicios se verían interrumpidos	1	4	2	8
Acciones no autorizadas	Uso no autorizado del equipo	No se cuenta con sistemas IDS o IPS (ataque informático)	Denegación de servicios, hurto de información	4	3	4	48
Compromisos de las funciones	Incumplimiento en la disponibilidad del personal	No existe documentación de la configuración de los servidores en caso que estos fallen.	Falta de documentación afecta la operatividad de los servicios	4	2	2	16
	Error en el uso	Falta de conocimiento acerca de las políticas seguridad	El usuario podría ejecutar acciones que comprometan la información.	4	3	3	27

Nota Fuente: Autores del proyecto.

En la tabla 42, Valoración del riesgo Directorio activo, antivirus, backups, dns, servidor proxy-firewall, dhcp, se detecta riesgos altos en estos activos, debido a que la dependencia de sistemas, aloja en su totalidad toda la información pública y privada de la universidad, lo que conlleva a que exista una amenaza latente antes tipos de ataques externos, al no contar con un sistema de monitoreo o registro sobre estos accesos. De igual manera en la valoración de estos activos, hay probabilidad de afectación alta por los daños físicos que puedan presentarse en la dependencia.

Los riesgos bajos en esta valoración se dan por la falta de mantenimiento periódico en los aires acondicionados. Como se menciona en la tabla 41, estos activos de soporte podrían verse afectados a largo plazo si no existe una temperatura adecuada para el correcto funcionamiento de los equipos que alojan estos servicios.

Tabla 43:

Valoración del riesgo Switches de acceso, telefonía análoga e IP, red de datos, red inalámbrica.

Tipo de amenaza	Amenaza	Vulnerabilidad	Impacto	Probabilidad de ocurrencia de amenazas	Tiempo que el servicio se encuentra sin funcionamiento	Perdidas de confidencialidad, integridad y/o disponibilidad de los activos	Nivel de riesgo
Daño físico	fuego	No existen sensores de humo o alarma contra incendios en el área de servidores.	Pérdida de información y daño material en los equipos que se alojan en la dependencia en caso de producirse un incendio.	2	4	4	32
		Existencia de materiales inflamables como escritorios caja de cartón, cubierta de machimbre etc. Dentro del cuarto de servidores.	Pérdida de información y daño material en los equipos que se alojan en la dependencia en caso de producirse un incendio.	3	4	4	48
	Daños por agua	Posibilidad de ocurrencia de filtraciones de agua en época de invierno, en toda la dependencia de sistemas	Daño en los equipos, ya que existe la posibilidad que el agua los afecte.	3	3	3	27
Pérdida de los servicios esenciales	Falla en los aires acondicionados	Mal mantenimiento en los aires acondicionados Condiciones inadecuadas de temperatura	Recalentamiento de los equipos en especial en el área de servidores y cuarto de telecomunicaciones	3	2	1	6

	Corte de suministro de energía	No se cuenta con una planta eléctrica para este tipo de incidentes	No se garantizaría la disponibilidad de los servicios ante un corte de energía prologando.	3	4	1	12
		Que los equipos no cuenten con las conexiones a tierra respectivas.	Daño de equipos	4	3	3	27
	Destrucción del equipos	El control de acceso a las áreas críticas en la división de sistemas (sala de servidores), carece de medidas efectivas.	Disponibilidad de los equipos	3	2	3	18
	Falla en los equipos de telecomunicaciones (Access point, switches)	Falla en la configuración de los parámetros que afectan los equipos	Funcionalidad de los equipos no es la adecuada.	1	3	2	6
		No se cuenta con un monitoreo de los equipos en la red	Monitoreo inadecuado de la red LAN	2	2	1	4
Eventos naturales	Fenómenos climáticos	Filtraciones de agua en la estructura de la dependencia.	Daño en los equipos de toda la dependencia	2	4	4	32
	Fenómenos sísmicos	Falta de capacitación del personal sobre cómo actuar ante un evento de esta clase.	Accidentes de los funcionarios ante un evento de este tipo	2	3	2	12
Compromiso de la información	Espionaje	No existe un registro por mac para el acceso de los equipos en los swicthes	Acceso no autorizado, puede haber suplantación de identidad.	3	4	4	48
	Recuperación de medios reciclados o desechados	No existe una política para la destrucción de material no utilizado (Discos duros). Con información importante.	Robo de información	1	2	2	4
	Hurto de equipos	Seguridad física insuficiente.	Hurto y/o manipulación de equipos	3	3	3	27
	Manipulación	Control de acceso a la	Manipulación no	2	3	1	6

	por Hardware	división de sistemas deficiente	autorizada de los equipos				
		Falta de seguridad en el rack del nodos de la emisora, los switches pueden ser manipulados	Hurto y/o manipulación de equipos	4	3	3	48
		Enlaces de cableado aéreo de fácil acceso	Corte de cables que afectaría la comunicación con otras dependencias.	4	4	2	32
	Manipulación por Software	Usuarios por defecto en los dispositivos con contraseñas débiles	Fácil acceso a los dispositivos	2	2	3	12
		Asignación errada de políticas y derechos de acceso para los clientes	Acceso no autorizada Abuso de privilegios	2	1	4	8
	Faltas de respaldo	No se respalda la información de configuración de los dispositivos (Switches, Access point.	Pérdida de información de configuración para respaldar el archivo ante un evento no deseado.	4	3	2	24
Fallas técnicas	Falla de equipo	Las altas temperaturas en el cuarto de servidores y telecomunicaciones pueden afectar el funcionamiento de los equipos.	Mal funcionamiento de los equipos	2	1	3	6
		No existe switches de respaldo en caso de que uno de estos falle	Continuidad de las operaciones en áreas críticas.	3	4	2	24
	Desconexión de puertos de los equipos	Personal de limpieza y mantenimiento puede desconectar cables accidentalmente.	Interrupción en las comunicaciones	2	3	2	12
Acciones no autorizadas	Uso no autorizado del equipo	No se cuenta con sistemas IDS o IPS (ataque informático)	Denegación de servicios, hurto de información	3	3	3	27
Compromisos de las funciones	Error en el uso	Uso inapropiado de software y/o hardware	Mal funcionamiento en los equipos y la plataforma tecnológica	1	2	2	4

			que soporta los servicios				
	Error en el uso	Falta de conocimiento acerca de las políticas seguridad	El usuario podría ejecutar acciones que comprometan la información.	2	1	3	6
	Error en el uso	No llevar registro de las modificaciones que se realizan en los equipos de conectividad	Perdida de información de la configuración de los equipos	3	2	2	12

Nota Fuente: Autores del proyecto.

En la tabla 43, Valoración del riesgo Switches de acceso, telefonía análoga e IP, red de datos, red inalámbrica, se evidencian riesgos altos en la falta de seguridad del rack ubicado en la emisora de la Universidad, el cual es compartido con los equipos de transmisión, estando expuestos a la manipulación inadecuada de los equipos que hacen parte de la división de sistemas, igualmente con la observación realizada, se pudo detectar que ciertos rack principales, no están siendo protegidos adecuadamente y están siendo expuestos a la manipulación de personal no autorizado, ya que se están utilizando estos cuartos como bodega; estando los activos principales de esta valoración en la división de sistemas, siguen estando propensos a las amenazas por daños físicos y fenómenos climáticos que se han venido mencionando en las otras valoraciones.

En los riesgos bajos, que se puedan presentar en esta valoración, pueden darse por la falta capacitación del personal en general de la universidad que tiene relación directa con la dependencia, el cual por desconocimiento y por la inadecuada conexión de los equipos, pues ser desconectados involuntariamente, presentándose una afectación mínima de los servicios.

Tabla 44:

Valoración del riesgo de las aplicaciones desarrolladas y las aplicaciones soportadas por la división de sistemas.

