FACULTAD DE INGENIERÍA Y CIENCIAS AGROPECUARIAS

DESARROLLO DE POLÍTICAS DE SEGURIDAD DE REDES PARA EL DATA CENTER ACADÉMICO DE LA FICA

Trabajo de Titulación presentado en conformidad con los requisitos establecidos para optar por el título de Ingeniero en Electrónica y Redes de Información.

Profesor guía

Magister William Eduardo Villegas Chiliquinga

Autor

Andrés Fernando Espinosa Mantilla

Año

2017

DECLARACIÓN DEL PROFESOR GUÍA

“Declaro haber dirigido este trabajo a través de reuniones periódicas con el estudiante, orientando sus conocimientos y competencias para un eficiente desarrollo del tema escogido y dando cumplimiento a todas las disposiciones vigentes que regulan los Trabajos de Titulación”.

_____

William Eduardo Villegas Chiliquinga
Magister En Redes de Comunicación
C.I: 1715338263

DECLARACIÓN DEL PROFESOR CORRECTOR

“Declaro haber revisado este trabajo, dando cumplimiento a todas las disposiciones vigentes que regulan los Trabajos de Titulación”.

_____

Luis Santiago Criollo Caizaguano
Magister En Redes de Comunicación
C.I: 1717112955

DECLARACIÓN DE AUTORÍA DEL ESTUDIANTE

“Declaro que este trabajo es original, de mi autoría, que se han citado las fuentes correspondientes y que en su ejecución se respetaron las disposiciones legales que protegen los derechos de autor vigentes.”

_____

Andrés Fernando Espinosa Mantilla

C.I: 1003201827

AGRADECIMIENTOS

El presente trabajo de titulación se elaboró gracias a la colaboración del Ing. Ángel Jaramillo y el Ing. William Villegas, a quienes expreso mi profundo agradecimiento por su dirección y valiosa asesoría. Un especial agradecimiento a mi madre, a mi abuela y familia por su apoyo en este largo caminar.

DEDICATORIA

Dedico este trabajo de titulación a Dios por indicarme el camino, así como darme la fuerza y determinación para cumplir con mis objetivos. A mi familia, amigos, profesores que supieron orientarme y compartir momentos enriquecedores. Para todos ellos el presente trabajo.

RESUMEN

El manejo de la información siempre debe asociarse con los elementos que la almacenan, gestionan y protegen, por lo cual conocer a los mismos y poder determinar cuáles serán sus riesgos es un tema de suma importancia. Dada esta premisa, el enfoque provisto a este trabajo de titulación es proveer un manual para manejar el data center académico de la FICA, enfocado en mejores prácticas y teniendo como guía normas internacionales como las que provee la UNE/ISO en su sección 27000.

Primeramente, se identificarán los activos que componen al data center individualmente, presentando en tablas las características más relevantes a tener en cuenta, a continuación, serán ingresados en un software que cumpla los requerimientos que indican las normas ISO.

Al momento de determinar las posibles amenazas, se debe tener en consideración el grado de importancia de cada activo de manera individual y la semejanza que tenga uno con otro, para así que hereden posibles peligros.

Una vez determinadas las posibles amenazas se realiza una guía de mejores prácticas o políticas, que son herramientas de prevención, haciendo realce en los peligros detectados previamente.

Para expresar de manera más comprensible los resultados en cada capítulo existen tablas, matrices, gráficos, además anexos indicando los componentes más relevantes del data center - obviamente guardando la discreción dada la relevancia de los mismos- que solventan un mejor entendimiento.

ABSTRACT

The management of information must always be associated with elements that store, manage and protect it. Therefore, knowing them and being able to determine what their risks will be is a very important issue. Given this premise, the provided approach to this titling work is to offer a manual to manage FICA the academic center data. The manual is focused on best practices and guided by international standards such as those provided by ISO in its section 27000.

Firstly, the components, which make up the data center, were identified individually, presented in the tables the most relevant characteristics to consider. Then they are entered into a software which have all the requirements indicated by ISO standards.

At the time of determining the possible threats, it is important to consider the degree of relevance of each asset individually and its similarity to each other so that they may inherit potential dangers.

Once identified the possible threats, a guide to best practices or policies is made, which are prevention tools, highlighting the hazards previously detected.

In order to express in a more understandable form the results, in each chapter there are tables, matrices, graphs, and annexes which indicates the most relevant components of the data center - obviously keeping discretion given the relevance of the same ones - that solve a better understanding.

ÍNDICE

ÍNDICE DE FIGURAS

INDICE DE TABLAS

1. CAPÍTULO I. INTRODUCCIÓN

1.1 Generalidades

La globalización trae consigo un sinfín de posibilidades, en el ámbito del manejo de la información no es diferente, ya que uno de los preceptos del nacimiento del internet fue la distribución equitativa de los recursos que puede proporcionar la información.

Una cita común al uso que se le da a la web es que “En internet hay lobos y corderos. Si no eres lobo, te toca ser cordero” (Chema Alonso, 2016), por lo cual el aspecto de seguridad debe siempre ser bien enfocado, así como ser la primera respuesta y preventiva ante cualquier amenaza.

Por esta razón las normas previstas por la ISO (International Organization for Standardization) para el correcto manejo de información y la seguridad que se debe tener al manipularla es sumamente importante. Por lo cual las normas manejadas en este trabajo de titulación como lo son la ISO 27001 y la 27002, nos provee de herramientas para enfrentar los retos de un mundo globalizado como en el que vivimos hoy en día.

1.2 Antecedentes

El aspecto de la seguridad en temas de infraestructura en general siempre se ha visto menospreciado, pese a la constante evolución en términos de conexión, equipos, velocidad de transferencia, etc. Siempre este aspecto de seguridad se ha tratado de manera renuente al momento de tomar decisiones y aplicarlas en consenso a una infraestructura.

La terminología que propicia la palabra seguridad es amplia, así mismo al momento de hablar del tema podemos abordar varios aspectos, por lo cual el enfoque que se da en este trabajo está dirigido hacia el Data Center que actualmente está por implementarse en la Facultad de Ingeniería y Ciencias Agropecuarias. Debido a ello, la información acerca de políticas, infraestructura en hardware y software, mantenimiento y mejora, requiere que se use(n)

norma(s) de entidades que hacen énfasis en lineamientos de Plan de Seguridad Informático.

1.3 Justificación

Las entidades universitarias, debido a la creciente cantidad de alumnos que registran además de los que ingresan periodo a periodo- tienen como particular interés establecer condiciones adecuadas en temas de manejo y seguridad informática por lo cual se entiende la creciente demanda de mejoras en ámbitos de seguridad, razón por la cual no puede ser tratado como un tema sin relevancia, ya que los datos que se manejan de un ser humano, están amparados por los derechos de los mismos, haciéndose de vital importancia el planteamiento de mejoras y aplicaciones de técnicas en el buen manejo de la información.

1.4 Objetivos

1.4.1 Objetivo General

Realizar una propuesta técnica de infraestructura y políticas de seguridad adaptadas al Data Center académico de la FICA, teniendo de referencia los estándares UNE-ISO/IEC 27001 y UNE-ISO/IEC 27002 aplicable para las políticas de seguridad.

1.4.2 Objetivos Específicos

- Identificar los activos en la infraestructura técnica que permitan diagnosticar, evaluar y diseñar procedimientos para brindar soporte y seguridad a la información.
- Elaborar una matriz de riesgo de la seguridad del Data Center.
- Diseñar verificadores de cumplimiento de las políticas de seguridad definidas por la UNE-ISO/IEC 27002.

1.5 Alcance

El alcance de este trabajo de titulación es una propuesta a una infraestructura por implementarse en la Facultad Ingeniería y Ciencias Agropecuarias en las carreras de Ingeniería Electrónica y Redes de la Información e Ingeniería en Redes y Telecomunicaciones en la Universidad de las Américas, por lo cual el estudio se hará en forma progresiva y a la vez se entregará el análisis de la infraestructura, normas aplicables, políticas, buenas prácticas, de tal manera

que se proponga una mejora a la implementación de la misma, por esta razón se usarán técnicas de manejo de seguridad, otorgadas por entidades relacionadas con el tema, como la ISO, IEEE etc.

Para alcanzar el cumplimento de lo mencionado anteriormente se aplicará los conocimientos adquiridos a lo largo de la carrera, haciendo énfasis en materias como: Seguridad de Redes, Seminario de Redes, Marco Regulatorio de Telecomunicaciones, además del uso de herramientas de software.

2. CAPÍTULO II. FUNDAMENTACIÓN TEÓRICA

2.1 Seguridad de la Información

Se puede definir como el área de la informática que tiene por objetivo primordial resguardar la infraestructura computacional de potenciales ataques que afecten la integridad de la información.

La finalidad del proceso que cumple la seguridad de la información no es solo brindar protección a la información, sino a todo el proceso que comprende esta protección como:

- Acceso
- Uso
- Divulgación
- Interrupción
- Destrucción No Autorizada

2.1.1 Acceso a la Información

Es el proceso que se define como el conjunto de métodos que sirven para explorar, categorizar, cambiar y entrar a la información que se encuentra en un sistema, este sistema puede encontrarse en diferentes ambientes como: bases de datos, internet, bibliotecas, archivos, expedientes, etc.…

Una característica fundamental de este concepto es el hecho que es aplicado a la información ya procesada para que sea útil al entendimiento humano, o incluso al procesamiento automático de determinado sistema programado para así hacerlo.

2.1.2 Uso de la Información

Para dar una definición debemos partir del principio que este uso debe ser ético, por lo cual debe tener la premisa de seguir objetivos como los siguientes:

- Propiciar el incremento de conocimiento del usuario para disminuir las alternativas lógicas posibles.
- Generar una materia prima de calidad para que el usuario encargado de la toma de decisiones proporcione acertados planteamientos.
- En el aspecto de control, entregar un ciclo de pautas de evaluación y decisión para fines de comprobación.

2.1.3 Divulgación de la Información

Divulgar un comentario o criterio siempre debe ser enfocado a enriquecer las mentes, es una promulgación común, por lo cual la tarea de difundir información procesada es de vital importancia.

El concepto en sí que aglomera la propagación de información puede ser amplio, el enfoque de definición que se da en este trabajo es el procesamiento y transmisión de conocimiento científico de tal forma que resulte comprensible al usuario final.

2.1.4 Interrupción de la Información

En el enfoque informático que se busca promover en este trabajo se lo define como un paréntesis temporal que se da a la ejecución de determinado procedimiento.

En pocas palabras es una señal enviada, para ejecutar una instrucción de pausa, esto permite al administrador de la información generar un recurso

adicional, para realizar un cambio o simplemente detener transitoriamente el proceso.

2.1.5 Destrucción No Autorizada de la Información

La viabilidad en el tema de la seguridad de la información, con el paso del tiempo ha ido tomando mayor influencia, sea cualesquiera el ámbito en el que se almacene y administre, por lo cual el acceso no autorizado a los recursos informáticos es sumamente riesgoso, es uno de los aspectos más críticos, donde intervienen las políticas a ser mencionadas en este trabajo, las cuales dotarán de herramientas para así evitar violaciones de seguridad y la perdida de bienes tan valiosos.

2.2 Activo

Partiendo del significado de activo que se refiere a cualquier elemento que tiene valor para la entidad, por ende voluble a sufrir ataques, sea este tangible o intangible, se desarrollará este concepto, así como su identificación, clasificación y valoración dependiendo de la disponibilidad, confidencialidad, autenticidad, integridad y trazabilidad.

- Disponibilidad. - probabilidad de que una persona o cosa, en este caso sistema, esté presente cuando se la necesite.

- Confidencialidad. - característica que presenta la información, por la cual solo el personal debidamente autorizado puede entrar a la misma.

- Autenticidad. - es la garantía de que determinado elemento es verdadero o confiable.

- Integridad. - se menciona que tal persona o elemento es íntegro cuando, no ha sufrido modificaciones, por lo cual posee sus segmentos intactos.

- Trazabilidad del uso del servicio. - la Oficina Asesora de Sistemas la define como “el cuestionamiento de qué daño causaría no saber a quién se le presta tal o cual servicio, o desconocer quién hace uso del mismo

qué y cuándo" (Universidad Distrital Francisco José de Caldas Oficina Asesora de Sistemas, 2011).

2.2.1 Identificación de Activos

La identificación de activos se puede considerar el primer peldaño para iniciar un proceso, como el que se define de objetivo a realizar en este trabajo. Para identificar el contexto que abarca la palabra activo, se ha definido previamente su significado, y el parámetro a tomar en cuenta para la identificación de activos es la data a manejarse.

La norma española UNE-ISO/IEC 27000 indica como activos los siguientes componentes o funcionalidades:

A. "la información

B. los recursos lógicos, como las aplicaciones informáticas y el software

C. los recursos físicos, por ejemplo un ordenador o el hardware

D. los servicios

E. el personal y sus cualificaciones, competencias y experiencia

F. los recursos intangibles, como la reputación y la imagen" (Comité técnico AEN/CTN 71 Tecnología de la información cuya Secretaría desempeña AMETIC, 2012, p.7).

2.2.2 Clasificación de Activos

Esta clasificación se realizará dependiendo del tipo de amenaza que pueden ocasionar diferentes clases de inconvenientes, respecto a la finalidad que tiene cada activo para cumplir su rol de funcionalidad dentro de la organización. En esta etapa se utilizará la herramienta PILAR Análisis y Gestión de Riesgos; la misma que asocia y organiza los activos por capas, por ello se define: "Las capas no tienen ningún impacto en análisis de riesgos: es solamente una

manera de organizar los activos para una mejor comprensión y comunicación" (PILAR Ayuda y Gestión de Riesgos, p.43). Por consiguiente, se ligará cada activo a su respectiva capa.

2.2.3 Valoración de Activo

Una vez concluido el proceso de clasificación se debe tomar en cuenta la definición realizada previamente respecto a las características que determinan a un activo. La herramienta PILAR Análisis y Gestión de Riesgos, con la que se desarrollará la presente tesis utiliza dos sistemas evaluadores: el cuantitativo y el cualitativo. El segundo fue elegido para proseguir con el presente trabajo de titulación. El sistema cualitativo explica que el método de calificación se basa en los riesgos tomando en consideración criterios proporcionados por la siguiente tabla:

Tabla 1.

