PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR SEDE ESMERALDAS

FACULTAD:

CIENCIAS ADMINISTRATIVAS Y CONTABLES

ESCUELA:

INGENIERÍA DE SISTEMAS Y COMPUTACIÓN

TESIS DE GRADO

GESTIÓN DE RIESGO DEL DATA CENTER DE LA PUCESE BASADA EN ESTÁNDARES INTERNACIONALES

LÍNEA DE INVESTIGACIÓN

GOBIERNO Y ADMINISTRACIÓN DE TECNOLOGÍA DE INFORMACIÓN

PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERA DE SISTEMAS Y COMPUTACIÓN

AUTORA:

CARMEN MOSQUERA RIVA

ASESORA:

ING. SUSANA PATIÑO ROSADO

ESMERALDAS, JULIO DEL 2016

Disertación Aprobada luego de haber dado cumplimiento de los requisitos exigidos por el reglamento de Grados de la Pontificia Universidad Católica del Ecuador Sede en Esmeraldas, previa la obtención del Título de Ingeniera de Sistemas y Computación.

Ing. Susana Patiño Rosado
ASESORA DE TESIS

Ing. Kléber Vera Tortorella
LECTOR 1

Ing. Juan Casierra Cavada
LECTOR 2

Ing. Xavier Quiñónez Ku
DIRECTOR DE ESCUELA

FECHA: …….

AUTORÍA

Yo, **CARMEN PILAR MOSQUERA RIVA,** declaro que la presente investigación enmarcada en el actual trabajo de tesis es absolutamente original, auténtica y personal.

En virtud que el contenido de esta investigación es de exclusiva responsabilidad legal y académica de la autora y de la PUCESE.

_____

CARMEN PILAR MOSQUERA RIVA

C.I. 080321597-9

AGRADECIMIENTO

A mi padre celestial, Dios, por bendecirme y darme la sabiduría para concluir este proyecto de tesis porque sin Él nada hubiera sido posible.

A mis padres, Dora y Martín, por ser pilar fundamental en mi formación como profesional y brindarme los recursos para el desarrollo de mi carrera universitaria.

A mis hermanos, Sergio, Edwin y Mónica, por darme su apoyo incondicional.

A mi asesora, Ing. Susana Patiño, por su tiempo y dedicación para la elaboración de mi tesis, quien con su conocimiento contribuyó para la realización de un buen trabajo.

A mis docentes, profesores de toda la carrera universitaria, que formaron mi criterio como ingeniera en cada una de las cátedras impartidas.

DEDICATORIA

A mi esposo, Bolívar, por su apoyo y ánimo que me brinda día con día para alcanzar nuevas metas, tanto profesionales como personales.

A mis hijos, Nahomy y Martín, prolongación de mi vida y fuente inagotable de fortaleza.

ÍNDICE DE CONTENIDOS

CAPÍTULO III

CAPÍTULO IV

ÍNDICE DE TABLAS

ÍNDICE DE GRÁFICOS

RESUMEN

El presente proyecto está desarrollado de acuerdo a la necesidad que se presenta en el Departamento de TIC´s de la PUCESE con respecto al Data Center, que ha percibido la responsabilidad de salvaguardar la información alojada en él.

Se obtuvo información referente a la manera como es administrado el data center de la PUCESE, en base a entrevistas realizadas al personal del departamento que se involucra diariamente con esta infraestructura; así como de una encuesta realizada a los usuarios de los servicios web considerados críticos, es decir, docentes y personal administrativo.

El principal objetivo de esta investigación fue realizar una gestión de riesgos para el data center de la PUCESE basada en estándares internacionales. El aspecto de alimentación eléctrica, climatización, seguridad, falta de protección ante eventualidades, no contar con políticas de tratamiento de riesgos; todas estas variables afectan el desempeño de la infraestructura tecnológica para la institución; se hizo el análisis de riesgo para evaluar el nivel de preparación ante los impactos producidos por las falencias en el data center.

La información debe mantenerse integra y su cuidado confiable, el funcionamiento de los equipos servidores debe ser efectivo y eficiente; y los servicios que provee un centro de procesamiento de datos debe estar siempre disponibles. Sin embargo, estos requerimientos no se alcanzan a cabalidad en el data center de la PUCESE. Por lo tanto, para facilitar la administración de riesgos del centro de datos se desarrolló una gestión de riesgos de acuerdo a las normas ICREA Std-131-2013 e ISO/IEC 27001.

El presente trabajo se compone de cuatro capítulos, expuestos a continuación:

- En el Capítulo 1. MARCO TEÓRICO, en el cual se define los conceptos sobre gobierno de TI (Tecnologías de la Información), gestión de riesgos, seguridad de TI, estándares internacionales, data center, entre otros.

- En el Capítulo 2. DIAGNÓSTICO, se establece el antecedente diagnóstico, objetivos diagnósticos y las variables consideradas en este proyecto, también se

muestra la mecánica operativa para la investigación, finalizando con la determinación del problema.

- En el Capítulo 3. PROPUESTA, se inicia con los antecedentes consideradores para la realización de este proyecto, objetivos de la propuesta, el alcance de la propuesta, la metodología aplicada para evaluar la infraestructura según las normas ICREA 2013 e ISO/ IEC 27001, plan de tratamiento de riesgos, observaciones, recomendaciones y conclusiones obtenidos del análisis de riesgos.

- En el Capítulo 4. IMPACTOS, se detalla los niveles de impactos que tiene el proyecto; luego se detalla las conclusiones y recomendaciones. Finalmente la bibliografía y anexos que validan la presente investigación.

ABSTRACT

This project is developed according to the needs presented in the Department of ICT of PUCESE regarding the Data Center, that has perceived the responsibility to safeguard the information stored on it.

Information was obtained concerning the way it is managed the data center of the PUCESE, based on interviews with department staff who engages daily with this infrastructure; as well as a survey of users of the web services considered critical, i.e. teachers and administrative staff.

The main objective of this research was to conduct risk management for the data center of the PUCESE based on international standards. The appearance of power, HVAC, security, lack of protection against eventualities not have policies risk treatment; all these variables affect the performance of the technological infrastructure for the institution; risk analysis was done to assess the level of preparedness for the impacts of shortcomings in the data center.

The information must be kept integrated and reliable care, operation of server computers must be effective and efficient; and services that provides a data center must be always available. However, these requirements are not met fully in the data center of the PUCESE. Therefore, to facilitate risk management data center risk management according to the ICREA Std-131-2013 and ISO / IEC 27001 was developed.

This paper consists of four chapters, set forth below:

- Chapter 1. THEORETICAL FRAMEWORK, in which the concepts of government IT (Information Technology), risk management, IT security, international standards, data center, including defined.

- Chapter 2. DIAGNOSIS, diagnosis history, diagnosis purposes and the variables considered in this project is established, operational mechanics research also shows, ending with problem determination.

- Chapter 3. PROPOSAL, begins with consideradores background for this project, objectives of the proposal, the scope of the proposal, the methodology used to assess the infrastructure according to the ICREA 2013 and ISO / IEC 27001, plan risk treatment, observations, recommendations and conclusions of the analysis of risks.

- Chapter 4. IMPACTS, impact level has the project or the present investigation is detailed; then detailed conclusions and recommendations. Finally the bibliography and appendices that validate this investigation.

CAPÍTULO I

1 MARCO TEÓRICO

1.1 Pontificia Universidad Católica del Ecuador Sede Esmeraldas

1.1.1 Filosofía Institucional

La Pontifica Universidad Católica del Ecuador Sede Esmeraldas (PUCESE) es una institución de educación superior asentada en la provincia. Fundada oficialmente el 5 de junio del 1981 con el compromiso de formar profesionales capacitados con obligación moral para aportar con la economía de la provincia. Promueve las normas del buen vivir y buena convivencia entre sus miembros, garantizando la práctica de valores.