Tipo de amenaza	Amenaza	Vulnerabilidad	Impacto	Probabilidad de ocurrencia de amenazas	Tiempo que el servicio se encuentra sin funcionamiento	Perdidas de confidencialidad, integridad y/o disponibilidad de los activos	Nivel de riesgo
Daño físico	fuego	No existen sensores de humo o alarma contra incendios en el área de servidores.	Pérdida de información y daño material en los equipos que se alojan en la dependencia en caso de producirse un incendio.	2	3	3	18
	Daños por agua	Posibilidad de ocurrencia de filtraciones de agua en época de invierno, en toda la dependencia de sistemas	Daño en los equipos, ya que existe la posibilidad que el agua los afecte.	2	4	4	32
Pérdida de los servicios esenciales	Falla en los aires acondicionados	Mal mantenimiento en los aires acondicionados	Recalentamiento de los equipos en especial en el área de servidores y cuarto de telecomunicaciones	3	2	1	6
	Corte de suministro de energía	No se cuenta con una planta eléctrica para este tipo de incidentes	No se garantizaría la disponibilidad de los servicios ante un corte de energía prologando.	3	3	1	9
	Destrucción del equipos	El control de acceso a las áreas críticas en la división de sistemas (sala de servidores), carece de medidas efectivas.	Disponibilidad de los equipos	2	2	4	16
Eventos naturales	Fenómenos climáticos	Filtraciones de agua en la estructura de la dependencia.	Daño en los equipos de toda la dependencia	2	2	2	8
	Fenómenos	Falta de capacitación del	Accidentes de los	2	1	1	2

	sísmicos	personal sobre cómo actuar ante un evento de esta clase.	funcionarios ante un evento de este tipo				
Compromiso de la información	Espionaje	No existe un registró del monitoreo de los accesos SFTP desde afuera de la Universidad.	Acceso no autorizado, puede haber hurto o manipulación de la información a las cuales tienen acceso	2	2	4	16
	Recuperación de medios reciclados o desechados	No existe una política para la destrucción de material no utilizado (Discos duros). Con información importante.	Robo de información	1	2	2	4
	Manipulación por Hardware	Cuartos de telecomunicaciones principales como casona y anexos utilizados como bodegas.	Manipulación no autorizada de los equipos	3	2	3	18
	Manipulación por Software	No existe un sistema de control de versiones para el desarrollo de las aplicaciones que se llevan a cabo en la dependencia	Perdidas de los archivos de configuración y/o desarrollo	4	3	2	24
Fallas técnicas	Falla de equipo	Las altas temperaturas en el cuarto de servidores y telecomunicaciones pueden afectar el funcionamiento de los equipos.	Mal funcionamiento de los equipos	2	1	1	2
	Saturación del sistema de información	No existe planificación del procesamiento de las aplicaciones desarrolladas	Alto consumo de recursos y bajo rendimiento de las mismas	2	2	1	4
	Desconexión de puertos de los equipos	Protección física de equipos inadecuada	Los servicios se verían interrumpidos	2	3	1	6
Acciones no autorizadas	Uso no autorizado del	No se cuenta con sistemas IDS o IPS	Denegación de servicios, hurto de información	2	3	3	18

	equipo	Ataque informático	Denegación de servicios, hurto de información	2	4	4	32
Compromisos de las funciones	Incumplimiento en la disponibilidad del personal	No existe procedimientos para entrega de los desarrollos en caso de cambio de personal	Desarrollo de las aplicaciones sin supervisión.	2	4	1	8
	Error en el uso	Falta de conocimiento acerca de las políticas seguridad	El usuario podría ejecutar acciones que comprometan la información.	2	2	1	4
	Error en el uso	No existe documentación de los desarrollos	Disponibilidad de las aplicaciones	3	3	1	9
	Error en el uso	Uso inapropiado de software y/o hardware	Manipulación inadecuada de las aplicaciones	2	2	1	4

Nota Fuente: Autores del proyecto.

En la tabla 44,Valoración del riesgo de las aplicaciones desarrolladas y las aplicaciones soportadas por la división de sistemas, se evidencian riesgos altos por la alta probabilidad de ataques informáticos a los que estos se exponen, ya que al materializarse una acción no autorizada el riesgo seria considerable.

En las demás amenazas en esta valoración, se encuentran riesgos bajos, como la manipulación por software y los fenómenos sísmicos que tienen un poco influencia sobre este tipo de activos.

Tabla 45:

Valoración del riesgo / Personal.

Tipo de amenaza	Amenaza	Vulnerabilidad	Impacto	Probabilidad de ocurrencia de amenazas	Tiempo que el servicio se encuentra sin funcionamiento	Perdidas de confidencialidad, integridad y/o disponibilidad de los activos	Nivel de riesgo
Daño físico	fuego	Desconocimiento en el manejo de extintores	Pérdida de información y daño material en los equipos que se alojan en la dependencia en caso de producirse un incendio.	2	3	3	18
Pérdida de los servicios esenciales	Falla en los aires acondicionados	Mal mantenimiento en los aires acondicionados	Recalentamiento de los equipos del área de trabajo y temperatura ambiente bastante alta	2	1	1	2
	Corte de suministro de energía	No se cuenta con una planta eléctrica para este tipo de incidentes	No se garantizaría la disponibilidad de los servicios ante un corte de energía prologando.	2	4	1	8
	Destrucción del equipos	El control de acceso a las áreas críticas en la división de sistemas carece de medidas efectivas	Disponibilidad de los equipos	2	1	1	2
Eventos naturales	Fenómenos climáticos	Filtraciones de agua en la estructura de la dependencia	Daño en los equipos de toda la dependencia	2	3	1	6
	Fenómenos sísmicos	Falta de capacitación del personal sobre cómo actuar ante un evento de esta clase.	Accidentes de los funcionarios ante un evento de este tipo	2	3	3	18
Perturbación debido a la radiación	Radiación	No existe un cuarto especial para estos equipos	Personal expuesto a este tipo de campos	3	3	3	27

Compromiso de la información	Recuperación de medios reciclados o desechados	No existe una política para la destrucción de material no utilizado (Discos duros). Con información importante.	Robo de información	2	3	1	6
	Manipulación por Hardware	Utilización de medios extraíbles	Hurto de información	2	2	1	4
	Desconexión de puertos de los equipos	Protección física de equipos inadecuada	Los servicios se verían interrumpidos	2	2	1	4
Acciones no autorizadas	Uso no autorizado del equipo	No se cuenta con sistemas IDS o IPS	Denegación de servicios, hurto de información	2	2	1	4
		Ataque informático	Denegación de servicios, hurto de información	2	3	1	6
Compromisos de las funciones	Error en el uso	Falta de conocimiento acerca de las políticas seguridad	El usuario podría ejecutar acciones que comprometan la información.	2	2	1	4
	Error en el uso	No existe documentación de los desarrollos	Disponibilidad de las aplicaciones	3	3	1	9
	Error en el uso	Uso inapropiado de software y/o hardware	Manipulación inadecuada de las aplicaciones	2	2	1	4

Nota Fuente: Autores del proyecto.

En la tabla 45, Valoración del riesgo / Personal, no se evidencia riesgos muy altos, para este tipo de activos, los riesgos altos que se evidencian se da por la falta de capacitación del personal sobre eventos que afecten la integridad de los funcionarios activos en la dependencia, en cuanto a daños físicos y eventos naturales. Otro riesgo alto a los que se exponen es la exposición a los campos magnéticos que se dan por el área reducida de la dependencia.

A diferencia de las anteriores valoraciones, en el que el correcto funcionamiento de los aires acondicionados son de vital importancia, en esta valoración, tiene una afectación muy mínima, sobre este activo, ya que no afecta la operatividad, pero si la correcta adecuación del área de trabajo de cada funcionario.

Tabla 46:

Valoración del riesgo / centro de cómputo.