Escala para una valoración cualitativa

Escala de Valoración	Valor	Descripción
MB: Muy Bajo	1	Irrelevante para efectos Prácticos
B: Bajo	2	Importancia menor para el desarrollo del proyecto
M: Medio	3	Importante para el proyecto
A: Alto	4	Altamente importante para el proyecto
MA: Muy Alto	5	De vital importancia para los objetivos que persigue el proyecto

Tomado de (Universidad Distrital Francisco José de Caldas, 2016)

2.3 Riesgos

Un riesgo se puede definir como el imprevisto que impide que se logre determinado objetivo en una organización o proyecto. Los autores de Introducción a Riesgo Informático citan en su publicación "La Organización Internacional por la Normalización (ISO) define riesgo tecnológico (Guías para la gestión de la seguridad de TI/TEC TR 13335-1, 1996) como: "La probabilidad de que una amenaza se materialice, utilizando vulnerabilidades existentes de

un activo o un grupo de activos, generándole pérdidas o daños”.” (Sena & Tenzer, p. 2).

2.3.1 Identificación de Riesgos

El proceso de identificación se lo ejecutará mediante posibles escenarios de ataques, esta fase es explicada gráficamente mediante un árbol de amenazas:

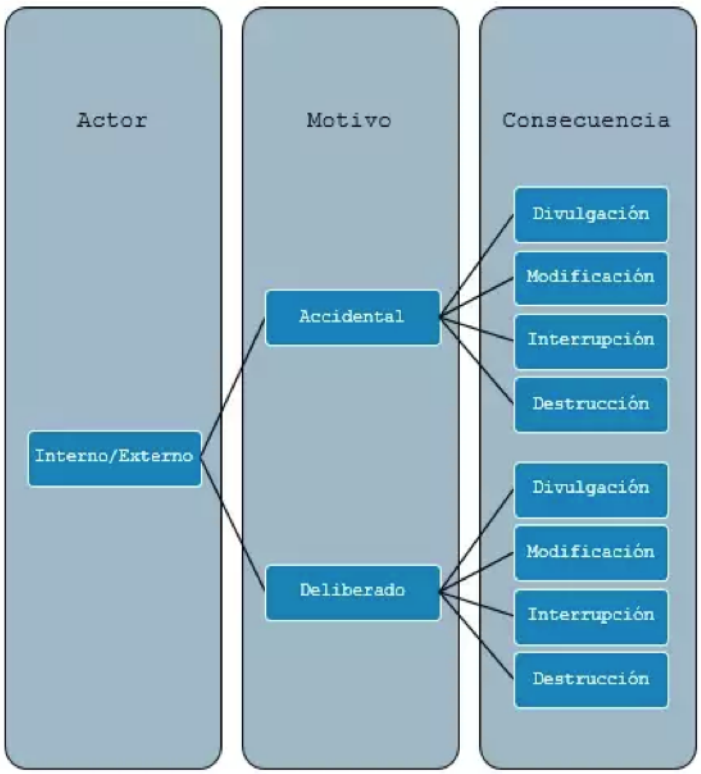

Figura 1. Árbol de posibles amenazas para un activo

Tomado de (Welivesecurity, 2016)

De igual forma, para definir la probabilidad de ocurrencia y su respectiva asignación de valor en la Escala de Valoración - presentada anteriormente en la tabla 1.2.3 - se calculará mediante la siguiente ecuación:

$$Riesgo = Amenaza\ (condición) + Impacto\ (consecuencia)$$ **(Ecuación 1)**

2.3.2 Valoración de Riesgos

Dado que los argumentos para la valoración de riesgos pueden ser subjetivos, la herramienta que se empleará, cuenta con una base de datos predefinida que proporciona una ayuda al momento de su estimación y despliega una matriz indicando los valores de probabilidad y degradación.

2.4 Plataforma de Equipos

Esta sección pretende abordar los conceptos generalizados de los aparatos que conjuga el data center, los mismos que serán progresivamente categorizados según sus características para la identificación de procesos y activos.

2.4.1 Switch

El switch en su terminología traducida es conmutador. Es un dispositivo utilizado en redes LAN (Local Area Network) por lo cual los instrumentos conectados estarán en una zona contigua al switch.

2.4.1.1 Características de un Switch

- Distribución de paquetes de datos, determinando su destino y enviándolos de forma eficaz.
- Interconectar las redes por medio de cables UTP, fibra óptica.
- Los equipos tienen varios puertos viniendo en configuraciones de 4, 8, 16, 32 y 52 puertos.
- Permiten crear redes virtuales, así como listas de acceso para definir características particulares a cada grupo formado.
- Cuentan con protocolos a implementarse que evitan, problemas de redundancia de paquetes.

Figura 2. Switch Cisco Nexus 3524x, 24 10G Ports

Tomado de (CDW Corporation, 2016)

2.4.2 SFPs (Small Form-Factor Pluggable)

El SFP es un dispositivo que efectúa funciones de transmisión y recepción de datos, además sirve de interfaz entre instrumentos de ruteo, conmutación de datos y un enlace de fibra óptica.

2.4.2.1 Características de un SFP

La principal característica es su base, ya que dependiendo de la distancia de conexión que puede ir desde los 2km hasta los 120km, se utilizarán fibras monomodo y multimodo.

Figura 3. DS-SFPFC8G-SW

Tomado de (Cisco Systems, 2016)

2.4.3 Cables UCS (Unified Computing System)

Son cables conectores de poder para sistemas unificados, elaborados siguiendo parámetros de calidad y especificaciones técnicas para su correcto desempeño.

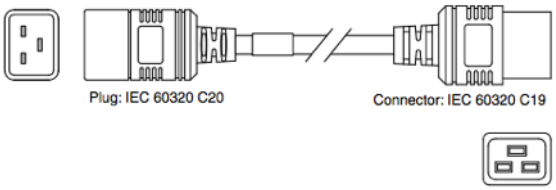

Figura 4. CAB-C19-CBN

Tomado de (Cisco Systems, 2016)

2.4.4 PDU (Power Distribution Units)

Unidades de distribución de energía, utilizadas en racks para mejorar la entrega de energía a los diferentes componentes del data center.

Tabla 2.

Características de la PDU

Descripción	RP208-30-1P-U-2
Voltaje de entrada	200 to 240 VAC ±10%
Frecuencia	50 to 60 Hz
Amperaje	30 A
Grado de la UL	24 A
Voltaje de salida	200 to 240 VAC
Temperatura de operación	10 a 50°C
Humedad relativa de operación	5 a 90% no condensada
Altura relativa de operación	0 a 3048m
Dimensión de la unidad (L x A x H)	1540 x 44 x 85 mm)

Tomado de (Cisco Systems, 2016)

2.4.5 Fibra Óptica

Se define como el mecanismo de transmisión de datos que emplea luz, configurado mediante frecuencias para así dar mejor uso a todo el espectro lumínico, esta luz utiliza ángulos de reflexión y cada cierta distancia necesita

repetidores de señal que lo que hace es tomar la señal, amplificarla y volverla a enviar.

2.4.5.1 Características de la Fibra Óptica

- En su mayoría las fibras ópticas están elaboradas a partir de arena o sílice.
- Sus componentes esenciales son el núcleo y el revestimiento, por el primero es donde viajará la luz que transmitirá los datos.
- Su funcionamiento esencialmente se basa en ser un camino para la luz radiada por los LEDs y los láseres.
- Se clasifican en dos tipos: fibras multimodo, utilizadas en distancias relativamente cortas que van desde 180 mts a 610 mts, y las fibras monomodo, requeridas en distancias largas, ya que el haz de luz viaja paralelamente a la fibra, se usa en distancias de hasta 400 km.

Figura 5. Cable de Fibra Óptica

Tomado de (ith network, 2016)

2.4.6 Rack

Es un armario donde se ubican los componentes electrónicos y de comunicaciones. Para evitar inconvenientes sus dimensiones fueron estandarizadas en base a la norma EIA 310-D; su principal funcionalidad es brindar en un área de trabajo, comodidad y funcionalidad a la misma.

2.4.6.1 Características del Rack

- Por normativa de instituciones especializadas sus tamaños son de 800, 1000, 1200, 1400, 1600, 1800, 2000 y 2200 mm.

- Se miden en unidades rack cuyas dimensiones son de 1,75 pulgadas equivalente a 44,45 mm de alto.

- El material del que están compuestos es metal, en la mayoría de los casos, siendo también utilizado el titanio, donde la corrosión puede ser un problema.

Figura 6. Rack AR3100

Tomado de (Anixter International, 2016)

2.4.7 Sistema de Enfriamiento

Bajo el enunciado de que el trabajo genera energía y calor, yace el argumento de tener un sistema de enfriamiento para los componentes electrónicos, el mismo debe adaptarse a los requerimientos de la infraestructura a montarse.

2.4.7.1 Consideraciones del Sistema de Enfriamiento

- El reparto de espacios es fundamental al momento de diseñar un data center, ya que se debe evitar a toda costa la mezcla de aire caliente con

aire frío, pues el consumo de energía aumentaría y la vida útil de los equipos disminuiría.

- El sobredimensionamiento es un error común al momento de emplear estos sistemas, debido a que se debe tener una proporción real del uso que se dará al data center.

- Un alto porcentaje de energía consume el sistema de enfriamiento por lo cual siempre se debe considerar que los equipos a usarse tengan consigo una certificación, y a su vez un buen mantenimiento.

Figura 7. Aire Acondicionado ASCS100

Tomado de (Anixter International, 2016)

2.4.8 Sistema de Energía

Tomando diferentes factores se podría concluir que este sistema es el más importante, ya que la energía proporcionada a los dispositivos electrónicos permite su funcionamiento. Además, se debe considerar la disponibilidad que deberán tener, pues si bien es cierto el data center de la facultad es de uso académico, no se debe dejar de considerar tener una redundancia al momento del funcionamiento del equipo.

2.4.8.1 Características del Sistema de Energía

- Usando las técnicas y tecnologías de la actualidad se puede ahorrar un 30% de energía, realizando periódicamente auditorías energéticas.

- El control del suministro de voltaje que deberá tener cada equipo es muy importante, por lo que medidores y reguladores de voltaje deben ser calibrados de forma correcta.

- Las baterías o almacenadores de energía de backup siempre deberán estar operativos ante cualquier contingencia.

- Los distribuidores de energía deben ser categorizados correctamente, y colocados en lugares apropiados, para ser eficientes y seguros.

Figura 8. Batería SYH6K6RMT-TF3

Tomado de (APC by Schneider Electric, 2016)

2.4.9 Sistema de Monitoreo

Una de las conjeturas más comunes al momento de definir preceptos es el hecho de conocer qué se está cuidando. En este caso cuál sería el activo más importante: si los equipos que administran, manejan y resguardan los datos, o a su vez la información almacenada; porque si la inversión es considerable se asume que la información vale tanto o más.

2.4.9.1 Cualidades del Sistema de Monitoreo

- Ofrecer un control sobre lo que acontece en el data center.

- Proporcionar una bitácora del acceso al data center, para así brindar mayor seguridad a la entidad.

- Al contar con un registro visual, se podrán determinar fallos con mayor precisión y agilidad.

- Permite una visión remota de lo acontecido, para así en caso de una emergencia se adopten procedimientos correctos.

Figura 9. Monitor NBWL0355

Tomado de (APC by Schneider Electric, 2016)

2.4.10 Sistema de Start Up

El sistema de arranque del data center provee el impulso y controla el orden en el cual los diferentes sistemas darán inicio, la suma de todas estas estructuras en sí componen el sistema de arranque. Es un componente sumamente importante, ya que una mala configuración supondrá el incremento de energía, hasta incluso el colapso de la estructura.

Figura 10. Sistema Star up WASSEM5X8-AX-14

Tomado de (APC by Schneider Electric, 2016)

2.5 Normas Aplicables

La definición de norma yace en el hecho de consensuar una regla particular y hacerla general para así definir y agrupar métodos de instalación, monitoreo y control en diferentes organizaciones. El presente trabajo conceptualiza y adapta las normas ISO al manejo en términos de seguridad del data center académico de la FICA.

2.5.1 Norma Española UNE-ISO/IEC 27001

Elaborada por el comité técnico AEN/CTN 71 y publicada en noviembre de 2007 por la UNE-ISO, el planteamiento de esta norma es “aportar con un modelo para la creación, implementación, operación, supervisión, revisión, mantenimiento y mejora de un Sistema de gestión de la Seguridad de la información (SGSI)” (UNE-ISO/IEC 27001, p.5).

De la totalidad que abarca la norma descrita lo más relevante para el contexto del presente trabajo es el manejo que se le da a la terminología activos, como ciertamente lo describe en el apartado de la integridad “La propiedad de salvaguardar la exactitud y completitud de los activos” (UNE-ISO/IEC 27001, p.8).

2.5.1.1 SGSI

Se conoce como el Sistema de Gestión de la Seguridad de la Información a las siglas SGSI, el cual tiene por objetivo proveer a la organización que desee su implementación -sin importar el tamaño de la misma- brindar las herramientas necesarias para que alcance el objetivo.

El modelo “Planificar-hacer-verificar-actuar” (PDCA), involucra el proceso para alcanzar una SGSI.

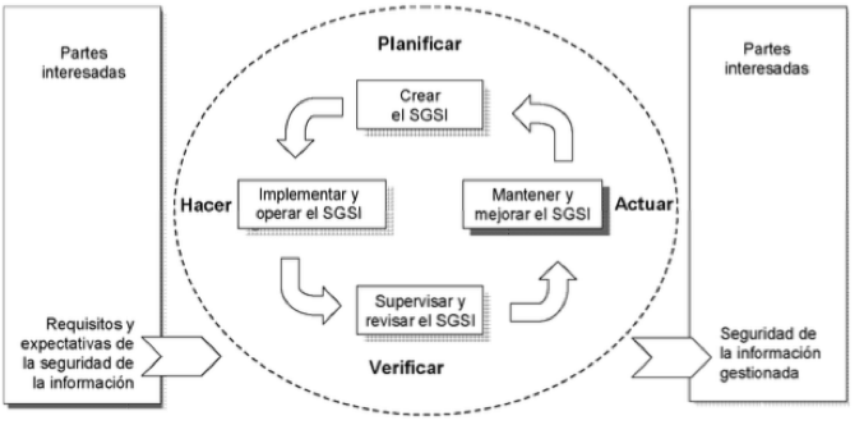

Figura 11. Modelo PDCA aplicado a los procesos del SGSI

Tomado de (UNE-ISO/IEC 27001, p.6)

2.5.1.2 Magerit

Son las siglas para la metodología de análisis y gestión de riesgos, fue elaborada por el Consejo Superior de Administración Electrónica. Su vinculación con las tecnologías de la información está conjuntamente ligada ya que las mismas requieren una gestión constante para cumplir sus objetivos.