El propósito de la PUCESE se ve reflejado en su misión, en el que pretende:

> *"Formar continua, personalizada e integralmente a seres humanos con sentido emprendedor social, ético, crítico y autocrítico, a la luz del evangelio, capaces de liderar y generar transformaciones en orden a una provincia solidaria, justa, pacífica y que respeta la biodiversidad, desarrollando propuestas científicas, innovadoras y sostenibles." (PEDI, PUCESE, 2011).*

La institución está enfocada en su intención de superar límites existentes y de crecer en el campo formación de profesionales, expresando en su misión lo siguiente:

> *"La PUCESE será una institución educativa en búsqueda permanente de la excelencia académica, con carreras acreditadas, apoyada en la estructura de trabajo por áreas de conocimiento; estrechamente vinculada a organizaciones de los sectores educativos, productivos, de salud y medioambientales de Esmeraldas, como provincia costera; participando en redes de investigación, intercambio y formación de estudiantes y docentes con instituciones de educación superior nacionales e internacionales, a través de trabajo cooperativo en propuestas de transformación social." (PEDI, PUCESE, 2011).*

1.1.1.1 Objetivos Estratégicos

Para alcanzar el éxito como institución y dar seguimiento al cumplimiento de la misión y visión PUCESE, se plantea 7 objetivos que representan las metas propuestas (PEDI-PUCESE, 2012):

- Fortalecer la estructura y los procesos administrativos y académicos.
- Elevar el nivel académico del ingreso y egreso, y la permanencia en la universidad.
- Impulsar la investigación y la innovación.
- Mejorar los canales de comunicación.
- Implementar las tics en todos los niveles de la gestión académica y administrativa
- Ser una universidad emprendedora con capacidad para generar proyectos empresariales y procesos de liderazgo orientados a los planes de desarrollo provincial y nacional.
- Fortalecer los vínculos con la comunidad que generen transformaciones efectivas en la provincia.

1.1.2 Estructura Orgánica

La PUCESE está conformada por departamentos, donde las principales autoridades son el Consejo Directivo, seguido del Pro-Rectorado a cargo de Lic. Aitor Urbina y el Consejo Académico.

El departamento de Sistemas consta entre las dependencias medulares de Pro-Rectorado debido a la importancia en el desarrollo de las actividades diarias en la institución, en la siguiente grafica se observa su ubicación en el organigrama de la PUCESE:

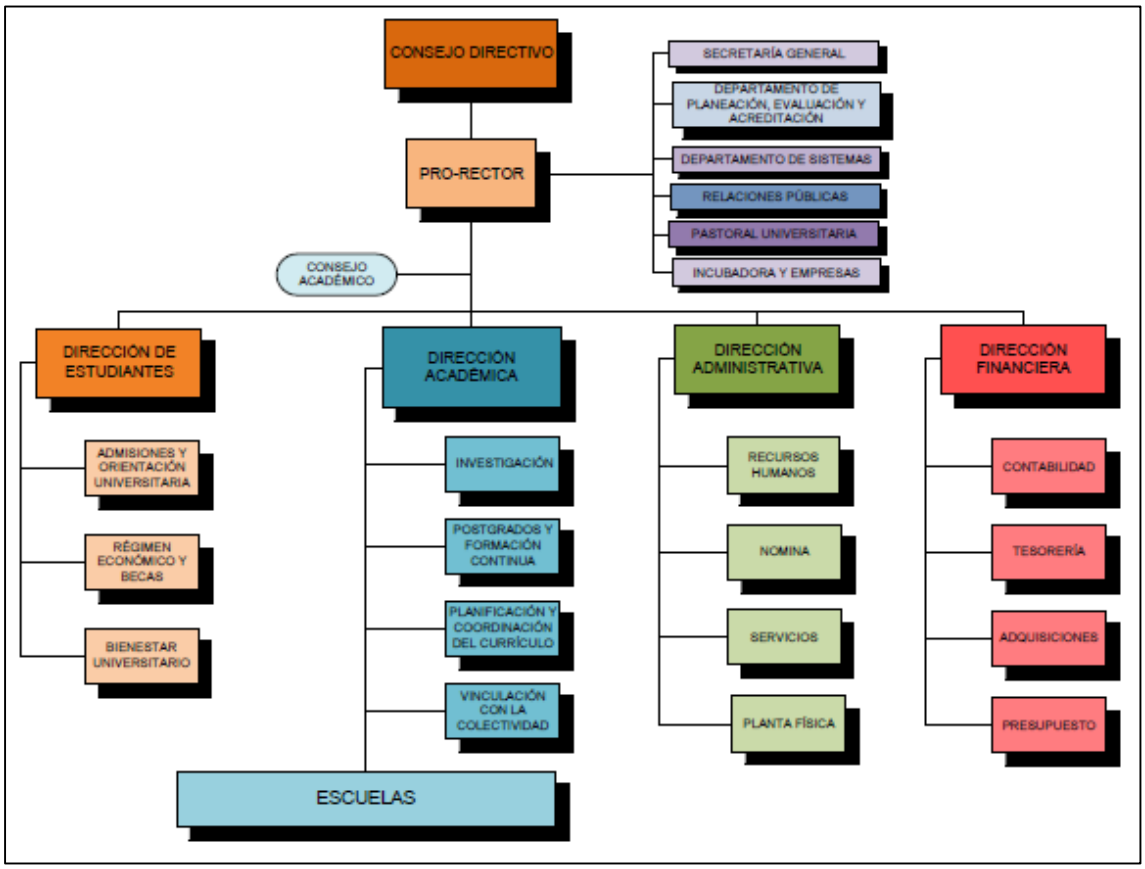


Gráfico 1: Organigrama PUCESE (PEDI-PUCESE, 2012)

1.1.3 Departamento de TIC’s

Al incrementarse la demanda del servicio de educación superior en estos últimos años en el país, y por ende, la PUCESE ha tenido que ampliar su oferta académica a la sociedad, esto conlleva al crecimiento en los servicios tecnológicos necesarios para poder responder a dicha demanda.

Desde esta óptica, la PUCESE debe garantizar disponibilidad, confiabilidad y continuidad de los servicios informáticos para el diario ejercicio del área administrativa y académica de la comunidad universitaria.

La PUCESE cuenta con un departamento de TIC’s que se encuentra organizado de la siguiente manera:

Gráfico 2. Estructura del Departamento de TIC's.

Fuente: propia del autor

El área de Redes y Comunicaciones vela por el buen funcionamiento de los servidores, dispositivos de comunicaciones de voz y datos. Es responsable de proteger los activos de información alojados en el data center, administra la infraestructura de redes desde el punto

de vista lógico y físicos. Lleva tareas de mantenimiento, control y desarrollo del cableado estructurado y de la ampliación de servicios de red.

Para todo lo antes mencionado la PUCESE cuenta con una red de voz y datos, con servicios de las siguientes características:

- Está conectada al internet con un servicio de banda ancha corporativo prestada por una fusión entre CNT, que es servicio de última milla entre Esmeraldas –Quito, y ReadyNet como puerta de enlace al internet; con ancho de banda de 100 MB.

- Se cuenta con un equipo Router Cloud MikroTik que realiza funciones de administrador de la red LAN de la PUCESE.

- Se cuenta con servidores de comunicaciones clones configurados con Sistema Operativo Linux CentOs V6.5, y servidores de aplicaciones con Windows Server 2008 y Linux CentOs V6.5.

- En Desarrollo de Software se generan soluciones requeridas para automatizar las tareas de financieras, de personal y académicas. Dichas soluciones son adquiridas a proveedores de software, y si es posible se desarrollan directamente por el equipo del departamento.

- Como Soporte Técnico se utiliza servidores de HP Proliant G5 y G8, con procesadores Xeon, conexiones de Gigabit Ethernet y discos en RAID.

1.2 Gobierno de TI

1.2.1 Generalidades

La información está presente en cada una de las actividades que se realizan en las empresas y considerando la creciente exigencia en el empleo de tecnología en cada proceso, es necesario el uso de algún recurso de TI (Tecnología de la Información) **(Mariana Arroyo, 2015)**, además debe estar disponible para poder realizar la toma decisiones, es por ello que se emplea el concepto de Gobierno de TI.
Es el conjunto de relaciones y procesos que realiza el área de tecnología de la información en conjunto con la alta gerencia para usar los recursos de manera eficiente. Vinculando las metas de la organización, con los del Departamento de TI.