Tipo de amenaza	Amenaza	Vulnerabilidad	Impacto	Probabilidad de ocurrencia de amenazas	Tiempo que el servicio se encuentra sin funcionamiento	Perdidas de confidencialidad, integridad y/o disponibilidad de los activos	Nivel de riesgo
Daño físico	fuego	No existen sensores de humo o alarma contra incendios en el área de servidores.	Pérdida de información y daño material en los equipos que se alojan en la dependencia en caso de producirse un incendio.	3	3	4	48
	Daños por agua	Posibilidad de ocurrencia de filtraciones de agua en época de invierno, en toda la dependencia de sistemas	Pérdidas de equipos	3	3	4	48
		Tendido de cables expuestos a cortes, específicamente desde la entrada de la universidad hasta la división de sistemas	Falla en las comunicaciones	2	3	4	24
Pérdida de los servicios esenciales	Falla en los aires acondicionados	Mal mantenimiento en los aires acondicionados	Recalentamiento de los equipos en especial en el área de servidores y cuarto de telecomunicaciones	3	2	2	12
	Corte de	No se cuenta con una	No se garantizaría la	3	4	3	48

	suministro de energía	planta eléctrica para este tipo de incidentes	disponibilidad de los servicios ante un corte de energía prologando.				
	Destrucción del equipos	El control de acceso a las áreas críticas en la división de sistemas (sala de servidores), carece de medidas efectivas.	Disponibilidad de los equipos	2	3	4	24
Eventos naturales	Fenómenos climáticos	Filtraciones de agua en la estructura de la dependencia.	Daño en los equipos de toda la dependencia	2	3	3	18
	Fenómenos sísmicos	Falta de capacitación del personal sobre cómo actuar ante un evento de esta clase.	Accidentes de los funcionarios ante un evento de este tipo	2	3	3	18
Compromiso de la información	Espionaje	No existe un registró del monitoreo de los accesos SFTP desde afuera de la Universidad.	Acceso no autorizado, puede haber hurto o manipulación de la información a las cuales tienen acceso	2	3	3	18
	Recuperación de medios reciclados o desechados	No existe una política para la destrucción de material no utilizado (Discos duros). Con información importante.	Robo de información	2	2	4	16
	Manipulación por Hardware	Cuartos de telecomunicaciones principales como casona y anexos utilizados como bodegas.	Manipulación no autorizada de los equipos	3	2	4	24
		Enlaces aéreos de fácil acceso para su manipulación o daño	Falla en las comunicaciones	3	4	3	36
	Manipulación por Software	No existe un sistema de control de versiones para el desarrollo de las aplicaciones que se llevan a cabo en la dependencia	Pérdidas de los archivos de configuración y/o desarrollo	2	2	3	12

	Hurto de equipos o documentos	Existe documentación en los escritorios de fácil acceso	Hurto de información	3	1	4	12
		Controles de acceso deficientes	Hurto de equipos y de información	2	3	3	18
Fallas técnicas	Falla de equipo	Las altas temperaturas en el cuarto de servidores y telecomunicaciones pueden afectar el funcionamiento de los equipos.	Mal funcionamiento de los equipos	3	2	2	12
	Desconexión de puertos de los equipos	Protección física de equipos inadecuada	Los servicios se verían interrumpidos	2	3	1	6
Acciones no autorizadas	Uso no autorizado del equipo	No se cuenta con sistemas IDS o IPS (ataque informático)	Denegación de servicios, hurto de información	2	3	4	24
Compromisos de las funciones	Incumplimiento en la disponibilidad del personal	Ausencia de personal	No se puede dar soporte oportuno a los servicios que ofrece la dependencia	2	3	3	18
	Erro en el uso	Falta de conocimiento acerca de las políticas seguridad	El usuario podría ejecutar acciones que comprometan la información.	2	3	2	12
	Error en el uso	Apropiación del plan de continuidad establecido	Falla en las continuidad de las operaciones que se llevan en la dependencia	3	3	3	27
	Error en el uso	No existe un procedimiento de respuesta a eventos e incidentes de seguridad	Interrupción en los servicios	2	3	3	18

Nota Fuente: Autores del proyecto.

En la tabla 46, Valoración del riesgo / centro de cómputo, se evidencian riesgos muy altos y altos en las mayoría de las amenazas ya que en esta valoración se entra a evaluar la dependencia en su totalidad, en cuanto a su infraestructura y área en general, la cual deja ver la vulnerabilidad más importante al que esta expuestos todos los activos, ya que depende de una adecuada infraestructura y área apropiada, la protección necesarios que debe darse a los elementos que en este se encuentren.

En esta tabla no se evidencian riesgos bajos, debido a la importancia de estos activos. Pero si se presentan ciertos riesgos moderados a tenerse en cuenta para garantizar asi, la funcionalidad de los diferentes procesos y servicios que presta la división de sistemas a la comunidad en general.

Se puede concluir con las valoraciones realizadas, que la división de sistemas cuenta con una adecuada infraestructura tecnológica para dar soporte y prestar sus servicios a la comunidad en general; se pudo detectar que el riesgo mas alto en el que se encuentran estos activos es la inadecuada infraestructura física donde se alojan, ya que están propensos a amenazas naturales en una baja proporción y amenazas deliberadas e una gran proporción, ya que desde su exterior o diseños estructurales presentan fallas como es el caso de los ventanales en vidrio y techo en eternit, que no son los adecuados para esta dependencia de vital importancia para la institución.

Internamente se presentan fallas al no contar un área mas amplia donde se puedan alojar los activos principales de la dependencia, y todos aquellos equipos y elementos de comunicación (discos duros, cintas, switches, ect.), evidenciadose cajas de cartón, bolsas plásticas, falta de mantenimiento periódicos a los aires acondicionados y demás cerca a los servidores,

colocándolos a exposición de daños físcos e incluso pérdidas, aunque el acceso sea limitado no cuenta con un nivel de seguridad adecuado.

4.3.4 Tratamiento del riesgo

Teniendo en cuenta la evaluación de riesgo realizado, se contempla para este análisis la reducción de los mismos según como se indica en la sección 4.2.2.5, la cual contempla por parte de la división de sistemas la reducción de todos aquellos riegos que se encuentra.

A continuación se describen los riesgos que fueron detectados mediante la evaluación del riesgo y se menciona la medida control y/o recomendación que debe tenerse en cuenta para lograr la reducción del mismo.

Tabla 47:

Tratamiento del riesgo.

Ítem	RIESGO	CAUSA	CONTROL Y/O RECOMENDACIÓN
1	Daño físico de los equipos en el área de servidores y cuarto de telecomunicaciones	En la sala de servidores se encuentra un techo de eternit con machimbre, lo cual no es apto para este tipo de cuartos	Se recomienda asegurar la cubierta de la sala de servidores para evitar el ingreso de agua en tiempo de invierno y evitar el daño de los equipos, en su defecto colocar placa
2	Fácil acceso a los equipos	En la sala de servidores y el cuarto de telecomunicaciones se encuentra con ventanales de vidrio que no son de seguridad, siendo fáciles de romper y pueden causar un incidente por personal mal intencionado en contra de la institución afectando los equipos que en estas áreas se encuentran	Se recomienda para estas áreas instalar ventanas con vidrio capaces de soportar grandes presiones o en su defecto sería mejor sellarlos
3	Probabilidad y/u ocurrencia de incendio	Se encuentra en la sala de servidores y cuarto de	Se recomienda gestionar ante las altas directivas la creación de una