2.5.1.2.1 Objetivos de Magerit

1. Concienciar a los responsables de las organizaciones de información de la existencia de riesgos y de la necesidad de gestionarlos

2. Ofrecer un método sistemático para analizar los riesgos derivados del uso de tecnologías de la información y comunicaciones (TIC)

3. Ayudar a descubrir y planificar el tratamiento oportuno para mantener los riesgos bajo control Indirectos

4. Preparar a la Organización para procesos de evaluación, auditoría, certificación o acreditación, según corresponda en cada caso (Portal Administración Electrónica PAE, 2012).

2.5.2 Norma Española UNE-ISO/IEC 27002

Desarrollada por el Comité Técnico conjunto ISO/IEC JTC 1, esta norma tiene como uno de sus objetivos el manejo de buenas prácticas para la gestión de la

seguridad de la información. Para esto, se maneja a la información como un activo más, por lo cual debe cumplir los enunciados que plantea la misma para su correcto manejo.

2.5.2.1 Políticas de Seguridad

La elaboración de políticas que vayan acorde a los temas involucrados, debe ser una premisa para la consensuada toma de decisiones de parte de la dirección dentro de una organización. Lo que buscan las políticas como lo define la norma es “La Dirección proporcionará indicaciones y dará apoyo a la seguridad de la información de acuerdo con los requisitos del negocio y con la legislación y las normativas aplicables” (UNE-ISO/IEC 27002, p.16).

2.6 Plataforma de Servicios

Los servicios son la base en la cual trabajarán los diferentes sistemas, por consiguiente, se deberán elegir apropiadamente según el enfoque que se vaya dando con el pasar de los semestres.

2.6.1 Windows Server 2008 R2

Es la denominación que tiene el sistema operativo de Windows diseñado para servidores, para permitir el control de máquinas u ordenadores, este servicio está enfocado hacia el cliente.

2.6.1.1 Características de Windows Server 2008 R2

- Brindar a los profesionales en TI un mejor manejo en la infraestructura de servidores tanto físico como en red, permitiéndoles así enfocarse en sectores críticos de la organización.

- Incrementar la seguridad informática en cada aspecto del negocio.

- Proporcionar confiabilidad al momento de dar mantenimiento e implementación de diferentes sistemas.

- Ayudar en la compatibilidad entre aplicaciones y servicios, además de ofrecer herramientas instintivas.

Figura 12. Logo Windows Server 2008

Tomado de (Windows Corporation, 2016)

3. CAPÍTULO III. IDENTIFICACIÓN DE ACTIVOS Y PROCESOS

3.1 Creación de un proyecto con PILAR Análisis y Gestión de Riesgos

La herramienta PILAR Análisis y Gestión de Riesgos en su versión 5.4.7 para el sistema operativo OS X El Capitán nos permite visualizar probables amenazas, calcula los riesgos e incluye la posibilidad de implementar medidas para reducir el riesgo a valores aceptables; basándose en la metodología Magerit y en la norma ISO/IEC 27002.

Para lo cual lograr lo descrito se necesita como requisitos lo siguiente:

- Actualización del entorno Java.
- Licencia educativa proporcionada por los creadores de la herramienta PILAR Análisis y Gestión de Riesgos.

PILAR Análisis y Gestión de Riesgos cuenta con tres versiones:

- EAR / PILAR
- EAR / PILAR Basic
- EAR / microPILAR

Estas herramientas incluyen diferentes características, pero todas ella orientadas hacia un mismo fin. Cabe destacar que para el desarrollo del

presente capítulo se utilizó la versión completa - EAR / PILAR - en el nivel medio de la misma.

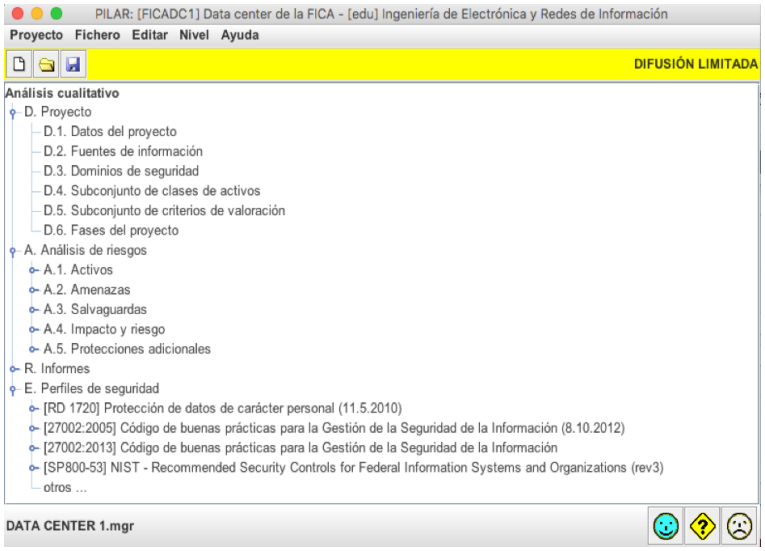

Figura 13. Panel Principal herramienta PILAR

3.2 Registro de datos del proyecto Data Center de la FICA

Una vez creado el proyecto se procederá a ingresar los datos provenientes del inventario realizado por la empresa ANDEANTRADE S.A, encargada de proveer los equipos y la instalación de los mismos; para lo cual la herramienta PILAR cuenta con diferentes categorías.

3.2.1 Datos del proyecto

En esta sección se ingresa la información concerniente a los datos más relevantes del proyecto, así como la asignación de un código - que debe ser único -, el nombre y la difusión que tendrá en este caso será limitada dada la magnitud del proyecto.

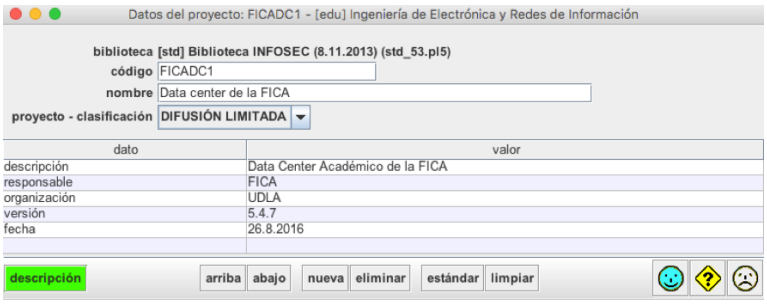

Figura 14. Panel Datos del proyecto herramienta PILAR

3.2.2 Fuentes de información

La presente sección es definida por el glosario de términos que incluye la herramienta PILAR como “El análisis de riesgos se alimenta con información procedente de alguna fuente: persona a cargo del activo, persona responsable del activo, inventario, repositorio de datos, ley, regulaciones, contratos,… PILAR permite establecer una colección de fuentes de información, de modo que más adelante se puede asignar la información a las fuentes, y posteriormente seleccionar información dependiendo de su origen.” (PILAR Análisis y Gestión de Riesgos, 2011).

De acuerdo a esta definición la fuente de información utilizada es el inventario realizado por la empresa ANDEANTRADE S.A. Este panel cuenta con tres campos de información que son: código, nombre y descripción.

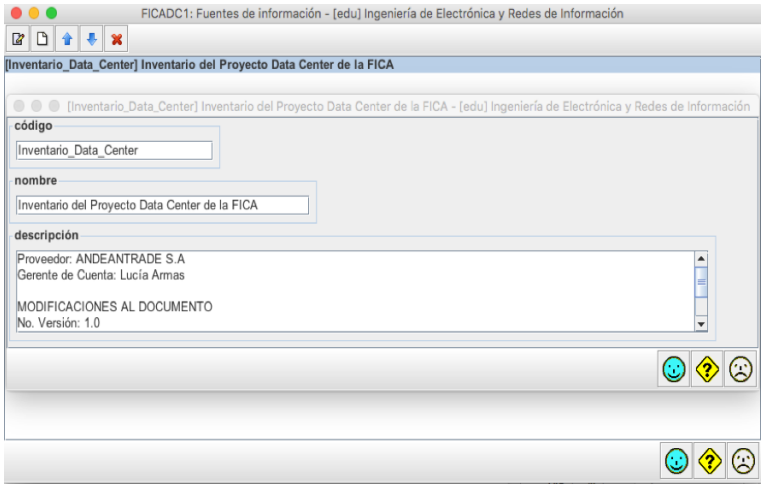

Figura 15. Panel Fuentes de información herramienta PILAR

3.2.3 Dominios de seguridad

Un dominio de seguridad -especificado por el glosario de términos- es “una colección de activos uniformemente protegidos, típicamente bajo una única autoridad. Los dominios de seguridad se utilizan para diferenciar entre zonas en el sistema de información” (PILAR Análisis y Gestión de Riesgos, 2011).

Se definieron dos dominios, uno principal y otro dentro de este. El primero es la red universitaria o la red base, y el segundo es la conexión a internet con la que cuenta el campus Queri.

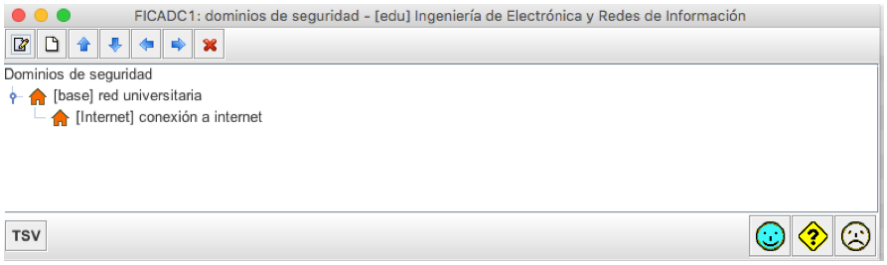

Figura 16. Panel Dominios de seguridad herramienta PILAR

3.2.3 Fases del proyecto

Las fases del presente proyecto se realizarán con base en los capítulos que presenta el trabajo de titulación. Estas etapas tienen la finalidad de proporcionar un nivel de madurez que evidencie el progreso de aplicación de las salvaguardias, además de proyecciones de hipotéticas fallas.

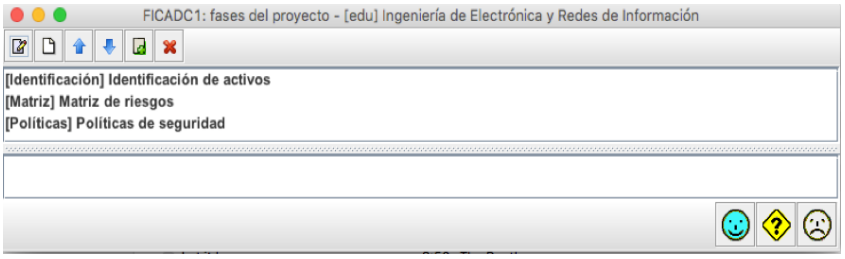

Figura 17. Panel Fases del proyecto herramienta PILAR

3.3 Identificación de activos del Data Center de la FICA

La herramienta PILAR presenta ya capas definidas que pueden ser modificadas o eliminadas, las mismas a su vez se categorizan dependiendo del activo.

Como se menciona anteriormente, el listado de equipos fue tomado del inventario provisto por la empresa ANDEANTRADE S.A. Los equipos fueron clasificados y categorizados en diferentes tipos de activos como indica la figura, además se presentarán las características más relevantes de los mismos.

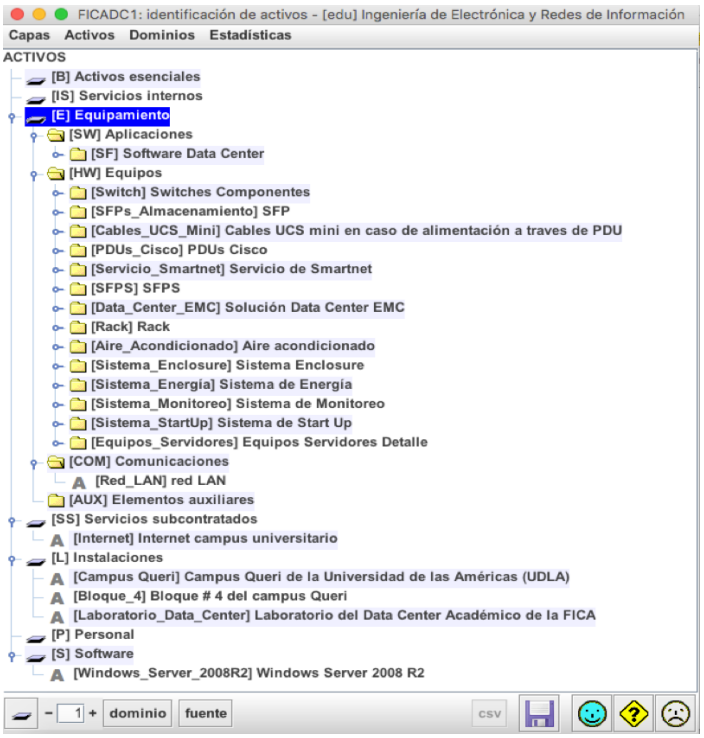

Figura 18. Panel Identificación de activos herramienta PILAR

3.3.1 Equipamiento

3.3.1.1 Software Data Center

La presente sección cuenta con el código [SF] para su identificación y con cinco activos que integran la sección del software base del data center como se presenta en la siguiente figura, cabe mencionar que la sección entre corchetes es el código único del activo y su definición.

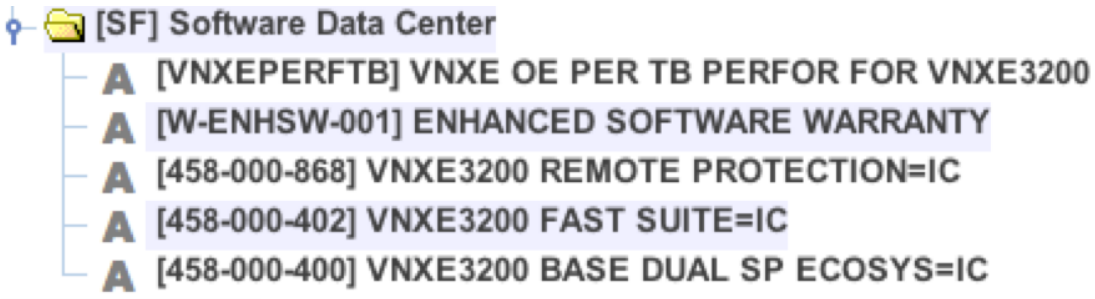

Figura 19. Software Data Center

3.3.1.1.1 Características de [VNXEPERFTB] VNXE OE PER TB PERFOR FOR VNXE300

Tabla 3.