Como beneficio hace posible que los servicios de los TI se brinden con el máximo valor posible y se mantenga a las Tecnologías de la Información alineadas con las estrategias del negocio.

El Gobierno de TI, es una metodología de trabajo que orienta a proveer estructuras que incorpora a los procesos de TI, recursos de TI con las tácticas y objetivos de la empresa.

1.2.2 Continuidad del Negocio

Detalla los procesos y procedimientos que una entidad realiza para garantizar las funciones esenciales puedan continuar durante y después de una eventualidad. Debido a que es un área crítica y demanda mayor atención se plantea la gestión para la continuidad del negocio.

La Gestión de la Continuidad del Negocio (GNC) es el proceso de administración integral para establecer y mantener un plan que permita al negocio y a TI responder a incidentes e interrupciones de servicio para la operación continua de los procesos críticos para el negocio

y los servicios de TI requeridos, y mantener la disponibilidad de la información a un nivel aceptable para la empresa. (Ríos, 2014)

Además, permite anticiparse a las condiciones de crisis y garantizar el normal desarrollo de actividades, identificando riesgos de magnitud considerable que pone en peligro el funcionamiento de las actividades del negocio e ideando acciones a tomar en caso de que éstos se susciten.

1.2.2.1 Ciclo de vida de la Gestión de Continuidad del Negocio

Ofrece una correcta orientación sobre las medidas que se desempeñan, las cuales ocupan un papel importante en el mantenimiento y rápida restauración en las actividades.

La **gráfica 3** muestra el ciclo de vida de la Gestión de Continuidad del Negocio:

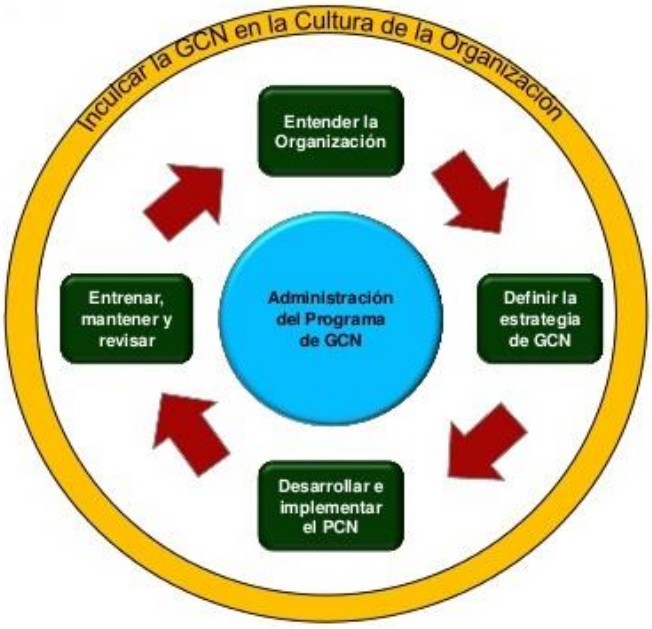


Gráfico 3. Ciclo d vida del GNC (Ríos, 2014)

1.2.3 Gestión de Riesgos Tecnológico

Cuando inicia actividades una institución la gerencia debe tener en cuenta que el riesgo es latente y estará presente en todo momento del desarrollo, por medio de diferentes factores como: cambios en el entorno, la intensidad de la competencia y la tecnología que va avanzando de manera vertiginosa.

Para disminuir estos factores se incorpora a las empresas la Gestión de Riesgos Tecnológicos.

La gestión de riesgos es un proceso efectuado por el departamento de riesgos de una entidad, su director y todo su personal restante. Está diseñado para identificar eventos potenciales que puedan afectar a la organización, gestionar sus riesgos dentro del riesgo aceptado y proporcionar una seguridad razonable sobre el logro de los objetivos. (Andrade, 2013)

Las estrategias de la gestión de riesgos incluyen trasladar el riesgo a otra parte, evitar el riesgo, minimizar el efecto negativo o la probabilidad del riesgo, incluso la aceptación de algunas o todas las consecuencias posibles o reales de un riesgo particular.

Como objetivo, busca reducir los diferentes riesgos relativos a un escenario preseleccionado a un nivel aceptado por la sociedad. Se puede referir a numerosos tipos de amenazas provenientes del medio ambiente, la tecnología, los seres humanos, las empresas y la política. Por otra parte, involucra a todos los recursos disponibles por los seres humanos o por una entidad de manejo de riesgos.

Para la gestión de riegos de una infraestructura tecnológica existen normas, marcos de trabajo y metodologías que se emplean. (Chavez, 2013)

A continuación se detallan las mismas:

- **ISO/IEC 27005:2008**

Proporciona directrices para la gestión de riesgos de seguridad de la información. Apoyada en conceptos generales especificados en la ISO/IEC 27001 y ha sido diseñada para ayudar a la puesta en práctica satisfactoria del análisis y la gestión del riesgo, fase principal del diseño de todo buen sistema de gestión de la seguridad de la información. (Avellaneda, 2008)

Es aplicable a todo tipo de organización que tenga la intención de manejar los riesgos que se susciten en el ámbito de la seguridad de la información.

- **NIST SP800-30**

Es una guía que permite administrar riesgos de TI enfocados en sistemas de información-SDLC. (Chavez, 2013)

Principales objetivos:

a) Proteger la habilidad de la organización para alcanzar su misión (no sólo activos de TI).
b) Una función esencial de administración, no sólo en la administración técnica.
c) Proveer lineamientos para el desarrollo de un programa de administración de riesgos.
d) Proveer información con controles de seguridad efectivos.

- **UNE 71504:2008**

Es una norma realizada por la Asociación Española de Normalización y Certificación (AENOR), orientada al análisis y la gestión de riesgos para los sistemas de información. Según esta norma, a la gestión de riesgos se la define como base para las fases de caracterización de activos, cálculo de riesgo intrínseco, cálculo de riesgo efectivo, entre otros. (Devia & Pardo, 2014)

- **MAGARIT**

Fue desarrollado con el sentido de servir de metodología de análisis y gestión de riesgos, que ofrece un método sistemático para analizar los riesgos derivados del uso de tecnologías de la información y comunicaciones para implementar medidas de control más adecuadas que permitan tener riesgos mitigados.

Se basa en analizar el impacto que puede tener para la empresa la violación de la seguridad, buscando identificar las amenazas que pueden llegar a afectar la compañía y las vulnerabilidades que pueden ser utilizadas por estas amenazas, logrando así tener una identificación clara de las medidas preventivas y correctivas más apropiadas. (Amaya, 2013)

1.3 Seguridad de TI

1.3.1 Aspectos Generales de Seguridad de TI

Es una disciplina que se encarga de preservar la integridad y la privacidad de la información almacenada en un sistema informático. Puede emplear herramientas para proteger desde el punto de vista de software o mediante dispositivos. Las amenazas pueden darse desde software maliciosos que se instalan en las computadoras personales o llegar de manera remota por medio de la Internet.

Se enfoca a la protección integral de una infraestructura tecnológica, basándose en una serie de estándares, protocolos, reglas, métodos y leyes concebidas para minimizar los riesgos que se presenten afectando a la infraestructura o a los datos contenidos en ella y a todo lo que una entidad valore que signifique riesgoso, como la incorrecta manipulación de información confidencial.

Para que sea confiable, la Seguridad de TI debe garantizar la integridad de la información, la confidencialidad de los datos manejados y permitir la completa estabilidad en el sistema con el empleo de herramientas.

1.3.2 Riesgos

Para la Real Academia de la Lengua Española define riesgo como: "Contingencia o proximidad de un daño."

En cambio para el área de Tecnología de la Información, define a los riesgos como tomados en negocios asociados con el uso, propiedad, operación, la participación, la influencia y la adopción de TI dentro en una empresa. **(Solano & Zúñiga, 2013)**

1.3.2.1 Riesgo Tecnológico

La tecnología está siendo utilizada de manera inadecuada para incursionar en las organizaciones aprovechando las vulnerabilidades existentes por protecciones inapropiadas y por su constante cambio, motivo que hacen cada vez más difícil mantener actualizadas esas medidas de seguridad.