		telecomunicaciones materiales como cajas de cartón, escritorios de madera, materiales plásticos, etc., los cuales al generarse un corto o un incidente provocado por personas mal intencionadas pueden ocasionar un incendio	bodega para almacenar todos estos elementos, para evitar así la pérdida de equipos e información en caso de ocurrir un incidente
4	Pérdida de las réplicas y backup en caso de algún desastre	Se encontró en la sala de servidores las soluciones de alta disponibilidad, y una de estas la SAD 2, debe estar ubicada en la sede de bellas artes	Se recomienda gestionar la adecuación del cuarto de telecomunicaciones en la sede de bellas artes para albergar dicha solución. Con el fin de poder garantizar las disponibilidad de la información
5	Posibilidad de pérdida de información en caso de daño de equipos físicos	Se encontró en la sala de servidores, servicios en equipos físicos, que no han sido migrados a la solución de alta disponibilidad	Se recomienda realizar la migración de aquellos servicios que están equipos físicos a la solución de virtualización que se encuentra en los servicios de alta disponibilidad
6	Pérdida o daño en los equipos servidores	Se encontró los servidores físicos ubicados en escritorios de madera, lo cual no es recomendable ya que se puede iniciar un incendio por un corto	Se recomienda realizar la migración de los servidores físicos a los servidores de alta disponibilidad con el fin de eliminar estos equipos físicos
7	Pérdida de los activos (equipos, personal, entre otros) en caso de incendio.	Se encontró que en la sala de servidores y el cuarto de telecomunicaciones no existen dispositivos detectores de calor, de humedad ni contra incendios	Se recomienda la adquisición e instalación de estos dispositivos que son de vital importancia en estas áreas con el fin de prevenir un daño mayor ante un incidente
8	Retraso en el tiempo para el restablecimiento del servicio	Se encontró en el cuarto de telecomunicaciones que los switches y patch cord no se encuentran identificados	Se recomienda realizar el etiquetado respectivo para estos dispositivos para facilitar su identificación
		Se encontró que no existe un sistema de monitoreo de los equipos de red y las aplicaciones soportadas.	Se recomienda realizar la configuración de un sistema que permita el continuo monitoreo de los dispositivos
9	Manipulación, alteración, perdida de la información y de los equipos de TI	Se encontró que los controles de acceso al centro de cómputo son débiles	Se recomienda gestionar mecanismos de acceso biométrico y con huella dactilar a las áreas críticas y de igual forma ubicar cámaras de acceso de acceso a la dependencia
10	Retraso en el tiempo para el restablecimiento del servicio	Se encontró en la dependencia que los puntos de red no se encuentran rotulados sobre la canaleta	Se recomienda hacer el rotulado respectivo de los puntos de red para facilitar su identificación
11	Pérdida en los enlaces de	Se encontró que hay ciertos	Se recomienda organizar el

	comunicación, entre las dependencias de la institución.	enlaces que llegan de forma aérea a la división de sistemas y estos ingresan de una forma inadecuada al cuarto de telecomunicaciones, siendo de fácil acceso para personal malintencionado	tendido de cable aéreo que llega a la dependencia e ingresarlos por conductos subterráneos
		Se encuentra que el ingreso del cableado telefónico (11 líneas troncales) y la fibra óptica de TV san Jorge desde la portería de la universidad hasta el área de postgrados se realiza de forma aérea y está expuesta a cualquier tipo de acceso (caída de árboles, lluvia personal mal intencionado)	Se recomienda realizar la instalación de ductos para realizar el tendido de cables desde la entrada de la universidad hasta el área de postgrados
12	Daño en la infraestructura de la dependencia	A fueras de la división de sistemas se encuentra una palmera de bastante envergadura que en caso de presentarse una fuerte tormenta puede romperse y afectar las instalaciones	Se recomienda hacer la gestión ante la oficina de planeación con el fin de realizar un estudio sobre la posibilidad de retirar la palmera del área
		Antena de Internet sin luces de aproximación aérea, que puede ocasionar accidentes aéreos por cercanías con el batallón	Se recomienda realizar el cambio del bombillo de señalización en la antena de Internet
13	Robo o perdidas de información confidencias	Se encontró que en algunos puestos de trabajo existe documentación de fácil acceso	Se recomienda aplicar la política de escritorios limpios con el fin de evitar el hurto de información sensible
		Se encontró que en algunos equipos de trabajo no está configurados el sistema de protección de pantalla por tiempo de inactividad	Se recomienda realizar una revisión en los equipos del área y configurar los sistemas de protección de pantalla por inactividad
14	Tratamiento inadecuado de la información y de los recursos por desconocimiento de las políticas de seguridad	Se encontró unas políticas de seguridad establecidas y aprobadas pero que no están socializadas	Se recomienda hacer la socialización, capacitación y continua realimentación de las policías de seguridad que fueron aprobadas con el fin de que sean utilizadas y conocer su finalidad
15	Acceso indebido a la información	Se encuentra que no se tienen configurados sistemas como IDP o IPS para los accesos indebidos a la información	Se recomienda realizar la configuración de un sistema de prevención de intrusos para prevenir posibles ataques
16	Altos Tiempo en el restablecimiento y/o continuidad de los servicios	No se encuentra un plan de continuidad establecido	Se recomienda gestionar la creación un plan de continuidad para todos los procedimientos y/o actividades que soporta la división

			de sistemas
		Se encuentra que no existen los procedimientos escritos para el restablecimiento de los servicios en caso de pérdida de información	Se recomienda realizar la documentación respectiva de los procedimientos que se llevan a cabo para el restablecimiento de los servicios en caso de pérdida de información
		No se existe documentación de ciertas aplicaciones que son desarrolladas por la división de sistemas	Se recomienda establecer las políticas que deben seguirse para el desarrollo de software y en su defecto realizar la documentación de las aplicaciones ya desarrolladas
17	Daño físico al personal de la división de sistemas	No existe identificación de la delimitación de las áreas críticas ni la señalización de las rutas de evacuación ante un evento inesperado	Se recomienda hacer la señalización respectiva de las áreas críticas y la señalización de las rutas de evacuación

Nota Fuente: Autores del proyecto.

Conclusiones

El análisis de riesgos desarrollado en la dependencia de la división de sistemas basado en la norma ISO:IEC 27005/2011, permitió clasificar los activos, con los que cuenta la dependencia, identificar las amenazas y vulnerabilidades de los mismos y a su vez el nivel de importancia para cada uno de estos.

El establecimiento del contexto permitió definir los criterios básicos que establece la norma y seguir los lineamientos que esta menciona para su correcto desarrollos, es de vital importancia mencionar que es el primer análisis de riesgos que se realiza en la dependencia basado en la norma; lo que permitió de una forma metódica poder identificar los riesgos a los que esta área se expone.

El análisis de riesgos deja ver que tan alto es el riesgo a los que los que los activos se exponen y a partir de estos se plantea unas recomendaciones que a través del tratamiento deben darse a las amenazas encontradas.

Es de vital importancia resaltar que este análisis dejo ver las falencias que existen en el áreas y sienta los precedentes para tomar las acciones necesarias que permitan garantizar a una eficiente funcionalidad de los diferentes servicios que presta la división de sistemas.

Referencias

Angarita, A., Tabares, C. (2012). Análisis de riesgos para el proceso administrativo: Departamento de informática en la empresa de acueducto y alcantarillado de Pereira S.A E.S.P, basados en la Norma ISO 27005. Universidad Tecnológica de Pereira. Pereira.

ASCANIO SANCHEZ, Sandra Liliana CARDENAS ESTUPIÑAN, Yuraima Karina y QUINTERO QUINTERO, Erika Tatiana. "Guía de gestión de riesgos para el departamento de sistemas de la empresa apuestas Cúcuta 75." Trabajo de Grado. Especialista en Auditoria de Sistemas. Ocaña: Universidad Francisco de Paula Santander. Facultad de Ingeniería. Departamento de Especialización en Auditoría de Sistemas. (2015), 133 p.

COPNIA. (2012). Administración del riesgo. [En línea] Disponible en: https://copnia.gov.co/uploads/filebrowser/DCALIDAD/RMpr01%2520ADMINISTRACION%2520DEL%2520RIESGO.pdf.

DECONCEPTOS. (Sin fecha). [En línea] Disponible en: http://deconceptos.com/general/informacion.

DEPARTAMENTO ADMINISTRATIVODE FUNCIÓN PÚBLICA. (2006). Guía de administración del riesgo. [En línea] Disponible en: file:///C:/Users/Sofia/Downloads/GUIA_ADMINISTRACION_DEL_RIESGO_-_DAFP.pdf.

DEPARTAMENTO ADMINISTRATIVO DE FUNCIÓN PÚBLICA. (2011). [En línea] Disponible en: http://portal.dafp.gov.co/portal/pls/portal/formularios.retrive_publicaciones?no=1592.

DEPARTAMENTO DE LA FUNCIÓN PÚBLICA. (Sin fecha). Riesgos_DAFP. [En línea] Disponible en: http://pgcltda.com/inicio/files/RIESGOS_DAFP.pdf.

De Salas, C., Arriaga, E., Pla, E. (2006). Guía para auditorías para el sistema de gestión de prevención de riesgos laborales. [En línea] Disponible en: https://books.google.com.co/books?isbn=8479787880.

ESPINOZA RODRIGUEZ, Indira del Valle GOMEZ CARVAJAL, Virginia Carolina. "Análisis de los riesgos operativos y ocupacionales existentes en el departamento de ingeniería de petróleo de la universidad de oriente de Anzoátegui" Trabajo de grado. Ingeniero Industrial. (2009), 265 p.