Características de VNXEPERFTB

Cantidad	7
Tipos de almacenamiento	• Microsoft Exchange • Carpetas Compartidas • iSCSI Genéricos • VMware • Hyper-V
Host	Windows Server 2008 R2
Objetivos gestionados	Hyper-V datastores
Servidor de almacenamiento	iSCSI server

Tomado de (EMC Corporation, 2012)

3.3.1.2 Switches y Componentes

Las características de los equipos de conmutación se presentan en la siguiente sección, cabe mencionar que el área cuenta con el código [Switch] para su identificación y con diez activos presentados en la siguiente figura:

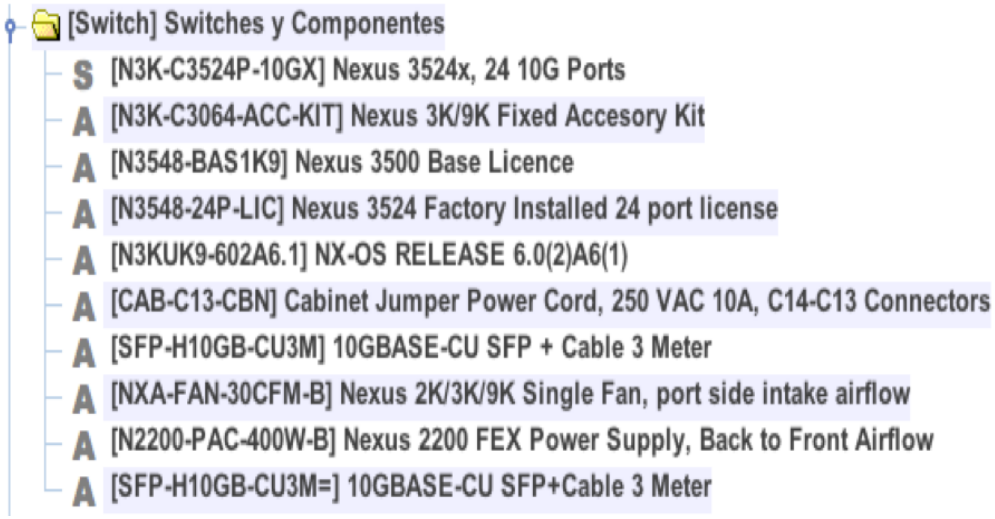

Figura 20. Switches y Componentes

3.3.1.2.1 Características de [N3K-C3524P-A0GX] Nexus 3524x, 24 10G Ports

Tabla 4.

Características de N3K-C3524P-A0GX

Cantidad	2
Tipo de hardware	Switch Cisco Nexus 3524x
Tipos de conectores	• RJ-45 • Serial (consola) • SFP+ • Type A USB
Frecuencia	50/60 Hz
Voltaje nominal	AC 120/130 V
Capacidad de switching	960 Gb/s
Velocidad de switching	10 Gb Ethernet

Tomado de (CDW, 2016)

3.3.1.2.2 Características de [N3K-C3064-ACC-KIT] Nexus 3K/9K Fixed Accessory Kit

Tabla 5.

Características de N3K-C3064-ACC-KIT

Cantidad	2
Tipo de hardware	Accesorios de arreglo para Nexus 3K/9K
Contenido	• 2 soportes de montaje de frente en ángulo deslizables • 2 soportes de corredora trasera de montaje • 2 rieles deslizantes • 16 tornillos de montaje • Cable de consola • 1 lengüeta con dos orificios • 2 tornillos de cabeza Phillips • 1 documento de cumplimiento de la CAO • 1 DCNM DVD

Tomado de (Provantage, 2016)

3.3.1.2.3 Características de [CAB-C13-CBN] Cabinet Jumper Power Cord, 250 VAC 10A, C14-C13 Connectors

Tabla 6.

Características de CAB-C13-CBN

Cantidad	4
Tipo de hardware	Cable Jumper
Amperaje	10 A
Voltaje	250 VAC
Tipo de plug	SS10A
Tipo de conector	HS10S
Longitud del cable	0.68 m

Tomado de (Cisco, s.f)

3.3.1.2.4 Características de [SFP-H10GB-CU3M] 10GBASE-CU SFP + Cable 3 Meter

Tabla 7.

Características de SFP-H10GB-CU3M

Cantidad	4
Tipo de hardware	• SFP • Cable
Velocidad de datos Ethernet	10 Gb/s
Velocidad de datos fibra óptica	8 Gb/s
Longitud del cable	3 m

Tomado de (10Gtek, 2015)

3.3.1.2.5 Características de [N2200-PAC-400W-B] Nexus 2200 FEX Power Supply, Back to Front Airflow

Tabla 8.

Características de N2200-PAC-400W-B

Cantidad	4
Tipo de hardware	Fuente de alimentación
Potencia	400 W

3.3.1.3 SFP

La siguiente sección cuenta con el código [SFPs_Almacenamiento] para su identificación y con un activo presentado en la siguiente figura:

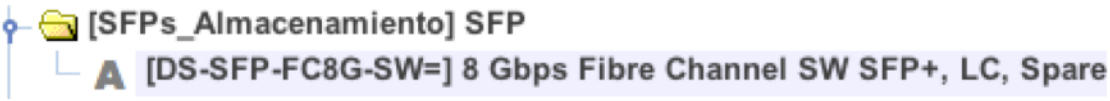

Figura 21. SFP

3.3.1.3.1 Características de [DS-SFP-FC8G-SW=] 8 Gbps Fibre Channel SW SFP+, LC, Spare

Tabla 9.

Características de DS-SFP-FC8G-SW=

Cantidad	4
Tipo de hardware	Módulo de transceptor SFP+-LC de modos múltiples
Velocidad de transferencia de datos	8.5 Gb/s
Longitud de onda óptica	850 nm
Protocolo de interconexión de datos	Canal de fibra de 8 Gb (onda corta)
Distancia máxima de transferencia	520 m

Tomado de (MISCO, s.f)

3.3.1.4 Cables UCS mini en caso de alimentación a través de PDU

La presente sección posee el código [Cables_UCS_Mini] para su identificación y con un activo presentado en la siguiente figura:

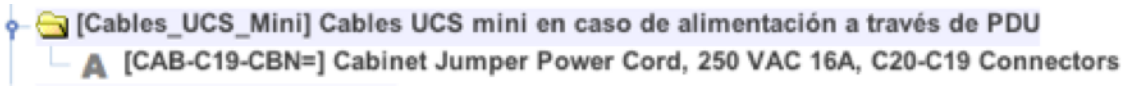

Figura 22. Cables UCS mini en caso de alimentación a través de PDU

3.3.1.4.1 Características de [CAB-C19-CBN=] Cabinet Jumper Power Cord, 250 VAC 16A, C20-C19 Connectors

Tabla 10.

Características de CAB-C19-CBN=

Cantidad	4
Tipo de hardware	Cabinet Jumper
Amperaje	16 A
Voltaje	250 VAC
Dimensiones	9.2 x 3.9 x 2.7 pulg.

Tomado de (Cisco, s.f)

3.3.1.5 PDUs Cisco

La sección PDU posee el código [PDUs_Cisco] para su registro y con dos activos presentados en la siguiente figura:

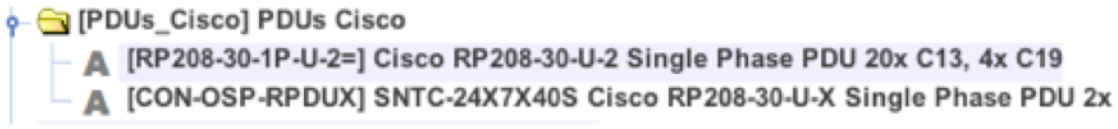

Figura 23. PDUs Cisco

3.3.1.5.1 Características de [RP208-30-1P-U-2=] Cisco RP208-30-U-2 Single Phase PDU 20x C13, 4x C19

Tabla 11.

Características de RP208-30-1P-U-2=

Cantidad	2
Tipo de hardware	UCS
Tipos de receptáculos	• C13 • C19
Cantidad C13	20
Cantidad C19	4

Tomado de (Cisco, 2013)

3.3.1.5.2 Características de [CON-OSP-RPDUX] SNTC-24X7X40S Cisco RP208-30-U-X Single Phase PDU 2x

Tabla 12.

Características de CON-OSP-RPDUX

Cantidad	2
Tipo de hardware	PDU
Voltaje de entrada	200 a 240 VAC
Frecuencia	50 a 60 Hz
Amperaje	30 A

Tomado de (Cisco, 2015)

3.3.1.6 Servicio de Smartnet

Esta sección del Servicio Smartnet cuenta con el código [Servicio_Smartnet] para su identificación y con un activo presentado en la siguiente figura:

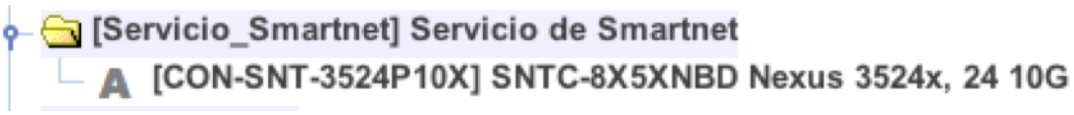

Figura 24. Servicio de Smartnet

3.3.1.6.1 Características de [CON-SNT-3524P10X] SNTC-8X5XNBD Nexus 3524x, 24 10G

Tabla 13.

Característica de CON-SNT-3524P10X

Cantidad	2
Tipo de software	Garantía de los equipos

Tomado de (myriad, s.f)

3.3.1.7 SFPS

La presente sección cuenta con el código [SFPS] para su identificación y con un activo presentado en la siguiente figura:

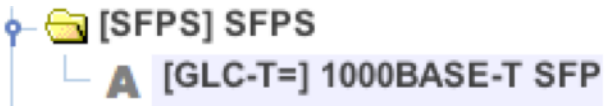

Figura 25. SFPS

3.3.1.7.1 Características de [GLC-T=] 1000BASE-T SFP

Tabla 14.

Características de GLC-T=

Cantidad	4
Tipo de hardware	Transceptor
Categoría	5 para cable de cobre
Tipo de conector a usar	RJ-45

Tomado de (Cisco, 2016)

3.3.1.8 Solución Data Center EMC

El detalle de las propiedades con las que cuentan los equipos de la siguiente sección son presentados en la figura, cabe mencionar que el código [Data_Center_EMC] sirve para su identificación y poseen seis activos.

Figura 26. Solución Data Center EMC

3.3.1.8.1 Características de [V32-PWR-12] 2 C13 PWRCRD W / NEMA 5-15 PLUGS 125V 10A

Tabla 15.

Características de V32-PWR-12

Cantidad	2
Tipo de hardware	Conectores de alimentación
Clasificación	5-15
Voltaje	125 V
Amperaje	10 A

Tomado de (Fundación Wikipedia, 2016)

3.3.1.8.2 Características de [V32D12AN5PS6] VNXE3200; 2XSP DPE; 25X2.5 DS; 6X300GB 15K

Tabla 16.

Características de V32D12AN5PS6

Cantidad	1
Tipo de hardware	Matriz CORE
Cache	300 Gb
Interfaz	6 Gb/s
Capacidad Formateable	268.37 Gb
Data Buffer	16 Mb

Tomado de (EMC Corporation, 2015)

2.3.1.9 Rack

La sección a continuación cuenta con el código [Rack] para su identificación y con un activo presentado en la siguiente figura:

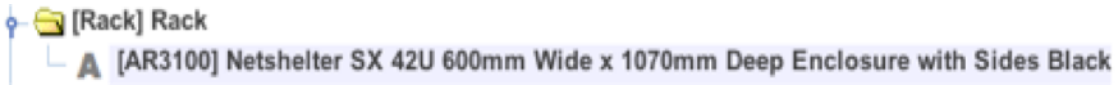

Figura 27. Rack

3.3.1.9.1 Características de [AR3100] NetShelter SX 42U 600mm Wide x 1070mm Deep Enclosure with Sides Black

Tabla 17.

Características de AR3100

Cantidad	1
Tipo de hardware	Rack
Altura	42 U
Capacidad de peso estática	3006.2 lb
Profundidad de montaje	191.0 a 915.0 mm
Capacidad de peso dinámica	2254.6 lb

Tomado de (B&H, 2016)

3.3.1.10 Aire Acondicionado

La presente sección cuenta con el código [Aire_Acondicionado] para su identificación y con un activo presentado en la siguiente figura:

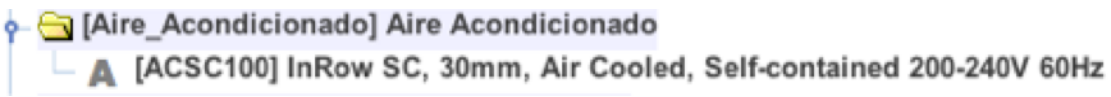

Figura 28. Aire Acondicionado

3.3.1.10.1 Características de [ACSC100] InRow SC, 300mm, Air Cooled, Self-contained 200-240V 60Hz

Tabla 18.

Características de ACSC100

Cantidad	1
Tipo de hardware	Aire Acondicionado
Capacidad nominal de enfriamiento	5.25 kW
Humedad relativa del aire entrante	34 %
Temperatura de aire de entrada	29.44 ºC
Circulación de aire	566.34 l/s

Tomado de (ATN, 2013)

3.3.1.11 Sistema Enclosure

La presente sección se maneja con el código [Sistema_Enclosure] para su identificación y con cinco activos presentados en la siguiente figura:

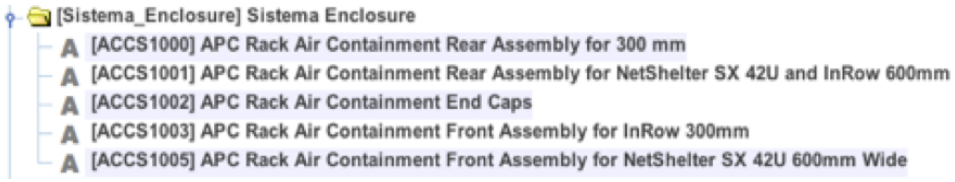

Figura 29. Sistema Enclosure

3.3.1.11.1 Características de [ACCS1000] APC Rack Air Containment Rear Assembly for InRow 300 mm

Tabla 19.

Características de ACCS1000

Cantidad	1
Tipo de hardware	APC Rack
Altura máxima	199.1 cm
Ancho máximo	30.0 cm
Profundidad máxima	19.6 cm
Peso	11.91 kg

Tomado de (APC, 2016)

3.3.1.12 Sistema de Energía

La siguiente sección cuenta con el código [Sistema_Energía] para su identificación y con dos activos presentados en la siguiente figura:

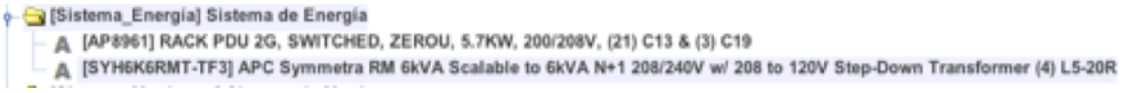

Figura 30. Sistema de Energía

3.3.1.12.1 Características de [AP8961] Rack PDU 2G, SWITCHED, ZEROU, 5.7KW, 200/208V, (21) C13 & (3) C19

Tabla 20.