La mala utilización de la tecnología es la causante de las vulnerabilidades y riesgos que exponen las empresas. El riesgo tecnológico se percibe desde tres aspectos **(Castro, 2012)** y cada uno tiene su manera de ser contrarrestado, detallado a continuación:

- **Infraestructura tecnológica**

Se aplica procedimientos de control y barreras físicas ante amenazas para prevenir daño o acceso no autorizado a recursos e información confidencial valiéndose de controles de acceso físico, tarjetas de identificación, servicios básicos de soporte de continuidad, entre otros. (Castro, 2012)

- **Lógico**

Se da con respecto al uso de software y sistemas, enfocados a proteger los datos y garantizar el acceso autorizado a la información por parte de usuarios a través de procedimientos correctos haciendo uso de control de acceso a la red interna y externa, soluciones de protección contra programas maliciosos, protocolos para el intercambio y cifrado de información y demás opciones. (Castro, 2012)

- **Factor humano**

Considerado como critico debido a su naturaleza impredecible, el personal o recurso humano debe ser regulado y orientado para la concienciación de procedimientos realizados en cada una de sus actividades.

1.4 Estándares Internacionales

1.4.1 ITIL

1.4.1.1 Generalidades

Biblioteca de Infraestructura de TI es el enfoque de más aceptación en la Gerencia de Servicios de TI, por proporcionar un conjunto cohesivo de las mejores prácticas. Se alinea con varias normas de calidad internacionales como la ISO/IEC 20000 (Código de Prácticas de la Gestión de Servicios de TI). **(PeopleCert, 2015)**

Es un conjunto de libros en los cuales se encuentran documentados todos los procesos referentes a la provisión de servicios de tecnologías de la información para organizaciones. **(Soporte Remoto Mexico, 2008)**

Mediante procedimientos, roles, tareas y responsabilidades que se pueden acoplar a cualquier organización de TI, genera una descripción minuciosa de mejores prácticas, que facilitan la comunicación y administración de los servicios de TI.

Es un marco de trabajo orientado a procesos que puede ser utilizado y adaptado por las organizaciones.

1.4.1.2 Ciclo de vida de los servicios de TI

Se basa en un ciclo de vida que consta de cinco etapas, cada una tiene un conjunto de procesos/ actividades/ buenas practicas descritas en un núcleo. **(Oriente, 2014)**

Gráfico 4. Ciclo de vida de un servicio de TI (Garcia, 2015)

Se observa que la estrategia del servicio es la base del sistema. En cambio, el diseño, transición y operación del servicio operan en ciclo y la mejora continua proporciona soporte para el afinamiento de las otras etapas.

1.4.1.3 ITIL V3

En el 2007 se produce esta versión con 5 libros, detallados a continuación junto con los procesos que conlleva cada uno **(Cadavid, 2015)**:

a) **Estrategia del servicio**

   Estrategia del Servicio

   Administración Financiera

   Administración del Portafolio de Servicios

   Administración de la Demanda

b) **Diseño del servicio**

   Administración del Catálogo de Servicios

Administración de Niveles de Servicios

Administración de la Capacidad

Administración de la Disponibilidad

Administración de la Continuidad de los Servicios de TI

Administración de la Seguridad de la Información

Administración de Proveedores

c) Transición del Servicio

Planeación y Soporte en la Transición

Administración de Cambios

Administración de Activos de Servicio y de Configuraciones

Administración de Liberaciones e Implementación

Validación y Pruebas del Servicio

Evaluación

Administración del Conocimiento

d) Operación del Servicio

Administración de Eventos

Administración de Incidentes

Administración de Soluciones de Servicios

Administración de Problemas

Administración de Acceso Funciones

Centro de Servicio al Usuario

Administración Técnica

Administración de Operaciones de TI

Administración de Aplicaciones

e) Perfeccionamiento continuo del servicio

Mejora en Siete Pasos

Cada libro representa a una etapa de la que constan dentro del ciclo de vida del servicio según ITIL V3. La **grafica 5** demuestra el flujo en el ciclo de vida del servicio según ITIL V3.

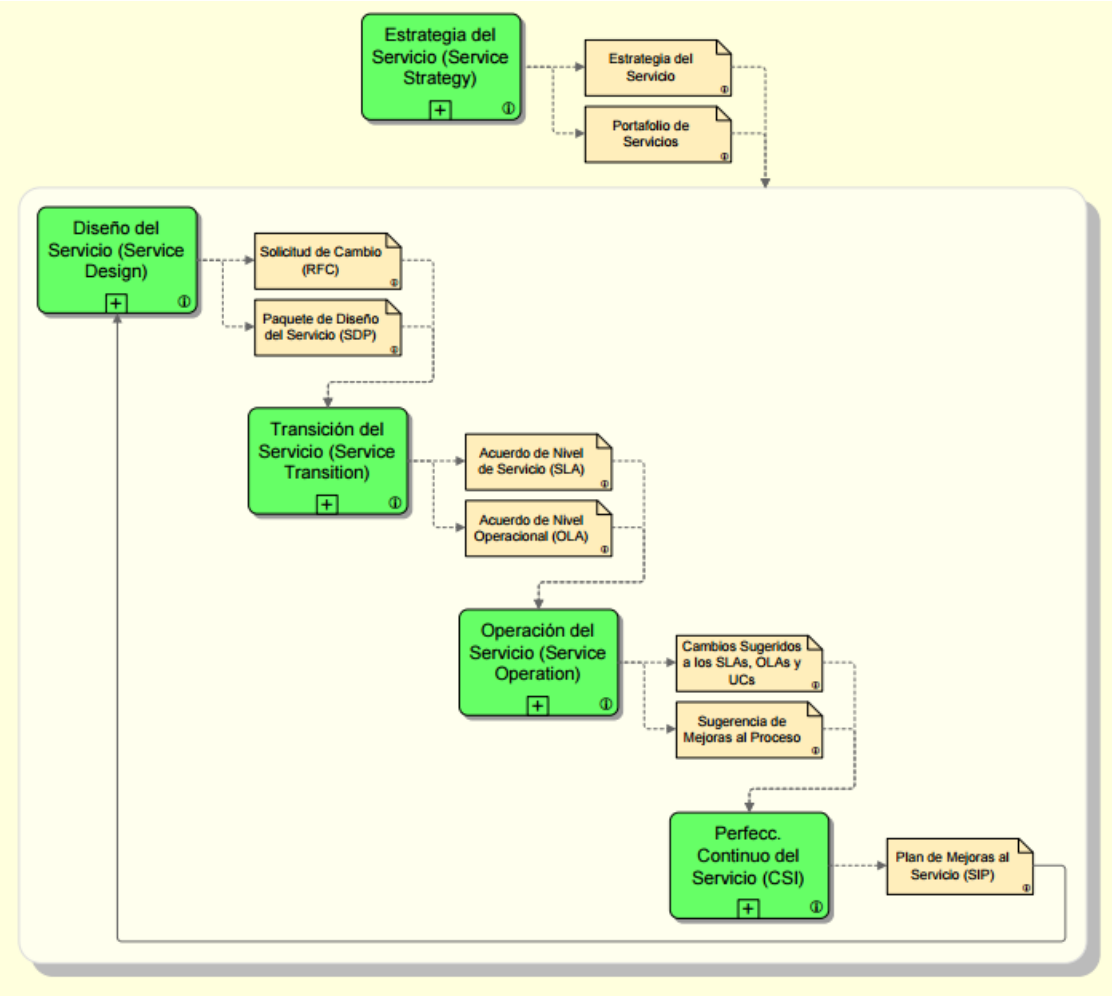


Gráfico 5. Ciclo de vida de servicio ITIL V3 (IT Process Maps GbR, 2010)

1.4.2 Norma ICREA

1.4.2.1 Concepto

Es un conjunto de recomendaciones y mejores prácticas concensadas entre varios países y un grupo de expertos en centros de procesamiento de datos que define la manera de construir un data center de acuerdo con los niveles de confiabilidad y seguridad deseados **(International Computer Room Experts Assotiation, 2013)**.