INTERNATIONAL STANDARD ISO/IEC 27005:2011. (2011). Information technology – Security techniques – Information security risk management. [En línea] Disponible en: http://nsa.wkall.se/litteratur/iso_iec_27005-2011.pdf.

NORMA ISO/IEC 27000. (Sin fecha). Sistema de gestión de la seguridad de la información. [En línea] Disponible en: http://www.iso27000.es/download/doc_sgsi_all.pdf .

OSORIO RIVERO, Yenis Piedad y PÉREZ PÉREZ, Yesica María. "Diseño de una política de gestión de riesgos de la información para la dependencia de admisiones registro y control de Universidad Francisco de Paula Santander Ocaña." Trabajo de Grado. Especialista en Auditoria de Sistemas. Ocaña: Universidad Francisco de Paula Santander. Facultad de Ingeniería. Departamento de Especialización en Auditoría de Sistemas, (2014), 166 p.

UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA. (2011). Manual de funciones y de competencias laborales. [En línea] Disponible en: https://ufpso.edu.co/ftp/pdf/manuales/gh/M-GH-DRH-001BII.pdf.

UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA. (2014). Sistema de información institucional. [En línea] Disponible en: https://divisis.ufpso.edu.co/contenido/15/sistemas-de-informacion.html.

UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA. (2014). División de sistemas. [En línea] Disponible en: https://divisis.ufpso.edu.co/contenido/10/presentacion.html.

UNIVERSIDAD NACIONAL DEL NORDESTE. (Sin fecha). Conceptos fundamentales. [En línea] Disponible en: http://exa.unne.edu.ar/ingenieria/computacion/Tema1.pdf

UNIVERSIDAD OBERTA DE CATALUNYA. (2008). Posgrados. [En línea] Disponible en: http://www.uoc.edu/masters/oficiales/img/913.pdf.

VMware. (Sin fecha). [En línea] Disponible en: http://www.vmware.com/co/products/vcenter-server/features.html.

Apéndices

Apéndice A. Formato de comunicación y consulta del riesgo

COMUNICACIÓN Y CONSULTA DE RIESGO	Código:	DS-GR-01
	Versión:	01
	Elaborado:	21-07-2016

COMUNICACIÓN Y CONSULTA DE RIESGO		
COMUNICANTE	Fecha:	Dependencia:
	Nombre:	Cargo:

COMUNICADO	Riesgo:
	Causa:
	Consecuencia:

ACCIONES / DESICIONES	**FECHA**	**RESPONSABLES (S)**

Conclusiones:
Recomendaciones:

Apéndice B. Formato de valoración y tratamiento de riesgo

VALORACION Y TRATAMIENTO DEL RIEGSO	Código:	DS-GR-02
	Versión:	01
	Elaborado:	21-07-2016

Dependencia:		**Responsable:**			
Riesgo	**Fuente de riesgo**	**Área de Impacto**	**Evento**	**Causa**	**Consecuencia**

ANALISIS Y EVALUACION DEL RIESGO										
Control existente	**Está documentado**		**Se aplica el control**		**Minimiza el riesgo**		**Calificación del control**	**Impacto**	**Probabilidad**	**Nivel de riesgo**
	Si	No	Si	No	Si	No				

TRATAMIENTO DEL RIESGO					
Opción de tratamiento	**Acciones**	**Responsable**	**Recursos**	**Tiempo o fecha de ejecución**	**Periodicidad del monitoreo**

Elaborado por:	Fecha:
Revisado por:	Fecha:
Aprobado por:	Fecha:

Apéndice C. Formato de monitoreo y revisión del riesgo

MONITOREO Y REVISION DEL RIESGO			Código:	DS-GR-03
			Versión:	01
			Elaborado:	21-07-2016
Riesgo	**Fecha**	**Logros**	**Reportado A**	**Observaciones**

Elaborado por:	Fecha:
Revisado por:	Fecha:
Aprobado por:	Fecha:

Apéndice D. Acta de apertura de auditoría

ACTA DE APERTURA DE AUDITORIA

Análisis de riesgos informáticos de la dependencia División de Sistemas adscrita a la sud dirección académica de la UFPSO, basada en la norma ISO/IEC 27005:2011.

OBJETIVO: Realizar Análisis de riesgos informáticos de la dependencia División de Sistemas adscrita a la sub dirección académica de la UFPSO, basada en la norma ISO/IEC 27005:2011.
OBJETIVOS ESPECIFICOS: • Realizar un diagnóstico de la situación real de riesgos informáticos en la que se encuentra la División de Sistemas adscrita a la sub dirección académica de la UFPSO. • Elaborar el establecimiento del contexto que permita establecer los criterios para el análisis de riesgos correspondientes. • Realizar el análisis de riesgos identificando las amenazas, vulnerabilidades y hallar el nivel de riesgo. • Formular el tratamiento del riesgo basado en el análisis desarrollado.
ALCANCE: Identificar los riesgos mediante la aplicación de la norma ISO/IEC 27005:2011

FECHA: 1 de Abril del 2016
HORA: 3:00 pm
LUGAR: División de Sistemas UFPS Ocaña

ASISTENCIA

La reunión de apertura para el desarrollo de la auditoria basada en la norma ISO/IEC 27005:2011, contara con las siguientes personas.

Por parte del área auditada
Magister Antón García Barreto
Jefe de División de Sistemas

Por parte del grupo auditor
Leonardo Zambrano
Claudia Álvarez Romero
Julia Barbosa Llain

PRESENTACION:

El auditor líder realizo la presentación de cada uno de los integrantes del equipo de auditoria. Luego se realiza una descripción de la pretensión sobre la auditoria que se desea llevar a cabo, donde se aclara que esta se hará con fines académicos, y contara con la

confidencialidad necesaria del caso, al momento de la utilización de la información suministrada por la parte auditada.

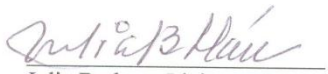
Teniendo en cuenta el aval por parte del Jefe de la División de sistemas, se estipula que el día 4 de abril, se dará comienzo a la auditoria y se contara con el apoyo para el desarrollo de dicha actividad.

En constancia firma,

Magister Antón García Barreto
Jefe División de sistemas

Leonardo Zambrano Z
Leonardo Zambrano
Auditor Líder

Claudia Alvarez Romero
Auditor



Julia Barbosa Llain
Auditor

Apéndice E. Plan de auditoría

PLAN DE AUDITORIA

EMPRESA:	Universidad Francisco de Paula Santander Ocaña		
Dirección:	Sede Algodonal		
Representante:	Antón García Barreto		
Cargo:	Jefe División de Sistemas	Correo electrónico / Teléfono:	anton@ufpso.edu.co 3115322027
Alcance: Identificar los riesgos mediante la aplicación de la norma ISO/IEC 27005:2011			
CRITERIOS DE AUDITORIA:	ISO/IEC 27005:2011		
Tipo de auditoria:	☐ OTORGAMIENTO	**X SEGUIMIENTO**	☐ RENOVACION
	☐ AMPLIACIÓN		☐EXTRAORDINARIA
Auditoría multisitio:	☐ Si X No		
Reunión de Apertura:	2016-04-01	Hora:	3:00 p.m
Reunión de Cierre:	2016-29-07	Hora:	5:00 p.m

Con un cordial saludo, me dirijo a usted para remitir el plan de la Auditoria que se realizará a la dependencia basado en la norma ISO/IEC 27005:2011

Por favor indique en la columna correspondiente, el nombre y cargo de las personas que atenderán cada entrevista y devolverlo a mi correo electrónico.

Para el balance diario de información del equipo auditor le agradezco disponer de una oficina o sala, así como también de acceso la documentación del sistema de gestión.

Para la reunión inicial le pido el favor de disponer un proyector para computador.

En cuanto a las condiciones de seguridad y salud en el trabajo aplicables a su organización, por favor informarlas previamente al inicio de la auditoría y disponer el suministro de los equipos de protección personal necesarios.