Características de AP8961

Cantidad	1
Tipo de hardware	PDU Rack
Entrada	5.7 kW
Conexiones de entrada	NEMA L21-20P
Conexiones de salida	• (21) C13 • (3) C19
Largo del cable	1.83 m

Tomado de (SRO, 2016)

3.3.1.12.2 Características de [SYH6K6RMT-TF3] APC Symmetra RM 6kVA Scalable to 6kVA N+1 208/240V w/ 208 to 120V Step-Down Transformer (4) L5-20R

Tabla 21.

Características de SYH6K6RMT-TF3

Cantidad	1
Tipo de hardware	APC Symmetra
Capacidad de potencia de salida	4.2 / 6.0 kW
Voltaje de entrada	120 / 208 V
Voltaje de salida	208 V
Eficiencia a plena carga	85 %
Frecuencia	60 Hz

Tomado de (APC, 2016)

3.3.1.13 Sistema de Monitoreo

Esta sección posee el código [Sistema_Monitoreo] para su identificación y con un activo presentado en la siguiente figura:

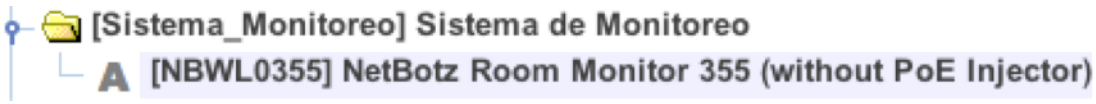

Figura 31. Sistema de Monitoreo

3.3.1.13.1 Características de [NBWL0355] NetBotz Room Monitor 355 (without PoE Injector)

Tabla 22.

Características de NBWL0355

Cantidad	1
Tipo de hardware	Cámara de monitoreo
Alerta de indicadores	• Energía • Cámara • Enlace de red • Indicador de temperatura
Cámara integrada	• 1280x1024 de resolución • 24 bits de color • 30 fotografías por segundo
Sensores	• Temperatura • Temperatura / humedad • Movimiento • Punto de rocío
Conectores	• 1 puerto Ethernet 10/100 Base-T • 1 USB de configuración • 4 puertos de sensor universal APC

Tomado de (APC Guard, 2015)

3.3.1.14 Sistema de StartUp

La siguiente sección cuenta con el código [Sistema_StartUp] para su identificación y con dos activos presentados en la siguiente figura:

Figura 32. Sistema de StartUp

3.3.1.14.1 Características de [WASSEM5X8-AX-14] Scheduled Assembly and Start-Up Service for InRow SC Air Cooled Self Contained

Tabla 23.

Característica de WASSEM5X8-AX-14

Cantidad	1
Tipo	Servicio para el sistema de arranque

3.3.1.15 Equipos Servidores Detalle

La siguiente sección presenta la mayoría de activos un total de treinta y uno, su identificación se muestra con el código [Equipos_Servidores] como se detalla en la figura:

Figura 33. Equipos Servidores Detalle

3.3.1.15.1 Características de [UCS-SPL-MINI] UCS SP Select 5106 AC2 Chassis w/FI6324, UCS Central license

Tabla 24.

Característica de UCS-SPL-MINI

Cantidad	1
Tipo	Licencia central

3.3.1.15.2 Características de [ND1-UAC1] Single phase AC power module for UCS 5108

Tabla 25.

Característica de ND1-UAC1

Cantidad	1
Tipo de hardware	Módulo de alimentación monofásica
Voltaje de entrada	100 / 120 V
Potencia de salida	1300 W
Frecuencia	50 a 60 Hz
Eficiencia	94 %

Tomado de (Cisco, 2016)

3.3.1.15.3 Características de [N20-CAK] Accessory kit for UCS 5108 Blade Server Chassis

Tabla 26.

Característica de N20-CAK

Cantidad	1
Tipo de hardware	Kit de accesorios para UCS 5108
Contenido	• Juego de rieles • KVM cable conector de la consola de dongle • 8 ventiladores

Tomado de (ZONES, 2016)

3.3.1.15.4 Características de [N20-FAN5] Fan module for UCS 5108

Tabla 27.

Características de N20-FAN5

Cantidad	8
Tipo de hardware	Módulo de ventilación para UCS 5108
Número de cuchillas	8
I/O slots	2
Voltaje de entrada	100 a 120 VAC
Fuente de alimentación	48 VAC

Tomado de (TABAKALERA, s.f)

3.3.1.15.5 Características de [N20-FWD13] UCS Blade Server Chassis FW Package 3.0

Tabla 28.

Características de N20-FWD13

Cantidad	1
Tipo de hardware	UCS chasis
Altura	26.7 cm o 6 RU (rack unit)
Ancho	44.5 cm
Profundidad	81.2 cm
I/O slots	2

Tomado de (Cisco, 2016)

3.3.1.15.6 Características de [UCSB-5108-PKG-HW] UCS 5108 Packaging for chassis with width blades

Tabla 29.

Características de UCSB-5108-PKG-HW

Cantidad	1
Tipo de hardware	UCS Blade Max Memory
Número de procesadores	4
Tipo de procesador	Intel Xeon
Frecuencia	3.3 Ghz

Tomado de (Alibaba, 2016)

3.3.1.15.7 Características de [UCSB-PSU-2500ACDV] 2500W Platinum AC Hot Plug Power Supply - DV

Tabla 30.

Características de UCSB-PSU-2500ACDV

Cantidad	4
Tipo de hardware	Fuente de alimentación - conectable en caliente - interna
Capacidad energética	2500 W
Diseñado para	UCS 5108 Blade Server Chassis SmartPlay 8 Expansion Pack

Tomado de (MISCO, 2016)

3.3.1.15.8 Características de [UCS-FI-M-6324] UCS 6324 In-Chassis FI with 4 UP, 1x40G Exp Port, 16 10GB do

Tabla 31.

Características de UCS-FI-M-6324

Cantidad	2
Tipo de hardware	UCS
Tipo de arquitectura	De corte a través y soporte de baja latencia
Velocidad	10 Gb Ethernet
Ancho de banda	80 Gbps
Número de puertos	5

Tomado de (NetworkOutlet, 2016)

3.3.1.15.9 Características de [CON-SNTE-FIM6324] SMARTNET 8X5X4 UCS 6324 In-Chs FI w/4 UP 1x40G E-Port

Tabla 32.

Características de CON-SNTE-FIM6324

Cantidad	2
Tipo de hardware	UCS
Diseñado para	I/O modulo para Cisco UCS 5108
Puertos de servidor	16 x 10GBASE-KR lanes
Rendimiento	500 Gbps
Estado de latencia	Menos de un microsegundo
Calidad de servicio (QoS) colas de hardware	16 (8 cada uno para unicast y multicast)

Tomado de (Cisco, 2016)

3.3.1.15.10 Características de [CAB-L520P-C19-US] NEMA L5-20 TO IEC-C19 6FT US

Tabla 33.

Características de CAB-L520P-C19-US

Cantidad	4
Tipo de hardware	Cisco Cable NEMA L5-20 para IEC-C19
Voltaje	125 VAC
Longitud del cable	1.83 m
Frecuencia	60 Hz
Compatibilidad	Cisco Nexus 7000 Switch Series

Tomado de (PROVENTAGE, 2016)

3.3.1.15.11 Características de [UCS-SPL-B20DM4-B1] UCS SP Select B200M4 Basic1 2/2xE52609 v3, 4x16GB, VIC1340

Tabla 34.

Características de UCS-SPL-B20DM4-B1

Cantidad	3
Tipo de hardware	Sistema convergente para servidores blade y en rack
Memoria	768 Gb
Rendimiento	80 Gb/s
Tipo de módulos	DIMM

Tomado de (Atomic North, 2015)

3.3.1.15.12 Características de [CON-SNTE-SPLB24B1] UCS B200 M4 Smart Play SPL Server, SMARTNET 8X5X4

Tabla 35.

Características de CON-SNTE-SPLB24B1

Cantidad	3
Tipo de hardware	UCS B200
Chipset	Intel C610
Tipo de memoria	24 DIMM slots
Controlador de almacenamiento	• SAS/SATA support • RAID 0 and 1 and JBOD

Tomado de (Cisco, 2016)

3.3.1.15.13 Características de [UCSB-HS-EP-M4-R] CPU Heat Sink for UCS B200 M4/B420 M4 (Rear)

Tabla 36.

Características de UCSB-HS-EP-M4-R

Cantidad	3
Tipo de hardware	Disipador de calor para UCS B200
Diseñado para	Cisco UCS B200
Peso	816 g
Dimensiones	31.8 x 23.5 x 10.2 cm
Ubicación	Posterior

Tomado de (Amazon, 2016)

3.3.1.15.14 Características de [C1-N1K-ESSTL] Nexus 1000V Essential Edition, Qty=2

Tabla 37.

Características de C1-N1K-ESSTL

Cantidad	3
Tipo de hardware	Cisco Nexus 1000V Switch para VMware
Bloques de seguridad	• ACL • AAA • DHCP/ DAI/ IPSG • PVLAN • Port-Sec
Operaciones de red	• SPAN / ERSPAN • Netflow • vTracker • SNMP • Syslog
Red de capacidad de extensión mediante	• VXLAN • SXP • Mac-Distribución

Tomado de (Cisco, 2016)

3.3.1.15.15 Características de [UCS-CPU-E5260D] 1.90 Ghz E5-2609 v3/85W 6C/15MB Cache/DDR4 1600MH

Tabla 38.

Características de UCS-CPU-E5260D

Cantidad	6
Tipo de hardware	Procesador
Tipo de procesador	Intel Xeon E5-2609V3
Número de núcleos	6
Cache	15 Mb
Diseñado para	• UCS C220 M4 • Smart Play 8 C220

Tomado de (MISCO, 2016)

3.3.1.15.16 Características de [UCS-MR-1X162RU-A] 16GB DDR4-2133-MHz RDIMM/PC4-1700D/dual rank/x4/1.2v

Tabla 39.

Características de UCS-MR-1X162RU-A

Cantidad	12
Tipo de hardware	Memoria
Velocidad	2133 Mhz
Tipo de RAM	Dual Rank
Capacidad de almacenamiento	16 Gb
Voltaje de alimentación	1.2 V

Tomado de (CDW, 2016)

3.3.1.15.17 Características de [UCSB-MLOM-4DG-D3] Cisco UCS VIC 1340 modular LOM for blade servers

Tabla 40.

Características de UCSB-MLOM-4DG-D3

Cantidad	3
Tipo de hardware	Cisco UCS VIC 1340
Número de puertos	2
Velocidad	40 Gb Ethernet
Diseñado para	• Cisco B200 M3 • Cisco B200 M4

Tomado de (Amazon, 2016)

3.3.1.16 Comunicaciones

La siguiente sección presenta la red de tipo LAN que presenta el campus posee el código [COM] para su identificación y con un activo presentado en la siguiente figura:

Figura 34. Comunicaciones

3.3.1.16.1 Características de [Red_LAN] Red LAN Campus Queri

Tabla 41.

Características de Red_LAN

Cantidad	1
Tipo	Red LAN
Tipo de cable	UTP
Tipo de conexiones	• Red Wireless • Red de cableado estructurado
Categoría cableado estructurado	6a
Tipos de Vlan	• Administradores • Profesores • Administrativos • Estudiantes • Usuarios • Soporte técnico

3.3.1.17 Servicios Subcontratados

La siguiente sección cuenta con el código [SS] para su identificación y con un activo presentado en la siguiente figura:

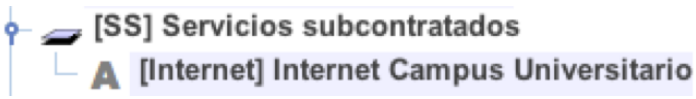

Figura 35. Servicios Subcontratados

3.3.1.17.1 Características de [Internet] Internet Campus Universitario

Tabla 42.

Características de Internet

Cantidad	1
Tipo	Internet
Ancho de banda	200 mbps

3.3.1.18 Instalaciones

Las instalaciones comprenden en forma ordenada el sitio donde se encuentra el data center, cuenta con el código [L] para su identificación y con tres activos presentados en la siguiente figura. Cabe mencionar que por motivos de seguridad no se presentan características explícitas de su ubicación y acceso:

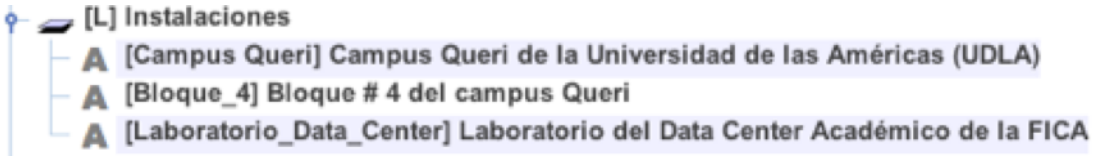

Figura 36. Instalaciones

3.3.1.19 Software

La sección final cuenta con el código [S] para su identificación y con un activo, que es el sistema operativo inicial con el cual contará el data center, presentado en la siguiente figura:

Figura 37. Software

3.3.1.19.1 Características de [Windows_Server_2008] Windows Server 2008 Data center edition

Tabla 43.

Características de Windows_Server_2008

Cantidad	1
Memoria RAM en 32 bits	64 Gb
Memoria RAM en 64 bits	2 Tb
Número mínimo de CPU	8
Número máximo de CPU	64

Tomado de (Baby Valdéz, 2016)

4. CAPÍTULO IV. MATRIZ DE RIESGOS

4.1 Asignación de Dependencias entre los activos del proyecto

Para definir el proceso de análisis de los peligros que serán presentados en matrices, se debe clasificar y asociar ciertos activos como principales (padres) y otros como secundarios (hijos), para lo cual la herramienta PILAR Análisis y Gestión de Riesgos, ofrece la posibilidad de hacerlo definiéndolo en base a criterios del usuario.

4.1.1 Árboles y buses de presentación de activos principales y secundarios

La herramienta PILAR brinda al usuario varias opciones de visualización de los avances que se van desarrollando en el proyecto, uno de estos es la presentación mediante árboles y buses de los activos principales (padres) y los secundarios (hijos), los mismos que serán distinguidos mediante los códigos asignados previamente.