1.4.2.2 Objetivo

Según la Norma Internacional para la Construcción e Implementación de Equipamiento de Ambientes para Equipos de Manejo de Tecnologías de Información y Similares (ICREA-Std-131-2013) tiene como finalidad al diseñar un centro de procesamiento de datos (CPD):

> *"Proporcionar a los equipos de cómputo el ambiente adecuado para cumplir de la mejor manera las funciones para las que fue diseñado, y los requerimientos especificaciones de los fabricantes de Hardware así como cumplir con los requisitos de confiabilidad, eficiencia y sustentabilidad exigidos por la comunidad internacional."*

1.4.2.3 Consideraciones y administración de riesgos

En la definición de instalaciones que serían necesarias al construir una sala de cómputo, se debe realizar un análisis que califique las prioridades de riesgo a fin de proteger los equipos de cómputo; la información, las instalaciones de soporte y la vida del personal. Se debe realizar un análisis de riesgos que contemple los aspectos siguientes: el personal de operación, su entrenamiento, las normas de seguridad y construcción que aplican, los procedimientos utilizados para la conservación de equipos, las especificaciones de los fabricantes, procedimientos de recuperación en casos de daños en la infraestructura y la redundancia deseada (International Computer Room Experts Assotiation, 2013).

El nivel de riesgo es el resultado de la evaluación de amenazas y vulnerabilidades de una localización y sus ambientes de Datos y Hardware, menos las medidas de control adoptadas para su mitigación. Dado que el CPD y comunicaciones es el ambiente sobre el cual se basa la operativilidad de los sistemas de información, es preciso hacer un análisis de riesgos de origen físico-ambiental, para planificar un proceso de administración de los riesgos continuos. Los riesgos deben ser controlados, transferidos o asumidos, y para cada una de estas decisiones deberá contarse con documentación formal que asocie a cada riesgo con la decisión adoptada y con fundamentos probados por la alta dirección de cada organización (International Computer Room Experts Assotiation, 2013).

En cuanto a la metodología de análisis de riesgos e impacto, y tomando estos trabajos como conclusiones sobre las que indican el nivel de protección y redundancia de la infraestructura para los ambientes de TIC´s mínimos necesarios para la continuidad del negocio, se toma como referencia los criterios y glosario de términos y definiciones de la norma ISO 27001: "Tecnología De La Información- Técnicas De Seguridad- Sistemas De Gestión De Seguridad De La Información - Requisitos" (International Computer Room Experts Assotiation, 2013).

1.4.2.4 Equipos a considerar

Como afirma (International Computer Room Experts Assotiation, 2013), se debe considerar como equipos de cómputo, a todos los equipos electrónicos de proceso que estén conectados a una misma red de comunicación de datos que los equipos del Ambiente de Tecnologías de la Información. Estos equipos deberán tener una puesta a tierra común, tener una alimentación eléctrica de la misma calidad, y ser mantenidos dentro del mismo ambiente.

El ambiente podrá contar con diferentes niveles de protección conforme sea el impacto que su no disponibilidad o pérdida, pudiera ocasionar para la continuidad del negocio. Para esta determinación, deberán tomarse en consideración las conclusiones del análisis de riesgos más actualizado (International Computer Room Experts Assotiation, 2013).

1.4.2.5 Lugar para la instalación

Para la selección del lugar más adecuado en el que se instale el Ambiente de Tecnologías de la Información, se deberá solicitar el apoyo de un perito en la construcción de salas de cómputo. Se deberá evaluar el lugar desde el punto de vista seguridad, alimentación eléctrica, posibles problemas estructurales, EMC, vibraciones e inundaciones. El Ambiente de Tecnologías de la Información, deberá alojarse en un edificio construido con materiales no combustibles; tomando en cuenta los riesgos relacionados como terremotos, sismos, perimetral, colindancias, aspectos hidrológicos, estabilidad política, problemas sociales potenciales; zonas cercanas con centros recreativos, escuelas y universidades; supermercados, grandes almacenes, fabricas, gasolineras, aeropuertos, rutas de aterrizajes de

aviones, y cualquier otro que pudiera aportar una carga de combustible o un problema político-social (International Computer Room Experts Assotiation, 2013).

Esto es: se deberán utilizar materiales que faciliten la administración de riesgos del entorno de la localización y de sus accesos, deberán tomarse en consideraciones los límites de supervivencias recomendados en la normativa internacional respecto las protecciones contra incendios para los equipos de centro de cómputo, proporcionando ambientes que garanticen los límites de temperatura y humedad externa e interna que no pongan en riesgo la integridad de los activos informáticos (International Computer Room Experts Assotiation, 2013).

1.4.2.6 Proyectos a considerar

Los proyectos que deberán integrarse en la planeación de una sala de cómputo son:

- Arquitectónico,
- Obras civiles,
- Instalaciones eléctricas,
- Climatización y ventilación (HVAC - calefacción, ventilación y aire acondicionado por sus siglas en ingles),
- Ámbito,
- Infraestructura de comunicaciones,
- Seguridad,
- Gobernabilidad y sustentabilidad.

El ambiente de tecnologías de la información deberá colocarse en un lugar en donde se tenga una exposición mínima al fuego, a gases corrosivos, a calor, a humos, al agua y a la intervención humana ajena a estas instalaciones. Se deberá construir una barrera contra fuego en el perímetro de colindancia de la sala con otros departamentos, que incluya paredes, pasos de ductos, techos y pisos (International Computer Room Experts Assotiation, 2013).

El ambiente de tecnologías de la información deberá diseñar en base a los resultados del análisis de riesgos físico-ambientales que deben ser anexados a los proyectos, de los cuales surgen los niveles de protección acordes a los niveles de servicios a proveer a los clientes internos y externos de la organización. Así mismo, el proyecto y su documentación conforme a obra, determinará su contribución al diseño del Plan de Continuidad de las Operaciones; en particular para minimizar el plazo de Retorno a la Normalidad en caso de Contingencias (International Computer Room Experts Assotiation, 2013)**.**

1.4.2.7 Clasificación

Basándose en la disponibilidad esperada, la clasificación del ICREA para los CPD´s se define en niveles de donde se normarán las instalaciones de acuerdo con los siguientes criterios (International Computer Room Experts Assotiation, 2013)**.**

El termino N se utiliza para referirse al nivel de redundancia requerido para los diferentes elementos de la infraestructura indicándose en lo general la totalidad del requerimiento o sea el 100% de algo (International Computer Room Experts Assotiation, 2013)

- **Nivel I:** Sala de computo de Ambiente Certificado QADC (Quality Assurance Data Center). Esta topología aporta un 95% de disponibilidad y es una configuración básica con los siguientes requerimientos mínimos (International Computer Room Experts Assotiation, 2013)**:**

  Eléctricos:

  1.- UPS con capacidad N.

  2.- Trayectoria única (SVA).

  3.- Tablero general de distribución de energía ininterrumpida o PDU con transformador tipo K20.

Climatización:

1.- Capacidad de enfriamiento N.

2.- Equipo de climatización N.

3.- Circuitos hidráulicos N.

4.- Alimentación eléctrica a equipos SVA.

Seguridad:

1.- Un control de acceso previo al CPD y para de equipos de soporte, comunicaciones, NOC y SOC (área de control cero "AC-0").

2.- Sistemas contra fuego: extintores manuales.

3.- Protección balística nivel I del CPD.

Comunicaciones:

1.- Sin redundancia.

Ámbito:

1.- Techo y muros con resistencia al fuego F60.