La información que se conozca por la ejecución de esta auditoria será tratada confidencialmente, por parte del equipo auditor y la empresa que audita.

El idioma de la auditoria y su informe será el español.

Los objetivos de la auditoría son:

- Realizar un diagnóstico de la situación real de riesgos informáticos en la que se encuentra la División de Sistemas adscrita a la sub dirección académica de la UFPSO.
- Elaborar el establecimiento del contexto que permita establecer los criterios para el análisis de riesgos correspondientes.
- Realizar el análisis de riesgos identificando las amenazas, vulnerabilidades y hallar el nivel de riesgo.
- Formular el tratamiento del riesgo basado en el análisis desarrollado.

Auditor Líder:	Leonardo Zambrano Z	Correo electrónico	leozam@ufpso.edu.co
Auditor:	Claudia Patricia Álvarez Romero	Auditor	Julia Barbosa LLain
Experto técnico:	Leonardo Zambrano Zambrano		

FECHA	HORA	PROCESO / ACTIVIDAD / REQUISITO POR AUDITAR	AUDITOR	CARGO Y NOMBRE
2016-04-01				
	3:00	INICIO DE LA AUDITORIA (PRESENTACION E INFORME DE LA AGENDA A TRATAR)	CLAUDIA ALVAREZ	
	3:30	SEGURIDAD FISICA - LOGICA	CLAUDIA ALVAREZ	
	4:00	ANALISIS DE RIESGOS	CLAUDIA ALVAREZ	
	4:15	GRUPO DE TRABAJO Y ROLES	CLAUDIA ALVAREZ	
	4:30	IDENTIFICACIÓN DE EVENTOS Y MEDIDAS PREVENTIVAS	CLAUDIA ALVAREZ	
	4:50	REUNION DE CIERRE	CLAUDIA ALVAREZ	
NOTA: La programación se puede ajustar de acuerdo al desarrollo y duración de las entrevistas.				
Observaciones:				
1. Favor disponer, para el día de la auditoria , los siguientes documentos: ➢ Una copia magnética del Plan de contingencia de TI.				

En constancia Firma

Magister Antón García Barreto
Jefe de División de Sistemas

Apéndice F. Encuesta realizada al jefe de división de sistemas de la Universidad Francisco de Paula Santander Ocaña

ENCUESTA REALIZADA AL JEFE DE DIVISION DE SISTEMAS DE LA UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA

Fecha: 29-06-2016

Nombre del encuestado: Arturo Garcia Barreto

Objetivo: Recopilar información que permita identificar los riesgos que afecten el correcto funcionamiento de la dependencia de la división de sistemas de la Universidad Francisco de Paula Santander Ocaña.

PREGUNTA	SELECCIONE
1. Los sistemas de información cuentan con un análisis de auditoria que permitan realizar una verificación o estudio sobre los cambios y/o modificaciones que fueron realizados por los funcionarios que tienen acceso a estos.	SI X NO ___
2. Se cuenta con un sistema de versiones que permita establecer el control de cambios que llevan los desarrollos en la dependencia.	SI ___ NO X
3. Se tienen establecidos los procedimientos para realizar las actualizaciones de los diferentes sistemas de información que se alojan en los servidores, y estos cuentan con el registro respectivo.(Ej actualización de versiones)	SI ___ NO X
4. Se tienen definidas claras y detalladamente las políticas de seguridad dentro de la dependencia	SI X NO ___
5. En caso de que la pregunta anterior fuera afirmativa, están se encuentran aprobadas por un comité o acta que las avale.	SI X NO ___
6. Los usuarios tienen conocimiento sobre la responsabilidad que tienen al darles acceso a los sistemas de información.	SI ___ NO X

7. Cuenta la dependencia con algún comité de apoyo que ayude a mejorar los procesos de seguridad de la información.	SI ____ NO X
8. Como considera que se encuentra la infraestructura de la seguridad en las bases de datos que soportan los diferentes sistemas de información que son soportados por la dependencia.	MUY BUENA____ BUENA X REGULAR____ MALA____
9. Cuenta la dependencia con un organigrama previamente autorizado o validado mediante u comité administrativo	SI ____ NO X
10. Las actividades que realizan los funcionarios de la infraestructura tecnológica son registrados para poder ser objeto de auditoria.	SI X NO____
11. Actualmente se han realizado simulacros de perdida de información estableciendo un término de respuesta por parte de los responsables para el restablecimiento de la misma	SI X NO____
12. Los controles de acceso al cuarto de servidores y al cuarto de comunicaciones como los considera	MUY BUENA____ BUENA X REGULAR____ MALA____
13. Se cuenta con un sistema de detección de incendio dentro de la dependencia,	SI ____ NO X
14. Teniendo en cuenta que se encuentra algunos extintores, el personal del área cuenta con alguna capacitación que permita la manipulación adecuada de los mismos en caso de presentarse alguna conflagración.	SI X NO____
15. Teniendo en cuenta que la electricidad en un factor importante para mantener la disponibilidad de los servicios, cuenta la dependencia con las medidas necesarias para dar respaldo en caso de una falla de energía	SI X NO____

16. Si la respuesta anterior fue afirmativa, se tiene un registro de los tiempos que estos soportan y de igual manera documentado las fallas eléctricas que se prestan en la dependencia.	SI X NO ___
17. Las instalaciones de datos y eléctricos son revisadas periódicamente y cuenta con el registró respectivo	SI X NO ___
18. Se cuentan con enlaces de Internet que respalden la caída de los servicios en caso de una falla en el canal principal.	SI X NO ___
19. Teniendo en cuenta que se tiene un Core de Swicthes de 75, se tiene en inventario algunos que den respaldo en caso de que estos fallen.	SI ___ NO X
20. Se tiene configurados sistemas como IDP o IPS para los accesos indebidos a los sistemas de información y a la red de datos que administra la dependencia	SI ___ NO X
21. Están definidas y socializadas las políticas sobre el uso de correo electrónico dentro de la institución.	SI X NO ___
22. Los equipos de desarrollo cuentan con el licenciamiento respectivo del software instalado.	SI X NO ___
23. Se realizan capacitaciones sobre el uso que debe darse a la información y como utilizar los recursos tecnológicos que se encuentran en el área.	SI ___ NO X
24. Los planos de red están debidamente actualizados y documentados con el fin de tener un mejor control a la hora de solucionar algún incidente.	SI X NO ___

Apéndice G. Entrevista realizada al jefe de división de sistemas de la Universidad Francisco de Paula Santander Ocaña

ENTREVISTA REALIZADA AL JEFE DE DIVISION DE SISTEMAS DE LA UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA

Fecha: 24-06-2016

Nombre del entrevistado: Anton Garcia Borrero

Objetivo: Recopilar información que permita identificar los riesgos que afecten el correcto funcionamiento de la dependencia de la división de sistemas de la Universidad Francisco de Paula Santander Ocaña.

1. De acuerdo a lo encontrado en el plan de contingencia, revisado y aprobado por usted, como podría detallar que se encuentra en seguridad física el centro de cómputo de la UFPSO.
   En estudio, no se cuenta con seguridad física apropiada
2. La dependencia ante un riesgo externo, cuenta con alguna alternativa establecida para minimizar la perdida de información en su área.
   backup, replicacion y un RBO contratado con un ente externo para copias de seguridad.
3. Los equipos dentro de la dependencia cuentan con algún sistema de protección de tal forma que la información que estos maneja no se vea afectada:
   Antivirus, y congelador de particiones.
4. La información que se aloja en los servidores cuenta con las copias de seguridad respectivas para el restablecimiento de las mismas, menciones los procedimientos.
   Si, en un datacenter externo, con su procedimiento escrito

5. Se hace una verificación de que las copias de los servidores se hallan realizado correctamente.

   Si

6. Cuenta con algún lugar de respaldo que permita el restablecimiento de los servicios en caso de que falle alguno de los servidores o en su totalidad.

   Se encuentra configurado el DRP, pero falta las adecuaciones físicas en bellas artes

7. Considera usted actualmente la sala de servidores es apta y contempla los requerimientos mínimos que aseguren el funcionamiento de cada uno de los equipos que allí se encuentran.