4.1.1.1 Árbol de activos del Software Data Center

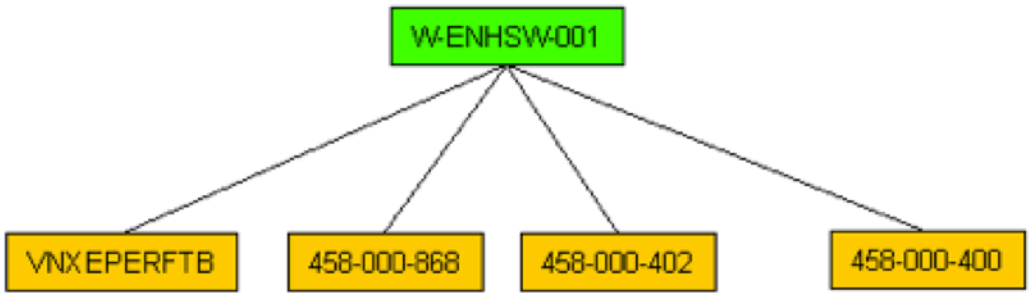

Figura 38. Árbol de activos Software Data Center

4.1.1.2 Árbol de activos del Switch y Componentes

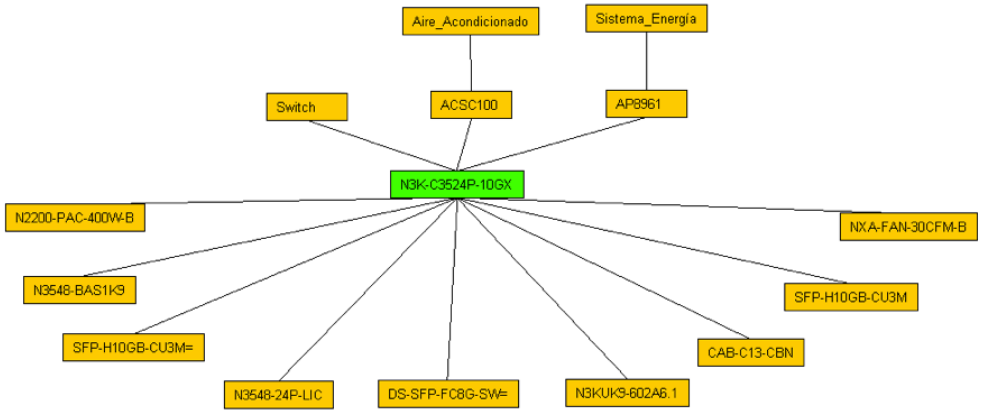

Figura 39. Árbol de activos Switch y Componentes

4.1.1.3 Bus de activos de Solución Data Center EMC

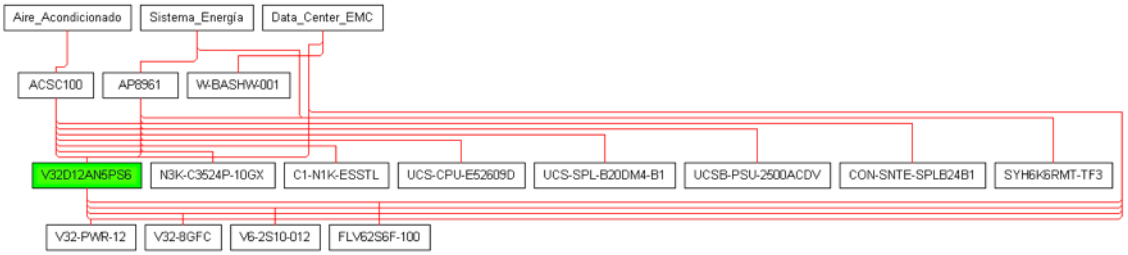

Figura 40. Bus de activos Solución Data Center EMC

4.1.1.4 Bus de activos del Aire Acondicionado

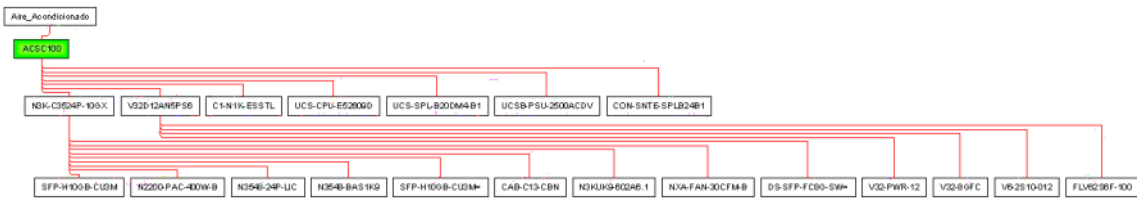

Figura 41. Bus de activos Aire Acondicionado

4.1.2 Valoración de los activos

Bajo los conceptos de disponibilidad, confidencialidad, autenticidad, integridad, y trazabilidad, cualidades que presenta un activo se otorgaron diferentes valoraciones en base a la fórmula del cálculo del riesgo para la totalidad de los activos.

Tabla 44.

Niveles de valoración

Nivel	Semántica
10	El valor más alto, el daño más alto
7	El valor más grande / el daño más grave que suele darse en servicios del sector privado o de la administración pública
5	Cuando las consecuencias afectan a otras organizaciones externas
3	Consecuencias limitadas, de carácter interno
0	Insignificante - puede ser obviado a todos los efectos prácticos

Tomado de (PILAR Análisis y Gestión de Riesgos, 2011)

[HW] Equipos					
[Switch] Switches y Componentes					
[N3K-C3524P-10GX] Nexus 3524x, 24 10G Ports	[9]	[1]	[3]	[2]	[2]
[N3K-C3064-ACC-KIT] Nexus 3K/9K Fixed Accesory Kit	[2]	[1]	[n.a.]	[2]	[5]
[N3548-BAS1K9] Nexus 3500 Base Licence	[1]	[0]	[n.a.]	[2]	[1]
[N3548-24P-LIC] Nexus 3524 Factory Installed 24 port license	[1]	[0]	[n.a.]	[2]	[1]
[N3KUK9-602A6.1] NX-OS RELEASE 6.0(2)A6(1)	[1]	[0]	[n.a.]	[2]	[1]
[CAB-C13-CBN] Cabinet Jumper Power Cord, 250 VAC 10A, C14-C13 Connectors	[8]	[2]	[n.a.]	[2]	[2]
[SFP-H10GB-CU3M] 10GBASE-CU SFP + Cable 3 Meter	[7]	[1]	[n.a.]	[2]	[2]
[NXA-FAN-30CFM-B] Nexus 2K/3K/9K Single Fan, port side intake airflow	[3]	[1]	[n.a.]	[2]	[2]
[N2200-PAC-400W-B] Nexus 2200 FEX Power Supply, Back to Front Airflow	[6]	[1]	[n.a.]	[2]	[2]
[SFP-H10GB-CU3M=] 10GBASE-CU SFP+Cable 3 Meter	[6]	[1]	[n.a.]	[2]	[2]

Figura 42. Niveles de valoración Switches y Componentes

4.1.3 Identificación de Amenazas

Para presentar las amenazas que pueden repercutir en las Instalaciones en las cuales se encuentra el Data Center, la herramienta PILAR cuenta con su propia biblioteca de amenazas, la misma que tiene de base la norma UNE-ISO/IEC 27002. Esta norma emplea la dependencia y clasificación de activos, provee información de los peligros a los cuales se expone cada activo, en este caso a las dependencias del campus.

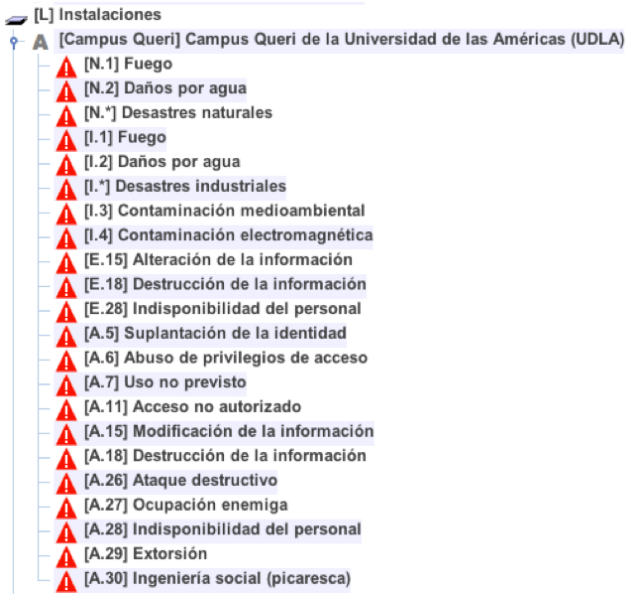

Figura 43. Listado de amenazas al Campus Queri y sus dependencias

4.1.4 Riesgo Acumulado

El riesgo como lo define la norma UNE-ISO/IEC 27002 es la “Combinación de la probabilidad de un suceso y de su consecuencia” (Comité técnico AEN/CTN 71 Tecnología de la información, 2009) por lo cual el riesgo acumulado se puede definir como la probabilidad de que el evento que afectó el activo ocurra una y varias veces, si este no es protegido.

Una vez realizado el procedimiento que requiere la herramienta PILAR, se determinó que el mayor impacto al funcionamiento del proceso se ve reflejado en la Red LAN del Campus Queri, como indica el siguiente gráfico:

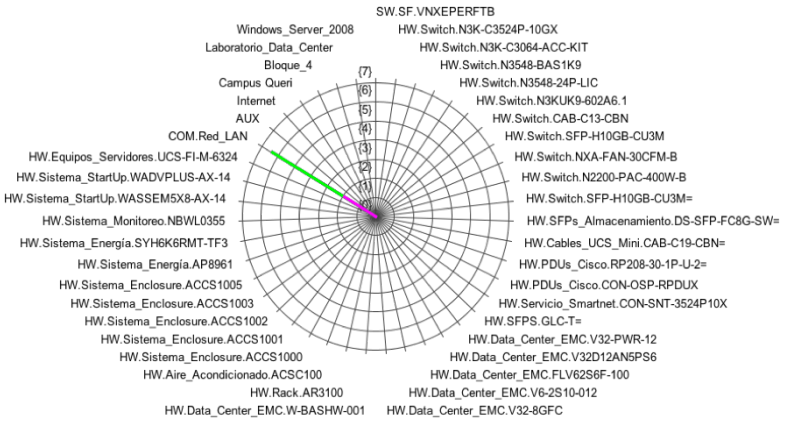

Figura 44. Riesgo acumulado / activo

Continuando con el análisis se determinó en base a las cinco dimensiones de un activo que el mayor peligro de la red LAN yace en la Confidencialidad y su riesgo es la Revelación de la información.

activo	[D]	[I]	[C]	[A]	[T]
ACTIVOS			{6,4}		
[B] Activos esenciales					
[IS] Servicios internos					
[E] Equipamiento			{6,4}		
[COM] Comunicaciones			{6,4}		
[Red_LAN] Red LAN Campus Queri			{6,4}		
[A.19] Revelación de información			{6,4}		
[SS] Servicios subcontratados					
[L] Instalaciones					
[P] Personal					
[S] Software					

Figura 45. Identificación de Riesgo acumulado / activo

4.1.5 Matriz de Riesgos

En base a la valoración de activos y en conjunto con las incidencias de amenazas, se calcularon valores únicos y acumulados de los activos más representativos para el data center, los cuales se presentarán en matrices. Para el efecto se adjunta la tabla detallada a continuación, con la finalidad de proporcionar una idea certera de los valores:

Impacto
[10] Nivel 10
[9] Nivel 9
[8] Alto (+)
[7] Alto
[6] Alto (-)
[5] Medio (+)
[4] Medio
[3] Medio (-)
[2] Bajo (+)
[1] Bajo
[0] Despreciable

Figura 46. Niveles de impacto

Tomado de (PILAR Análisis y Gestión de Riesgos, 2011)

4.1.5.1 Matriz de Nexus 3524x, 24 10G Ports

Tabla 45.

Matriz de Nexus 3524x, 24 10G Ports

Dimensión	Valor	Valores acumulados
[D] Disponibilidad	[9]	[9]
[I] Integridad de los datos	[1]	[2]
[C] Confidencialidad de los datos	[3]	[3]
[A] Autenticidad de los usuarios y de la información	[2]	[3]
[T] Trazabilidad del servicio y de los datos	[2]	[6]

4.1.5.2 Matriz de VNXE3200;2XSP DPE;25X2.5 DS; 6X300GB 15

Tabla 46.

Matriz de VNXE3200;2XSP DPE;25X2.5 DS; 6X300GB 15

Dimensión	Valor	Valores acumulados
[D] Disponibilidad	[9]	[9]
[I] Integridad de los datos	[1]	[2]
[C] Confidencialidad de los datos	[5]	[5]
[A] Autenticidad de los usuarios y de la información	[2]	[3]
[T] Trazabilidad del servicio y de los datos	[2]	[6]

4.1.5.3 Matriz de InRow SC, 30mm, Air Cooled, Self-contained 200-240V 60Hz

Tabla 47.

Matriz de InRow SC, 30mm, Air Cooled, Self-contained 200-240V 60Hz

Dimensión	Valor	Valores acumulados
[D] Disponibilidad	[8]	[8]
[I] Integridad de los datos	[1]	[1]
[C] Confidencialidad de los datos	[n.a]	[n.a]
[A] Autenticidad de los usuarios y de la información	[3]	[3]
[T] Trazabilidad del servicio y de los datos	[6]	[6]

4.1.5.4 Matriz de RACK PDU 2G, SWITCHED, ZEROU, 5.7KW, 200/208V, (21) C13 & (3) C19

Tabla 48.

Matriz de RACK PDU 2G, SWITCHED, ZEROU, 5.7KW, 200/208V, (21) C13 & (3) C19

Dimensión	Valor	Valores acumulados
[D] Disponibilidad	[10]	[10]
[I] Integridad de los datos	[2]	[2]
[C] Confidencialidad de los datos	[n.a]	[n.a]
[A] Autenticidad de los usuarios y de la información	[2]	[2]
[T] Trazabilidad del servicio y de los datos	[2]	[2]

4.1.5.5 Matriz de UCS 6324 In-Chassis FI with 4 UP, 1x40G Exp Port, 16 10Gb do

Tabla 49.