- **Nivel II:** Sala de computo en ambiente Certificado de clase mundial WCQA (World Class Quality Assurance). Esta topología aporta un 99% de disponibilidad y es una configuración con redundancia básica (N+1) con requerimientos mínimos en el grupo electrógeno, UPS, PDU; sistema de climatización. Controles para monitoreo de la red y para seguridad de la infraestructura; sistema de contra fuego; cableado de comunicaciones con redundancia; construcción con resistencia sísmica y resistencia al fuego de 60 minutos expuesto a incendio. Hermético (International Computer Room Experts Assotiation, 2013)**.**

- **Nivel III:** Sala de computo confiable con ambiente certificado de clase mundial S-WCQA (Safety World Class Quality Assurance). Esta topología aporta un 99.9% de

disponibilidad y es una configuración con redundancia que permite darle mantenimiento sin suspender la operación. Puede contar con una acometida (N+1) o varias acometidas independientes y grupo electrógeno fijo sin redundancia. UPS y PDU con redundancia 2N. Además, la topología de red eléctrica debe permitir el mantenimiento sin suspender operaciones. Con respecto al sistema de climatización, debe estar en redundancia N+1 e inclusive se puede emplear elementos portátiles para mantenimiento sin interrumpir servicio. Deben tener tres controles de acceso, circuito cerrado de televisión y protección balística. Redundancia hasta el cableado de distribución principal. La construcción debe ser hermética, con resistencia antisísmica y resistencia al fuego por un periodo de 90 minutos para techo y paredes (International Computer Room Experts Assotiation, 2013).

- **Nivel IV:** sala de computo de alta seguridad con certificación HS-WCQA (High Security World Class Quality Assurance). Esta topología aporta un 99.99% de disponibilidad y es una configuración con redundancia sin puntos únicos de falla (PUF), que permite darle mantenimiento con elementos propios y fijos sin suspender la operación, con los siguientes requerimientos mínimos: una acometida (en mediana o alta tensión) y grupo electrógeno con redundancia 2N o varias acometidas independientes (de diferentes subestaciones), en mediana o alta tensión y grupo electrógeno con redundancia N+1. En cualquiera de los casos, se deberán instalar transformadores en redundancia 2N. Los grupos electrógenos deberán ser para uso exclusivo de CPD. NO se aceptaran grupos electrógenos portátiles. A más, del sistema de climatización con redundancia 2N, debe contar con detector automático de fugas de agua. Debe tener cuatro controles de acceso previo al CPD; sistema contra fuego centralizado y cruzada con extinción automática; circuito cerrado de televisión para el CPD y zona de equipos de soporte; protección balística. Redundancia hasta el cableado de acceso. La obra civil consta de techo y muros resistentes al fuego por 90 minutos expuesto durante incendio; hermético; construcción antisísmica; su ubicación depende del resultado de un análisis de riesgos previo (International Computer Room Experts Assotiation, 2013).

- **Nivel V:** Sala de computo de alta seguridad y alta disponibilidad con certificación de clase mundial HSHA-WCQA (High Security, High Available World Class Quality Assurance). Esta topología aporta un 99.999% de disponibilidad y es una configuración con redundancia sin puntos únicos de falla (PUF), que permite darle mantenimiento con elementos propios y fijos sin suspender la operación, tolerante a fallas con los siguientes requerimientos mínimos: dos o más acometidas independientes (de diferentes subestaciones) en mediana o alta tensión y grupo electrógenos con redundancia 2N. Se deberán instalar transformadores en redundancia 2N. Los grupos electrógenos deberán ser para uso exclusivo del CPD. NO se aceptaran grupos electrógenos portátiles. UPS con redundancia 2N con tres bancos de baterías independizables con capacidad del 50% cada banco; PDU´s con redundancia 2N; doble vía de alimentación (A y B); la topología deberá permitir dar mantenimiento a los grupos electrógenos sin suspender la operación; sistema automatizado de respuesta; compartimiento de elementos principales (transformadores, acometidas, grupos electrógenos, UPS´s, baterías de UPS´s, tableros generales, tanques de combustibles). Climatización: capacidad de enfriamiento 2N; equipo de climatización 3N; doble rama de distribución hidráulica principal; circuitos hidráulicos 2N; alimentación eléctrica a equipos DVA en generadores de agua helada; la topología deberá permitir dar mantenimiento a cualquier elemento del sistema sin necesidad de suspender la operación del CPD con elementos propios; detección automática de fugas de agua; enfriamiento continúo para densidades superiores**;** respuesta automática a fallos**;** compartimentación de instalaciones; climatizaciones en zona de UPS´s. Cinco controles de acceso previos al CPD**;** sistemas contra fuego: detección centralizada y cruzada con extinción automática; detección temprana; circuito cerrado de televisión del CPD y en zonas de equipos de soporte. Redundancia total de comunicaciones. Techo y muros con resistencia al fuego F90; hermético; construcción sólida y la ubicación del inmueble depende del análisis de riesgos (International Computer Room Experts Assotiation, 2013)**.**

1.4.3 ISO 27001: "Tecnología de Información- Técnicas de Seguridad- Sistema de Gestión de Seguridad de la Información- Requisitos"

1.4.3.1 Generalidades

Es una norma internacional emitida por la Organización Internacional de Normalización (ISO – siglas en ingles) y describe cómo gestionar la seguridad de la información en una institución (27001Academy, 2016).

Además puede ser implementada en cualquier tipo de organización. Está redactada por los mejores especialistas del mundo en el tema y proporciona una metodología para implementar la gestión de la seguridad de la información en una organización. También permite que una empresa sea certificada; esto significa que una entidad de certificación independiente confirma que la seguridad de la información ha sido implementada en esa organización en cumplimiento con la norma ISO 27001 (27001Academy, 2016).

1.4.3.2 Funcionamiento

Proteger la confiabilidad, integridad y disponibilidad de la información, es el eje principal de la norma. Su aplicación: es un proceso que debe identificar los problemas potenciales que afectarían a la información y luego, definir un plan donde se evite o mitigue los riesgos posibles (27001Academy, 2016).

1.4.3.3 Metodología de Evaluación de Riesgos y Tratamiento de Riesgos

Para cumplir con el objetivo de esta normativa es necesario el empleo de tres documentos detallados a continuación (27001Academy, 2016):

- Cuadro de Evaluación de Riesgos: se detalla los recursos, vulnerabilidades y amenazas a la que está expuesta la información; y evaluar los niveles de riesgo (27001Academy, 2016).

- Cuadro de Tratamiento de Riesgos: en él se determina las opciones para el tratamiento de riesgos y los controles adecuados para los riesgos no aceptables. Se puede escoger de entre 133 controles establecidos en la norma ISO 27001 (27001Academy, 2016).

- Informe Sobre Evaluación y Tratamiento De Riesgos: en este documento consta de un resumen detallado del proceso de los documentos utilizados durante la evaluación y el tratamiento de los riesgos de la información (27001Academy, 2016).

1.4.4 Estándar TIA-942

Ideada con la intención de unificar criterios en el diseño de áreas de tecnologías y comunicaciones brinda una serie de especificaciones para comunicaciones, cableado estructurado y lineamientos para los subsistemas de infraestructura dependiendo de la disponibilidad pretendida. (Espinoza, 2012).

De este estándar parte la clasificación Tiers para data center.