   No

8. Dependiendo del grado de dificultad ante un falla presentada los funcionarios encargados tienen un tiempo de respuesta para la solución de dicha eventualidad: Si, depende de la falla

9. Se encuentran definidos los procedimientos para el restablecimiento de los servicios en caso de pérdida de la información

   No, se hacen pero no estan exactos.

10. Existe algún criterio de clasificación de la información dentro de la dependencia.

    SI____Mencionelos._____

    _____NO X

11. Cuantos aplicativos o sistemas son soportados por la dependencia. (37). Mencionelos.

12. De los sistemas anteriormente mencionados cuales son desarrollados por personal externo a la dependencia. (17).
Menciónelos

13. Que servicios presta a los sistemas de información que no son administrados por la división de sistemas.
Hosting, backup, dns, base de datos.

14. Los desarrollos de información soportados por la división de sistemas están debidamente documentados. SI____, haga una breve descripción de dichos documentos. Si, pero no completo
NO ____

15. Los desarrollos soportados por la división de sistemas cuentan con la seguridad pertinente que garanticen la integridad de la información. SI X, Justifique su respuesta.
falta la parte física
NO___

16. Los sistemas de información desarrollados por la división de sistemas, se han basado en alguna metodología. SI X, Menciónela
Scrum, en un 30%
NO___

17. Siendo la información el principal activo de la dependencia, como se garantiza la integridad, disponibilidad y confidencialidad, que esta suministra a los usuarios, de una breve descripción.

Alta disponibilidad, Replicacion y backup

18. Se tiene algún control para evitar que la información que se aloja en los servidores y a la cual los usuarios de la dependencia acceden, sea manipulada de forma indebida (Ej. Copiada, Inserción de código malicioso, consultas indebidas etc.) SI X, de una breve descripción.

Aplican ~~Sobo~~ hardening y ethical hacking 1 vez al año

NO

19. A nivel de cuarto de telecomunicaciones en los edificios principales ¿Qué medidas de seguridad se han tomado para mejorar el espacio y acceso a estos?

Se ha solicitado a planeacion la adecuacion fisica de centro de datos de la sede alvaro nal y sede bellas artes.

Apéndice H. Diferencias en las definiciones entre la ISO/IEC 27005:2008 y ISO/IEC 27005:2011

Nota: Este anexo está dedicado para los usuarios de la ISO/IEC 27001:2005. Como algunos términos y definiciones son diferentes en la guía ISO 73:2009 en comparación con los utilizados en la norma ISO/IEC 27001:2005, y posteriormente en la norma ISO/IEC 27005:2008, este anexo resume todos los cambios pertinentes.

Términos definidos en la ISO/IEC 27005:2008	Términos definidos en la ISO/IEC 27000:2009 usados en la ISO/IEC 27005:2008	Términos definidos en ISO, Guía 73:2009 usados en la ISO/IEC 27005:2011
n/a	**n/a**	**3.1** **Consecuencia** Resultado de un evento (3.3) que afectan los objetivos [ISO Guía 73:2009] Nota 1. Un evento puede dar lugar a una serie de consecuencias. Nota 2. Una consecuencia puede ser cierta o incierta y en el contexto de la seguridad de la información usualmente suele ser negativa. Nota 3. Las consecuencias pueden ser expresadas cualitativas o cuantitativamente. Nota 4. Inicialmente las consecuencias pueden escalar a través de efectos en cadena.
n/a	Control Los medios de gestión de riesgos,	**3.2** **Control** Medir la modificación del riesgo (3.9)

	incluyendo políticas, procedimientos, directrices, prácticas o estructuras organizativas, pueden ser administrativos, técnicos, de gestión o de naturaleza legal.	[ISO Guía 73:2009] Nota 1. Los controles para la seguridad de la información incluyen cualquier proceso, política, procedimiento, directriz, practica o estructura organizativa, que puede ser administrativo, técnico, de gestión o de naturaleza legal que modifican los riesgos para la seguridad de la información. Nota 2. Los controles no siempre pueden ejercer el efecto previsto sobre la modificación asumida. Nota 3. El control también se utiliza como sinónimo de garantía o contramedida.
n/a	**n/a**	**3.3** **Eventos** Ocurrencia de un cambio o de un conjunto particular de circunstancias. [ISO Guía 73:2009] Nota 1. Un evento puede ser una o más ocurrencias, y puede tener varias causas Nota 2. Un evento puede consistir en algo no sucede Nota 3. Un evento puede ser a veces referido como un “incidente” o un “accidente”.
n/a	**n/a**	**3.4** **Contexto externo** Ambiente externo en que la organización trata de alcanzar sus objetivos.

		[ISO Guía 73:2009] Nota. Contexto externo pude incluir: - Lo cultural, social, político, legal, normativo, financiero, tecnológico, económico, natural y competitivo ya sea internacional, nacional, regional o local. - Los factores claves y las tendencias que tienen los impactos en los objetivos de la organización, y la relación con las percepciones y valores de los actores externos.
3.1 **Impacto** Cambios adversos en los niveles del negocio sobre los objetivos trazados		La definición ha sido eliminada.
3.2 **Riesgo de seguridad de la información** Altamente probable que una amenaza dada explotara vulnerabilidades de un activo o grupo de activos y por lo tanto causa daño a la organización. Nota. Se mide en términos de una combinación de la probabilidad de un evento y su consecuencia.		La definición ha sido eliminada (ver nota 6 en 3.9)
n/a	**n/a**	**3.5** **Contexto interno** Ambiente interno, en que la organización trata de alcanzar sus objetivos. [ISO Guía 73:2009]

		Nota. El contexto interno puede incluir: - El gobierno, la estructura de la organización, las funciones y responsabilidades, políticas, objetivos y las estrategias que están en su lugar para lograrlos. - Las capacidades entendidas en términos de recursos y conocimientos (Por ejemplo, de capital, de tiempo, personas, procesos, sistemas y tecnologías). - Percepciones y valores de los grupos de interés internos. - Sistemas de información, flujos de información y la toma de decisiones procesos (formales e informales). - Relaciones y las percepciones de valor interno con las partes interesadas. - La cultura de la organización. - Norma, directrices y modelos adoptados por la organización. - Forma y el alcance de las relaciones contractuales.
n/a	**n/a**	**3.6** **Niveles de riesgos** Magnitud de un riesgo (3.9), expresado en términos de la combinación de consecuencias (3.1) y su probabilidad (3.7) [ISO Guía 73:2009]
n/a	**n/a**	**3.7 Probabilidad** Probabilidad de que algo suceda

		[ISO Guía 73:2009] Nota 1. En términos de gestión de riegos, la palabra “probabilidad” se utiliza para referirse a la probabilidad de que ocurra algo, ya sea definido, medido o determinado de forma objetiva o subjetiva, cualitativa o cuantitativamente, y se describe en términos generales o matemáticamente (como una probabilidad o una frecuencia durante un periodo de tiempo dado). Nota 2. En ingles el término “probabilidad” no tiene un equivalente directo en algunas lenguas; en su lugar, se utiliza a menudo el equivalente de la expresión “probabilidad”. Sin embargo, en inglés es normalmente interpretado como un término matemático. Por lo tanto, en la terminología de la gestión de riesgos, la “probabilidad” debe tener la misma interpretación que tiene en muchos idiomas distintos al inglés.
n/a	**Riesgo residual** Es el riesgo que permanece después del tratamiento del riesgo	**3.8 Riesgo residual** Es el riesgo que permanece después del tratamiento del riesgo. [ISO Guía 73:2009] Nota 1. El riesgo residual pude contener el riesgo no identificado. Nota 2. El riesgo residual también puede ser conocido como “riesgo retenido”.
	Riesgo	**3.9**

	Combinación de la probabilidad de un evento y su consecuencia.	**Riesgo** Efecto de incertidumbre de los objetivos [ISO Guía 73:2009] Nota 1. Un efecto es la desviación de lo esperado. Positivo y/o negativo. Nota 2. Los objetivos pueden tener diferentes aspectos (tales como financieros, de salud y seguridad, de seguridad de la información, el medio ambiente y sus objetivos) y se puede socializar en diferentes niveles (estratégicos, de toda la organización, proyecto o producto y proceso. Nota 3. El riesgo se caracteriza a menudo por referirse a posibles eventos (3.3) y consecuencias (3.1), o a la combinación de estas. Nota 4. El riesgo en la seguridad de la información es también expresado en términos de una combinación de consecuencias de un evento en la seguridad de la información asociado a la probabilidad (3.9) de ocurrencia. Nota 5. La incertidumbre en el estado, de un evento parcial, de la deficiencia de la información relacionada, con la comprensión o conocimiento de un evento, su consecuencia o la probabilidad.