Matriz de UCS 6324 In-Chassis FI with 4 UP, 1x40G Exp Port, 16 10Gb do

Dimensión	Valor	Valores acumulados
[D] Disponibilidad	[9]	[9]
[I] Integridad de los datos	[1]	[1]
[C] Confidencialidad de los datos	[3]	[3]
[A] Autenticidad de los usuarios y de la información	[2]	[2]
[T] Trazabilidad del servicio y de los datos	[2]	[2]

5. CAPÍTULO V. POLÍTICAS DE SEGURIDAD

5.1 Lineamientos principales para establecer políticas de seguridad

Inicialmente, en el proceso de creación de políticas se debe conocer objetivamente su definición, por lo tanto, se hará referencia a la norma UNE-ISO/IEC 27002 -en la que está basada la presente tesis- que la define como “Intención e instrucción global en la manera que formalmente ha sido

expresada por la Dirección de la organización.” (Comité técnico AEN/CTN 71 Tecnología de la información, 2009).

El presente trabajo se basa en el enfoque del autor se debe puntualizar que las normas son el contraste de lo que sugerido por la herramienta PILAR y la norma UNE-ISO/IEC 27002.

5.1.1 Punto de partida para la seguridad de la información

El punto de partida se considera un cierto número de requisitos o mejores prácticas para la seguridad de la información y sus activos, la norma UNE-ISO/IEC 27002 indica que estos controles para las mejores prácticas en términos de seguridad de la información son los siguientes:

a) “el documento de política de seguridad de la información
b) la asignación de responsabilidades de seguridad de la información
c) la concienciación, formación y capacitación en seguridad de la información
d) el procesado correcto en las aplicaciones
e) la gestión de las vulnerabilidades técnicas
f) la gestión de la continuidad del negocio
g) la gestión de los incidentes y las mejoras en seguridad de la información” (Comité técnico AEN/CTN 71 Tecnología de la información cuya Secretaría desempeña AMETIC, 2009, p.11).

5.1.2 Ámbitos de las Políticas de seguridad

En primer lugar, para detallar estas políticas se debe tomar en cuenta que las orientaciones de las mismas se determinarán en un análisis preventivo de incidentes, y motivando con este análisis para que en un futuro se puedan obtener certificaciones que avalen a la institución. Estos tipos de protección se sustentarán en lo otorgado por la herramienta PILAR como lo indica el siguiente gráfico:

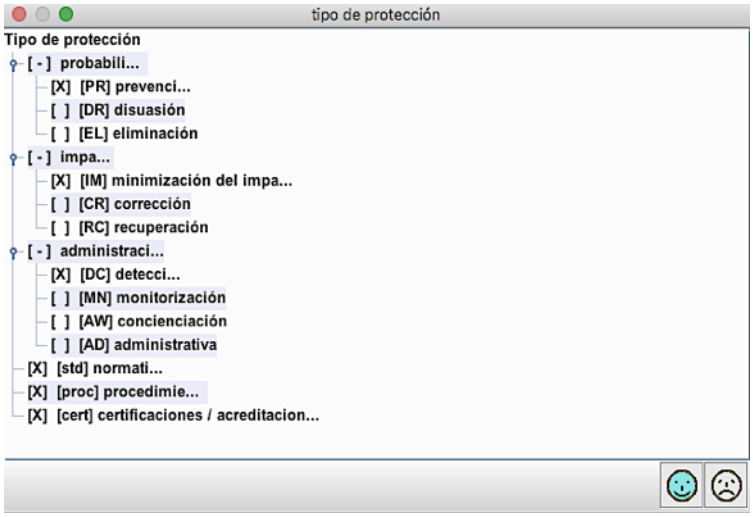

Figura 47. Tipos de protección

El enfoque para entregar diferentes mecanismos de control y de mejores prácticas, se dividirá en los parámetros de:

- Protecciones generales
- Protección de la información
- Protección de las comunicaciones
- Gestión de incidentes
- Organización

5.1.2.1 Políticas de Protecciones Generales

Las políticas a presentarse en esta sección serán divididas en dos grupos para abarcar los mayores requerimientos posibles.

5.1.2.1.1 Control de acceso lógico

1. Disponer de normativa para el control de accesos, basados en: requisitos de seguridad, tipos de acceso, motivos para modificar derechos de acceso, además de una revisión periódicamente.
2. Restricción de acceso a la información, mediante:
    - Autorización previa.
    - No poder acceder a la información sin una verificación previa de los derechos de acceso.

- Establecer acceso a los sistemas en horarios específicos de trabajo, y si fuera el caso determinar control del trabajo fuera del horario normal.
- Controlar privilegios de los usuarios (lectura, escritura, modificación, borrado, ejecución) y de otras aplicaciones.

3. La conexión en terminales, mediante:
    - Restricción de usuarios y grupos a ciertas estaciones de trabajo.
    - Bloqueo de la cuenta tras un número limitado de intentos fallidos.
    - Requerimiento de autorización para restablecer una cuenta bloqueada.
    - Notificación por mensajes indicando usos indebidos del sistema, así como prohibiciones de uso no autorizado.
    - Posterior a la conexión mostrar fecha y hora de la última conexión realizada con éxito.
    - Las contraseñas no pueden ser almacenadas en ningún proceso automático.
    - Los terminales se desconectan automáticamente tras periodos de inactividad.
4. El límite de tiempo de conexión se debe dosificar mediante mecanismos de limitación de red y restringir el número de sesiones concurrentes de un usuario.

5.1.2.1.2 Herramientas de seguridad

1. Establecer una herramienta de detección / prevención de intrusión.
2. Actualizar periódicamente la herramienta, así como el conjunto de firmas de producción utilizado.
3. La herramienta deberá permitir la elaboración de informes en diversos formatos (.html, .txt) y siguiendo diversos criterios (según el sistema, según la red, según la firma de producción).
4. El tipo de sensor debe estar basado en “host” o basado en red.
5. Contar con una herramienta de monitorización de tráfico, para ello la herramienta debe seguir las siguientes directrices:

- Se requiere autorización previa a su utilización.
- Se actualiza regularmente.
- Es posible recopilar, mostrar y analizar el tráfico de red, así como dividir las cabeceras y contenido del tráfico de red en los campos para una gran variedad de protocolos (ARP, RARP, ICMP, IGMP, TCP, UDP, FTP, Telnet, SMTP, DNS, HTTP, SNMP, SSL, IPX).

6. Disparo de alarmas en tiempo real.

5.1.2.2 Políticas de Protección de la Información

Las políticas consideradas en esta sección serán divididas en tres partes:

5.1.2.2.1 Inventario de activos de información

1. Disponer de un inventario de activos de información, el registro debe contar con una persona responsable y actualizarse regularmente.

5.1.2.2.2 Normativa

1. La información debe ser clasificada, así como los procedimientos para el tratamiento de la misma, y si esta se transfiere se debe mantener el nivel de clasificación.
2. Los atributos de seguridad deben mantenerse íntimamente ligados a la información almacenada, en proceso y transmitida.
3. Se protegerán los derechos de propiedad intelectual de la información.

5.1.2.2.3 Protección de confidencialidad

1. Cierta información debe estar cifrada y disponer de una normativa relativa al uso de cifrado.
2. Disponer de procedimientos relativos al cifrado de información, como procedimientos de cifra y de descifrado.
3. El mecanismo de cifrado debe revisar regularmente las vulnerabilidades de los algoritmos y emplear algoritmos certificados / acreditados.

5.1.2.3 Políticas de Protección de las Comunicaciones

Para las comunicaciones la referencia será la red LAN. Dado que en el tercer capítulo fue el activo que presentó mayores riesgos, se han dividido en varias

secciones el establecimiento de estas políticas.

5.1.2.3.1 Inventario de servicios de comunicación

1. Disponer de un inventario de servicios de comunicaciones, que contengan:
    - Registro de servicios propios.
    - Registro de servicios ajenos.
    - Identificación de la persona responsable.
    - Actualización regular del inventario.

5.1.2.3.2 Normativa del uso correcto de las comunicaciones

1. Se dispone de normativa sobre el uso correcto de las comunicaciones.

5.1.2.3.3 Procedimientos de uso de las comunicaciones

1. Se dispone de procedimientos de uso de las comunicaciones, basado en:
    - Uso rutinario.
    - Procedimientos específicos de seguridad.
    - Actuación en caso de funcionamiento anómalo.

5.1.2.3.4 Perfiles de seguridad

1. La aplicación de perfiles de seguridad se realiza de la siguiente forma:
    - Se reducen las opciones a las mínimas necesarias.
    - Se eliminan o modifican las cuentas estándar de usuario.
    - Se eliminan o modifican las cuentas estándar de administrador.
    - Solo los administradores autorizados pueden modificar la configuración.
    - Se activan los servicios de registro de actividad.
    - La aplicación del perfil se revisa periódicamente.

5.1.2.3.5 Cambios (actualizaciones y mantenimiento)

1. Designar personal responsable para autorizar y realizar cambios.
2. Disponer de procedimientos para ejecutar cambios.
3. Evaluar el impacto en la confidencialidad de los datos.
4. Realizar pruebas de regresión.
5. Documentar todos los cambios realizados.

5.1.2.4 Políticas de Gestión de incidentes

En base a lo indicado por la norma UNE-ISO/IEC 27002, en la sección de la Gestión de la continuidad del negocio, se detalla la importancia de minimizar el impacto en la organización por lo cual su objetivo dice lo siguiente "Contrarrestar las interrupciones de las actividades empresariales y proteger los procesos críticos de negocio de los efectos derivados de fallos importantes o catastróficos de los sistemas de información, así como garantizar su oportuna reanudación." (Comité técnico AEN/CTN 71 Tecnología de la información, 2009). Por lo cual las recomendaciones son:

1. Se dispone de procedimientos para la gestión de incidentes, de la siguiente forma:
    - Actuación frente a violaciones de la confidencialidad.
    - Actuación frente a alarmas de los sistemas de detección, prevención de intruso.
    - Actuación frente a alarmas de los sistemas de monitorización de integridad de los ficheros.
    - Actuación frente a alarmas de uso no autorizado del sistema.
    - Actuación frente a estaciones base wifi no autorizadas.
2. En caso de fallo del sistema se deja a este en un estado controlado, de la siguiente manera:
    - Se previene la fuga de información.
    - Se garantiza la integridad de la información.
    - Se previenen daños colaterales sobre otros sistemas.
    - Se previenen daños colaterales sobre personas afectadas.
3. La gestión del incidente se lo manejará de la siguiente manera:
    - Se suspenden cautelarmente los trabajos en el sistema afectado.
    - Se identifica y analiza la causa.
    - Se analiza el impacto del incidente.
    - Se planifica la implantación de medidas correctoras.
    - Se comunica con los afectados por el incidente tanto internos como externos.

- Se comunica con los implicados en el incidente para la recuperación de la información.
- Se informa de las acciones a la autoridad respectiva de la organización.
- Se recogen pistas de auditoria, atendiendo a su validez, calidad y completitud.
- Las evidencias recogidas se almacenan de forma segura.

5.1.2.5 Políticas de la Organización

El principal objetivo de la Organización interna del organismo, es como lo dice la norma UNE-ISO/IEC 27002, es “Gestionar la seguridad de la información dentro de la organización.” (Comité técnico AEN/CTN 71 Tecnología de la información, 2009). Por lo cual las recomendaciones son:

1. La coordinación interna se encargará de:
    - Aprobar metodologías, procedimientos, normas, etc.
    - Identificar no conformidades e incumplimientos.
    - Garantizar que todas las actividades de seguridad se llevan a cabo según la política.
    - La identificación de responsabilidades de la información, servicios, seguridad de la información y sistemas.

6. CONCLUSIONES Y RECOMENDACIONES

6.1 Conclusiones

Los activos fueron categorizados en dos grupos generales, los activos principales o padres y los que dependen o componen a los mismos. Esto sirvió para que al momento de asignar posibles peligros, se hereden los valores, para aproximarse a datos más específicos y precisos.

La herramienta PILAR de Análisis y Gestión de Riesgos cumplió todas las expectativas generadas sobre el manejo de los activos, brindando una observación detallada de los mismos y permitiendo visualizar sus principales debilidades.

Para el proceso de identificación de activos, se agrupó por su finalidad en la estructura del data center, así como cuáles serían los principales peligros en los enfoques que definen las normas ISO.

Una vez realizado el proceso de identificación, se obtuvo en base a fórmulas matemáticas y criterios personales asimilados en las diferentes materias, las escalas de valoración de riesgos, que han sido reflejados en las matrices y gráficos de riesgos los cuales se pudo concluir que son valores muy próximos a la situación actual del data center.

En el capítulo de las políticas de seguridad se procedió a dividirlas en diferentes secciones, tomando en cuenta especialmente los sectores más vulnerables especificados en el capítulo anterior, teniendo consideraciones reales con la finalidad de ser implementadas en todo lo concerniente al data center.

La norma ISO 27002 sirvió de base para realizar un contraste con las políticas entregadas por la herramienta PILAR, por lo cual todos los objetivos específicos y por ende el objetivo general fueron ejecutados en su totalidad,

siguiendo todas las indicaciones del docente guía.

Al momento de realizar un trabajo de similares características o con objetivos relacionados, el elegir una herramienta de software para evaluar los activos es de suma importancia, ya que el resultado obtenido puede ser erróneo y en algunos casos empírico.

El principal beneficio de usar la herramienta PILAR fue brindar a la institución un producto final que tiene la garantía de aplicar normas especializadas y certificadas en la materia. Por esta razón, el impacto a futuro será fructífero no solo para la facultad sino también a la universidad, pues constituirá una base para futuros proyectos.

6.2 Recomendaciones

El uso de la herramienta PILAR permitió por sus características entregar un trabajo que puede ser tomado en cuenta para futuras certificaciones en ámbitos de seguridad para la institución educativa.

Cada activo, de manera inherente, forma en conjunto un engranaje que cumple su propósito, por lo cual tener una valoración de su importancia individual es sumamente valiosa para dar mayor prioridad a su seguridad.

Las políticas de seguridad son procedimientos que buscan prevenir un posible incidente de riesgo para la organización, y en caso de suceder se convierten en una herramienta de ayuda para solucionar el inconveniente o en su caso contenerlo. Ante la posibilidad de no contar con estos métodos, la organización se ve expuesta a un riesgo latente y a su vez puede generar más daño que el beneficio que se está buscando.

Los factores externos, por lo general, son los que más inconvenientes presentan, por lo cual siempre es recomendable tomar medidas preventivas,

que se enfocan más a la logística; a la postre en temas económicos son muy beneficiosos, dado su bajo coste.

REFERENCIAS

Comité técnico AEN/CTN 71 Tecnología de la información cuya Secretaría desempeña AMETIC, (2012). Tecnologías de la información Técnicas de seguridad Sistemas de Gestión de la Seguridad de la Información (SGSI) Visión de conjunto y vocabulario. Madrid, España: AENOR.