1.4.4.1 Clasificación de Data Center

Basándose en niveles de fiabilidad según la disponibilidad, el Uptime Institute inventa este sistema de clasificación **(Guilarte, 2013)** detallado a continuación:

- **Tier I**

Disponibilidad del 99,671% de servicios y parada al año de 28:83 horas. Se le llama así al centro de datos básico que puede o no puede tener suelos elevados, generadores auxiliares o UPS. El tiempo promedio para implementar es de 3 meses. No hay necesidad de componentes

redundantes en la distribución eléctrica y de refrigeración. Indica que al menos una vez al año debe estar fuera de servicio por motivos de mantenimiento. (Guilarte, 2013)**.**

- **Tier II**

Disponibilidad de 99,74% de servicios. Centros de datos redundantes. Es menos susceptible a interrupciones por actividades planeadas o no planeadas. Tiene suelos elevados, generadores auxiliares y UPS. Está conectada a una única línea de distribución eléctrica y de refrigeración. Por motivos de mantenimiento se debe hacer una interrupción de servicio. (Guilarte, 2013)

- **Tier III**

Disponibilidad de 99,982% de servicios. Centros de datos mantenimiento concurrentes. Permite planificar actividades de mantenimiento sin afectar al servicio de computación, pero eventos no planeados pueden causar paradas no planificadas. Consta de múltiples líneas de distribución eléctrica y de refrigeración, pero únicamente con una activa. Para implementar este tipo de data center puede llevarse de 15 a 20 meses. (Guilarte, 2013)

- **Tier IV**

Disponibilidad 100% de servicios. Son los centros de datos tolerantes a fallos. Permite planificar actividades de mantenimiento sin afectar al servicio de computación crítico y es capaz de soportar al menos un evento no planificado del tipo de peor escenario sin impacto crítico en la carga. (Guilarte, 2013)

1.4.4.2 Elementos de Data Center básico:

Dentro de los requerimientos mínimos constan los elementos detallados a continuación en la **tabla** 1:

INFRAESTRUCTURA Y GESTIÓN DE DATA CENTER	DESCRIPCIÓN	ANEXOS
Tablero principal	Es la caja metálica en donde deben estar instalada los breakers de protección de UPS, aire acondicionado de precisión, data center y luminarias.	**Ver anexo 1**
Tablero de by pass	Cumple con la función de transferir la carga de energía de UPS a energía normal de la empresa distribuidora de energía electricidad, con la finalidad de realizar mantenimiento, reparación y/o pruebas del UPS sin interrumpir el servicio eléctrico de los equipos protegidos.	**Ver anexo 2**
Red eléctrica data center	En esta sección se considera a las acometidas que se emplearía para la alimentación de energía para el data center y los planos de la red eléctrica.	**Ver anexo 3**
Generador eléctrico	Es un aparato que produce energía eléctrica a partir del empleo de energía mecánica. Para poder funcionar hace uso de combustible, puede ser gasolina o diésel. (Cummins, 2016)**.**	**Ver anexo 4**

Tablero de transferencia automática	Es un interruptor eléctrico que cambia una carga entre dos fuentes, son automáticas y pueden cambiar cuando detectan que una de las fuentes ha perdido o ganado poder. Un interruptor de transferencia automática se instala a menudo donde se encuentra un generador de respaldo, para que el generador puede proporcionar energía eléctrica temporal si la fuente de energía falla (Diesel Service Generation, 2015)**.**	**Ver anexo 5**
UPS	Es una fuente de suministro eléctrico que posee una batería con el fin de seguir dando energía a un dispositivo en caso de interrupción eléctrica. (ALEGSA, 2016)**.**	**Ver anexo 6**
Aire acondicionado de precisión	Es un equipo o sistema diseñado para acondicionar ambientes destinados a salas de cómputo, salas de informática, procesadores de datos, centros de cálculos, centrales telefónicas y otras aplicaciones de proceso en las que existía la necesidad fundamental de asegurar la operación y conversación de la máquina de proceso. (Mundo HVACR, 2014) **.**	**Ver anexo 7**
Piso falso	Es un sistema constituido por elementos modulares apoyados sin fijación en una estructura de soporte, para obtener bajo la superficie de transito un espacio intermedio para alojar servicios e instalaciones. (GUÍA DE SOLUCIOINES TIC, 2011)**.**	**Ver anexo 8**

Ventosa	Herramienta utilizada para elevar y movilizar los paneles del piso falso.	**Ver anexo 9**
Hermetización de pasos de cables	Es el empleo de cepillos de listón, dos campos de fibras de dos hileras que están colocados enfrentados. Esto permite mantener la el aire refrigerado fiablemente en el suelo técnico. (Mink Bursten, 2015)	**Ver anexo 10**
Malla de alta frecuencia	Malla hecha con láminas de cobre que se utiliza para asegurar el aterrizaje de las desviaciones de alta frecuencia, generados por los equipos eléctricos. (Rubio, 2012).	**Ver anexo 11**
Aterrizaje de los pedestales	Son abrazaderas de puesta a tierra para piso elevado. Es el punto de fijación entre los pedestales de piso elevado con la malla de alta frecuencia.	**Ver anexo 12**
Sistema de puesta a tierra	Es el conjunto de varillas de cobre que se deben ubicar en el suelo, luego del tratamiento químico para garantizar la conductividad y evitar la corrosión de las varillas.	**Ver anexo 13**
Pintura antiestática	Tiene como objetivo complementar la protección antiestática para los equipos electrónicos del data center.	**Ver anexo 14**
Cableado	Hace referencia a las normas internacionales empleadas para cableado estructurado.	**Ver anexo 15**
Puntos de cobre	Son los nodos o puntos que constituyen una red informática.	**Ver anexo 16**

Racks y accesorios	Se hace referencia a los elementos necesarios para la implementación de la red.	**Ver anexo 17**
Fibra óptica	Es un medio de transmisión físico capaz de brindar velocidades y distancias superiores a las de cualquier otro medio de trasmisión.	**Ver anexo 18**
Canalización y tuberías	Es el proceso que se emplea para cubrir el cableado con canaletas o tuberías destinadas para ese fin.	**Ver anexo 19**
Sistema de control de acceso	Es el conjunto de elementos que permitirán garantizar la seguridad a las instalaciones del data center.	**Ver anexo 20**
Sistema de gestión y monitoreo	Es un sistema que permite el monitoreo de la temperatura y humedad en el data center.	**Ver anexo 21**
Sistema de detección y extinción de incendios	Sistema que permite la detección y extinción de conato de incendio mediante la instalación de sistema inteligente.	**Ver anexo 22**
Sistema de video seguridad	Sistema que permite grabar todo lo que se realiza en el perímetro asignado.	**Ver anexo 23**
Puerta de seguridad	Es la puerta que da acceso directo al espacio del data center. Está hecha de acero y protegida contra robo. Además, también es protección en caso de incendio.	**Ver anexo 24**

Tabla 1. Elementos básicos de un data center.

CAPÍTULO II

2 DIAGNÓSTICO

2.1 Antecedentes Diagnósticos

Para toda institución la información es considerada uno de los activos más importantes para la realización de cualquier actividad, y por ello debe ser protegida bajo los estatutos necesarios que garanticen su seguridad.

Desde el año 2008, el crecimiento continuo en la demanda de servicios por parte de la comunidad universitaria ha traído como consecuencia un desarrollo e implementación de nuevas tecnologías de la información y de la comunicación. Por ello, la PUCESE ha implementado un Data Center y varios puntos de interconexión de la infraestructura antes mencionada.

El desarrollo ha incrementado la necesidad de contar con procesos estándares para la administración de estas tecnologías y la mitigación de los riesgos. Hoy en la PUCESE no se cuenta con estandarización de procesos que evidencian el uso de las mejores prácticas en el ámbito de las TIC’s.

Para obtener la información y cumplir con el procedimiento del diagnóstico, se efectuaron técnicas como: entrevistas al Jefe del departamento de TIC's, al responsable del Data Center y encargados de las áreas de Soporte Técnico, Desarrollo de Software y Redes; además de encuestas realizadas a los usuarios de los servicios web sobre todos de aquellos sistemas críticos como son Web Administrativos y Web Docentes mismas que se detallan más adelante.

2.2 Objetivos Diagnósticos

Se plantean 3 objetivos diagnósticos que permiten conocer la situación actual del data center de la PUCESE:

1. Identificar los recursos tecnológicos disponibles en el data center de la PUCESE.
2. Determinar la calidad del servicio que brinda los servidores del centro de datos.
3. Identificar la gestión administrativa del data center de la PUCESE.

2.3 Variables Diagnósticas

- **Recursos del centro de datos:** son los recursos físicos y hardware que cuenta el data center de la PUCESE. Además también se considera los elementos que brinden seguridad a la infraestructura.
- **Servicios de TI:** las aplicaciones o software que brindan servicios a los departamentos PUCESE.
- **Organización de TI:** son los procesos que se cumplen el departamento de TIC's.