		Nota 6. El riesgo en la seguridad de la información está asociado potencialmente con amenazas que van a explotar las vulnerabilidades de un activo de información o conjunto de activos de información y por lo tanto causan daño a una organización.
n/a	**Análisis de riesgos** Uso sistemático de la información para identificar fuentes y para estimar el riesgo Nota El análisis de riesgo proporciona una base para la evaluación del riesgo, el tratamiento del riesgo y la aceptación del riesgo. [ISO/IEC 27001:2005]	**3.10** **Análisis de riesgos** Proceso de comprender la naturaleza del riesgo y determinar el nivel del riesgo (3.6) [ISO Guía 73:2009] Nota 1. El análisis de riesgo provee la base para la evaluación y decisiones acerca del tratamiento del riesgo. Nota 2. El análisis de riesgo incluye la estimación del riesgo.
n/a	**Evaluación del riesgo** Proceso global de análisis de riesgo y evaluación del riesgo. [ISO/IEC 27001:2005]	**3.11** **Evaluación del riesgo** Proceso global de identificación de riesgos (3.15), análisis de riesgos (3.10) y evaluación del riesgo (3.14) [ISO Guía 73:2009]
3.3 **Evitación del riesgo** Decisión de no involucrarse, o en su medida, retirarse ante una situación de riesgo [ISO/IEC Guía 73:2002]		Este término se encuentra cubierto en el tratamiento del riesgo.

3.4 **Comunicación del riesgo** Canje o intercambio de información sobre el riesgo entre la toma de decisiones y las partes interesadas.		**3.12** **Comunicación y consulta del riesgo** Proceso continuo e iterativo que una organización emprende para proporcionar, compartir u obtener información y entablar un dialogo con las partes interesadas (3.18), con respecto a la gestión del riesgo (3.9) [ISO/IEC 73:2009] Nota 1. La información puede relacionarse con la existencia, naturaleza, forma, verosimilitud, importancia, la evaluación, la aceptación y el tratamiento del riesgo. Nota 2. La consulta es un proceso bidireccional de comunicación informados entre una organización y sus partes interesadas, sobre un tema antes de tomar una decisión o determinación de una dirección en ese tema. La consulta es: - Un proceso que incide sobre una decisión a través de influencias en lugar de poder. - Un insumo para la toma de decisiones, no una decisión conjunta.
n/a	**n/a**	**3.13** **Criterios del riesgo** Términos de referencia contra lo cual el significado de un riesgo (3.9) se evalúa. [ISO Guía 73:2009]

		Nota 1. Los criterios de riesgo se basan en los objetivos de la organización, y en el contexto externo e interno. Nota 2. Los criterios de riesgo pueden derivarse de normas, leyes, políticas y otros requerimientos.
3.5 **Estimación del riesgo** Proceso para asignar valores a la probabilidad y consecuencia de un riesgo [ISO/IEC Guía 73:2002] Nota1. En el contexto de esta norma internacional, el término "actividad" se utiliza en lugar del término "proceso" para la estimación del riesgo. Nota 2. En el contexto de esta norma internacional el término "posibilidad" se utiliza en lugar del término "probabilidad" para la estimación del riesgo.		La definición ha sido eliminada
n/a	**Evaluación del riesgo** Proceso de comparación de la estimación del riesgo contra los criterios de riesgo para determinar la importancia del riesgo. [ISO/IEC 27001:2005]	**3.14** **Evaluación del riesgo** Proceso de comparación los resultados del análisis de riesgo (3.10) con los criterios de riesgo (3.13) para determinar si el riesgo y/o su magnitud son aceptables o tolerables. [ISO Guía 73:2009]

		Nota La evaluación del riesgo ayuda a la decisión sobre el tratamiento del riesgo.
3.6 **Identificación del riesgo** Proceso para encontrar, enumerar y caracterizar los elementos del riesgo. [ISO/IEC Guía 73:2002] Nota. En el contexto de esta norma internacional, el término "actividad" se utiliza en lugar del término "proceso" para la identificación del riesgo.		**3.15** **Identificación del riesgo** Proceso de buscar, reconocer y describir los riesgos. [ISO Guía 73:2009] Nota 1. La identificación de riesgos consiste en la identificación de fuentes de riesgo, los acontecimientos, sus causas y sus posibles consecuencias. Nota 2. La identificación de riesgos puede implicar datos históricos, análisis teóricos, informes y opiniones de expertos y las necesidades de los interesados.
n/a	**Gestión del riesgo** Actividades coordinadas para dirigir y controlar una organización con respecto a los riesgos.	**3.16** **Gestión del riesgo** Actividades coordinadas para dirigir y controlar una organización con respecto a los riesgos. [ISO Guía 73:2009] Nota. Esta norma internacional utiliza el término "proceso" para describir la gestión del riesgo en general. Los elementos dentro del proceso de gestión de riesgos se denominan "actividades".
3.7		Este término es remplazado por

Reducción del riesgo Acciones adoptadas para disminuir la probabilidad de consecuencias negativas, o ambas, asociadas con un riesgo. [ISO/IEC Guía 73:2002] Nota. En el contexto de esta norma internacional el término "posibilidad" se utiliza en lugar del término "probabilidad" para la estimación del riesgo.		"modificación del riesgo" y actualmente está cubierto en el tratamiento del riesgo.
3.8 **Retención del riesgo** Aceptación de la carga, pérdida o beneficio de la ganancia de un riesgo particular. [ISO/IEC Guía 73:2002] Nota. En el contexto de los riesgos en la seguridad de la información, solo las consecuencias negativas (pérdidas), son consideras en la retención del riesgo.		Este término está cubierto actualmente en el tratamiento del riesgo.
3.9 **Transferencia del riesgo** Compartir con la otra parte, la carga, pérdida o beneficios de ganancia de un riesgo. [ISO/IEC Guía 73:2002] Nota. En el contexto de los riesgos en la		Este término es remplazado por "riesgo compartido" y actualmente está cubierto en el tratamiento del riesgo.

seguridad de la información, solo las consecuencias negativas (pérdidas), son consideras para la transferencia del riesgo.		
n/a	**Tratamiento del riesgo** Proceso de selección e implementación de medidas, para modificar el riesgo. Nota. En esta norma internacional el término "control" se utiliza como sinónimo de "medida". [ISO/IEC 27001:2001]	**3.17** **Tratamiento del riesgo** Proceso para modificar el riesgo [ISO Guía 73.:2009] Nota 1. El tratamiento del riesgo puede involucrar: - Evitar el riesgo al decidir no iniciar o continuar con la actividad que da lugar a un riesgo. - Tomar o aumentar el riesgo con el fin de perseguir una oportunidad. - La eliminación de la fuente del riesgo. - Cambiar la probabilidad. - Cambiar las consecuencias. - Compartir el riesgo con la otra parte o partes (incluidos los contratos y financieramente el riesgo), y retener el riesgo por la elección tomada. Nota 2. El tratamiento de riesgos que tienen que ver con las consecuencias negativas son a veces denominadas: "mitigación de riesgos", "eliminación de riesgos", "prevención de riesgos" y "reducción de riesgos". Nota 3. El tratamiento del riesgo puede crear

		nuevos riesgos o modificar los riesgos existentes.
n/a	**n/a**	**3.18** **Partes interesadas** Persona u organización que puede afectar, o ser afectada, por una decisión o actividad percibida por ellos mismos. Nota. Una decisión puede ser tomada por las partes interesadas. [ISO Guía 73:2009]
	Amenaza Una causa potencial de un incidente no deseado, que puede resultar en daño a un sistema u organización.	La definición actual de la norma ISO/IEC 27000:2009 se aplica