Comité técnico AEN/CTN 71 Tecnología de la información, (2009). Tecnología de la Información Técnicas de seguridad. Código de buenas prácticas para la gestión de la seguridad de la información. Madrid, España: AENOR.

CDW Corporation, (s.f.). *Cisco Nexus 3524x - switch - 24 ports - managed - rack-mountable*. Recuperado el 23 de agosto de 2016, de https://www.cdw.com/shop/products/Cisco-Nexus-3524x-switch-24-ports-managed-rack-mountable/3649095.aspx

EAR / PILAR, (2014). EAR / PILAR documentación. Recuperado el 24 de agosto de 2016, de http://www.pilar-tools.com/doc/v54/help_es_e_2014-02-12.pdf

Fundación Wikipedia, (2016). Trazabilidad. Recuperado el 23 de agosto de 2016, de https://es.wikipedia.org/wiki/Trazabilidad

Garcis, R. M, (2012). Recuperado el 31 de agosto de 2016, de PILAR Análisis y Gestión de Riesgos: https://docs.google.com/document/d/15TYUClkxF_WYA1kTqCJa6bwQaCLlaEkwAQ-8EvFO7js/edit?pli=1

Mendoza, M. Á, (2014). welivesecurity Noticias, opiniones y análisis de la comunidad de seguridad de ESET. Recuperado el 30 de agosto de

2016, de 8 pasos para hacer una evaluación de riesgos (parte II): http://www.welivesecurity.com/la-es/2014/09/30/8-pasos-evaluacion-de-riesgos-2/

PILAR Análisis y Gestión de Riesgos, (2011). Glosario de Términos. Recuperado el 13 de noviembre de 2016, de http://www.pilar-tools.com/es/glossary/index.html

Portal Administración Electrónica PAE, (s.f). MAGERIT v.3 : Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Recuperado el 22 de agosto de 2016, de http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.V8IPpLVX-CR

Sena, L., & Tenzer, S. M, (2004). Introducción a Riesgo Informático. Recuperado el 30 de agosto de 2016, de http://www.ccee.edu.uy/ensenian/catcomp/material/riesgo.pdf

Universidad Distrital Francisco José de Caldas Oficina Asesora de Sistemas, (2011). Capitulo 5 Subproceso: Gestión del Riesgo. Recuperado el 30 de agosto de 2016, de http://www.udistrital.edu.co:8080/documents/276352/356568/Cap5GestionRiesgo.pdf

10Gtek, (2015). 10Gtek® for *Cisco SFP-H10GB-CU3M 10GBASE-CU Direct Attach Copper Cable, Twinax Cable, Passive,3-meter*. Recuperado el 15 de septiembre de 2016, de https://www.amazon.com/10Gtek®-SFP-H10GB-CU3M-10GBASE-CU-Passive-3-meter/dp/B00XVL71F2

Alibaba, (2016). *Cisco Server UCSB-5108-PKG-HW UCS 5108 Packaging for chassis with half width blades*. Add to My Cart Add to My Favorites Cisco Server UCSB-5108-PKG-HW UCS 5108 Packaging for chassis with half width blades. Recuperado el 18 de septiembre de 2016, de

https://switch-router.en.alibaba.com/product/60328527540-802096184/Cisco_Server_UCSB_5108_PKG_HW_UCS_5108_Packaging_for_chassis_with_half_width_blades_.html

APC, (2016). *APC Rack Air Containment Rear Assembly for NetShelter SX 42U and InRow 600mm*. Recuperado el 16 de septiembre de 2016, de http://www.apc.com/shop/kn/en/products/APC-Rack-Air-Containment-Rear-Assembly-for-NetShelter-SX-42U-and-InRow-600mm/P-ACCS1001

APC, (2016). *APC Symmetra RM 6kVA Scalable to 6kVA N+1 208/240V w/ 208 to 120V Step-Down Transformer (4) L5-20R*. Recuperado el 16 de septiembre de 2016, de http://www.apc.com/shop/us/en/products/APC-Symmetra-RM-6kVA-Scalable-to-6kVA-N+1-208-240V-w-208-to-120V-Step-Down-Transformer-4-L5-20R/P-SYH6K6RMT-TF3

APC Guard, (2015). *APC NetBotz Room Monitor 355*. Recuperado el 16 de septiembre de 2016, de http://www.apcguard.com/NBWL0355.asp

ATN, (2013). *InRow SC, 300mm, Air Cooled, Self-contained 200-240V 60Hz.* Recuperado el 16 de septiembre de 2016, de http://atn.com.mx/4066/pdf/APC_Inrow_ACSC100.pdf

B&H, (2016). *APC NetShelter SX 42U Enclosure (600 x 1070mm, Black).* Recuperado el 16 de septiembre de 2016, de https://www.bhphotovideo.com/c/product/616901-REG/APC_AR3100_NetShelter_SX_42U_Enclosure.html?gclid=Cj0KEQjw3s6-BRC3kKL_86XDvq4BEiQAAUqtZ4zDTDNTOFjjwKG6L8fyR_A5amhAWikWJWl-qZ-6DQgaAoHi8P8HAQ&c3api=2572%2C113041717267

CDW Corporation, (s.f.). *Cisco Nexus 3524x - switch - 24 ports - managed - rack-mountable*. Recuperado el 23 de agosto de 2016, de https://www.cdw.com/shop/products/Cisco-Nexus-3524x-switch-24-ports-managed-rack-mountable/3649095.aspx

Cisco, (2013). *Cisco R42610 Rack*. Recuperado el 16 de septiembre de 2016, de http://www.cisco.com/c/dam/en/us/products/collateral/servers-unified-computing/ucs-c-series-rack-servers/r42610_specsheet.pdf

Cisco, (2015). *Cisco Nexus 3548 Switch NX-OS Release Notes, Release 6.0(2)A6(1)*. Recuperado el 15 de septiembre de 2016, de http://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus3548/sw/release_notes/602_A6_1/n3k_rel_notes_6_0_2_a6_1.html#43761

Cisco, (2015). *Cisco RP Series Power Distribution Units*. Recuperado el 16 de septiembre de 2016, de http://www.cisco.com/c/en/us/products/collateral/servers-unified-computing/rp-series-power-distribution-units/data_sheet_c78-638923.html

Cisco, (2016). *Cisco UCS 5108 Blade Server Chassis*. Recuperado el 18 de septiembre de 2016 , de http://www.cisco.com/c/dam/en/us/products/collateral/servers-unified-computing/ucs-b-series-blade-servers/spec_sheet_c17-644224.pdf

Cisco, (2016). *Cisco Gigabit Ethernet Transceiver Modules Compatibility Matrix.* Recuperado el 16 de septiembre de 2016, de http://www.cisco.com/c/en/us/td/docs/interfaces_modules/transceiver_modules/compatibility/matrix/GE_Tx_Matrix.html

Cisco, (s.f). *Power Cord Specifications*. Recuperado el 15 de septiembre de 2016, de

http://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/c/hw/C220/install/C220/portcabl.pdf

EMC Corporation, (2012). *EMC VNXe SERIES STORAGE SYSTEMS.* Recuperado el 15 de septiembre de 2016, de https://www.emc.com/collateral/hardware/white-papers/h8178-vnxe-storage-systems-wp.pdf

EMC Corporation, (2015). *EMC VNXe3200 UNIFIED STORAGE SYSTEM.* Recuperado el 16 de septiembre de 2016, de https://www.emc.com/collateral/software/specification-sheet/h13842-vnxe-ss.pdf

IThelp, (2013). *Cisco SMARTnet for UCS Central Per UCS Domain License (Physical) Price.* Recuperado el 17 de septiembre de 2016, de https://www.ithsc.com/ciscohardwaremaintenance/SW-App-Sprt&Upgd-CON-SAU-UCSMGRAS-38_82-p-695532.html

MISCO, (s.f). *8 GBPS FIBRE CHANNEL SW SFP+ LC SPARE*. Recuperado el 16 de septiembre de 2016, de http://www.misco.es/product/518051/8-GBPS-FIBRE-CHANNEL-SW-SFPplus-LC-SPARE

Portal Administración Electrónica PAE, (2012). MAGERIT v.3 : Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Recuperado el 22 de agosto de 2016, de http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.V8IPpLVX-CR

Provantage, (2016). *Cisco Systems Nexus 3064PQ Accessory Kit*. Recuperado el 15 de septiembre de 2016, de http://www.provantage.com/cisco-systems-n3k-c31108tc-v~7CSCO3EP.htm

SRO, (2016). *Rack PDU 2G, Switched, Zero-U Vertical, 5.7KW, 200/208V, 21 x C13 & 3 x C19 (AP8961)*. Recuperado el 16 de septiembre de 2016, de http://www.server-rack-online.com/ap8961.html

ANEXOS

Anexo 1.- Imágenes del data center de la FICA

Figura Componente EMC²

Figura Componente APC

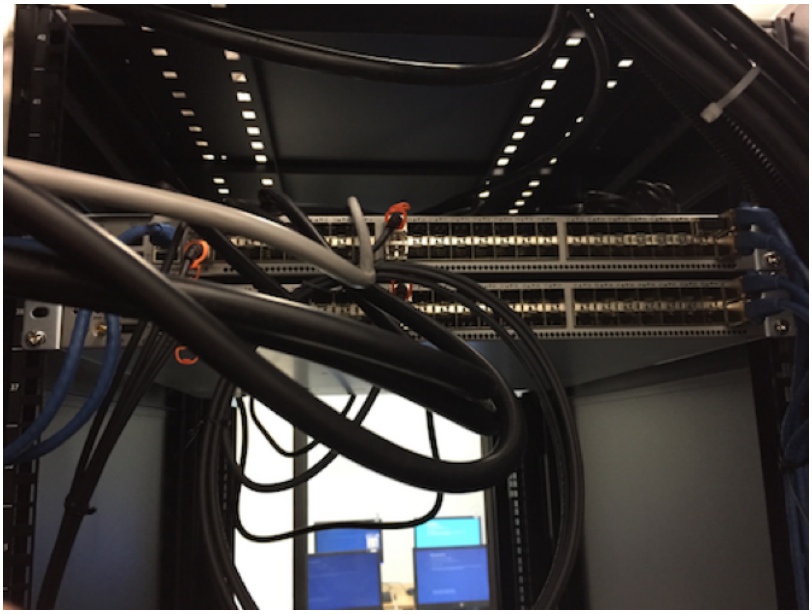

Figura Componentes Switches

Figura Componente PDU

Figura Componente Sistema de ventilación

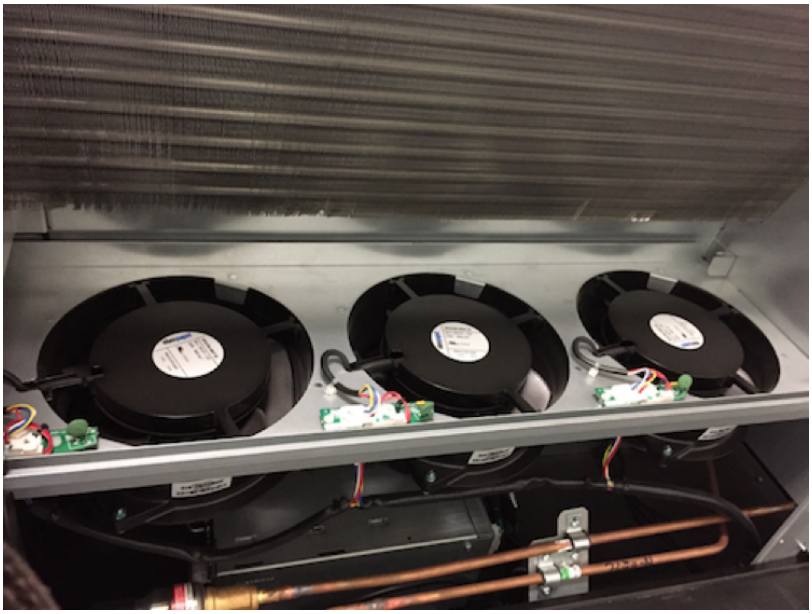

Figura Componente Ventiladores

Anexo 2.- Gráficos estadísticos herramienta PILAR

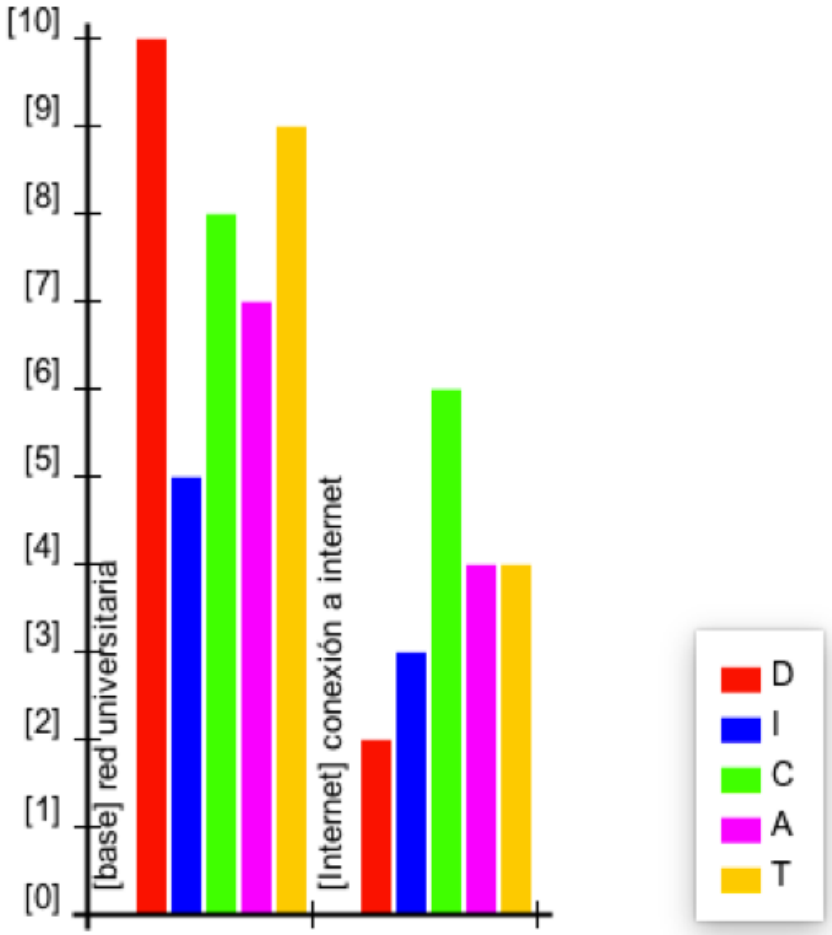

Figura Valor / Dominio de seguridad

Figura Valor / Activo