2.4 Indicadores Diagnósticos

- Recursos de centro de datos
    - ✓ Cumplimiento de normas
    - ✓ Vulnerabilidades
    - ✓ Redes
    - ✓ Hardware
- Servicios de TI
    - ✓ Tipo de servicio
    - ✓ Disponibilidad
    - ✓ Satisfacción

- Organización de TI
    - ✓ Estructura organizacional
    - ✓ Planes
    - ✓ Procesos

2.5 Matriz de relación

OBJETIVOS DIAGNÓSTICOS	VARIABLES	INDICADORES	TÉCNICAS	FUENTES DE INFORMACIÓN
Identificar los recursos tecnológicos disponibles en el data center de la PUCESE.	Recursos de Centro de Datos	✓ Ambiente Físico ✓ Incidentes ✓ Responsabilidad	Entrevista	Encargados de las áreas de TIC´s (Redes, soporte técnico y desarrollo de software)
		✓ Estándares ✓ Seguridad ✓ Ambiente físico	Entrevista	Responsable del Data Center
Determinar la calidad del servicio que brinda los servidores del centro de datos.	Servicios de TI	✓ Tipo de servicio ✓ Disponibilidad ✓ Satisfacción ✓ Percepción de la seguridad de la información ✓ Calidad	Encuesta	Usuarios de los servicios del Data Center
Identificar la gestión administrativa del data center de la PUCESE.	Organización de TI	✓ Estructura organizacional ✓ Planes ✓ Procesos	Entrevista	Jefe del departamento de TIC

Tabla 2. Matriz Diagnóstico.

2.6 Mecánica operativa

2.6.1 Población y Muestra

Para la realización de este proyecto se trabajó con la población integrada por las personas que utilizan los servicios web de la PUCESE (PUCESE, 2016): personal administrativo 70 y 170 docentes; datos proporcionados por el departamento de Recursos Humanos. Esta población cuenta con 240 personas. Para el cálculo de la muestra del proyecto se utilizará el tipo de muestreo PROBABILÍSTICO, cuya fórmula es:

$$\textbf{1.}\quad \mathrm{n} = \frac{\mathrm{N} * \delta^2 * Z^2}{(\mathrm{N}-1)E^2 + \delta^2 * Z^2}$$

Dónde:

$\boldsymbol{N}$ = Tamaño de la población → 240 personas

$\boldsymbol{E}$ = Error admisible → 0.08

$\boldsymbol{\delta}$ = Varianza → 0.25

$\boldsymbol{Z}$ = Nivel de confianza → 1.96

$\boldsymbol{n}$ = Tamaño de la muestra → ?

$$\textbf{2.}\quad \mathrm{n} = \frac{240 * 0.25 * (1.96)^2}{(240-1)0.08^2 + 0.25 * (1.96)^2}$$

3. $\mathrm{n} = 92.568$ → Tamaño de la muestra = 93 personas

2.6.2 Información Primaria

Para la presente investigación se aplicaron dos tipos de técnicas de investigación, la cuales son:

Entrevista

Se realizaron entrevistas dirigidas al Jefe del Departamento de TIC's el dia 5 de mayo del 2016 con el propósito de obtener información relacionada con la gestión administrativa del Data Center; en la misma fecha al Responsable del Data Center y a los Encargado de la área Redes y Comunicación; en la fecha del 6 de mayo del año en curso se entrevistó a el responsable del área de Desarrollo de Software y al encargado de Soporte Técnico del Departamento de TIC´s de la PUCESE, con la intention de conocer de incidentes con respecto a sus responsabilidades en el Data Center. **Ver anexos 25, 26, 27, 28 y 29.**

Encuesta

Se desarrollaron encuestas a docentes y personal administrativo en los días 11 y 12 de mayo del 2016. Estas personas utilizan a diario los servicios web que proporciona el Data Center de la PUCESE en la realización de sus actividades en el sistema: registro de notas, actividades administrativas y más. La encuesta se hizo con el propósito de determinar la calidad del servicio que brinda los servidores del centro de datos. **Ver anexo 30.**

2.7 Información Secundaria

En el presente trabajo se han investigado documentos de los siguientes tipos: Artículos científicos, proyectos de tesis e información en la web, con información referente a lineamientos a seguir para la gestión de riesgos de TI y centros de cómputo.

2.8 Tabulación y análisis de Información

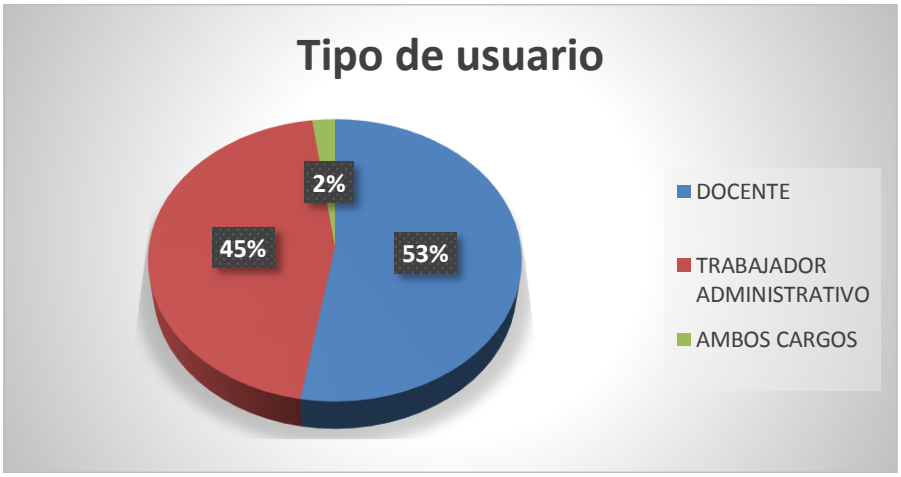
2.8.1 Encuesta

Esta parte de los instrumentos está formada por un cuestionario de 6 preguntas, dirigidas a los usuarios de los servicios web de la PUCESE (Docentes, Trabajadores), con el propósito de determinar el grado de satisfacción de los servicios web.

2.8.1.1 Encuesta dirigida a los usuarios de los servicios web.

PREGUNTA 1: ¿Qué tipo de usuario es?

Tabulación:



Grafica 6. Tipo de usuarios de los servicios web
Fuente: Propia del autor

Análisis:

En la gráfica se observa que la mayoría de los encuestados que se benefician de los servicios que provee el data center de la PUCESE son los docentes con el 53%, frente a la diferencia de 45% perteneciente a los trabajadores administrativos. Existe una pequeña cifra del 2% de los encuestados que cumplen ambos cargos, es decir, son docentes y personal administrativo.

PREGUNTA 2: ¿Cuán satisfecho está Ud. con el servicio de red que ofrece la PUCESE?

Tabulación:

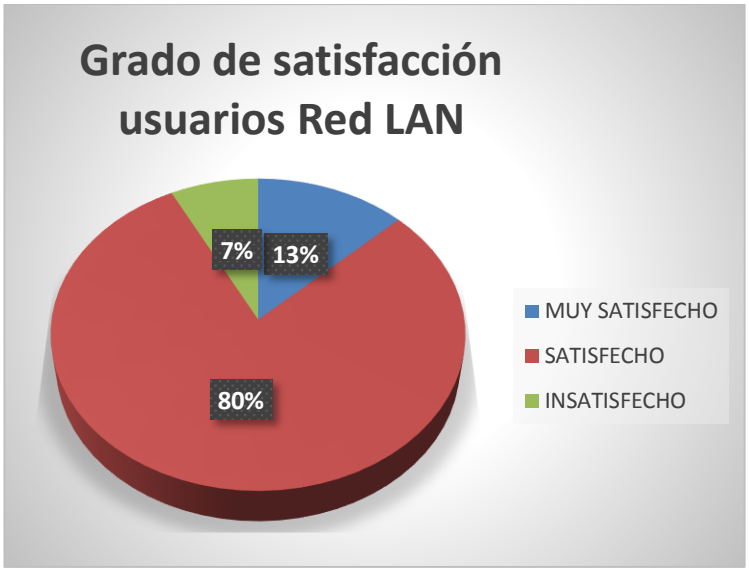


Gráfico 7. Grado de satisfacción del servicio de Red LAN
Fuente: Propia del autor

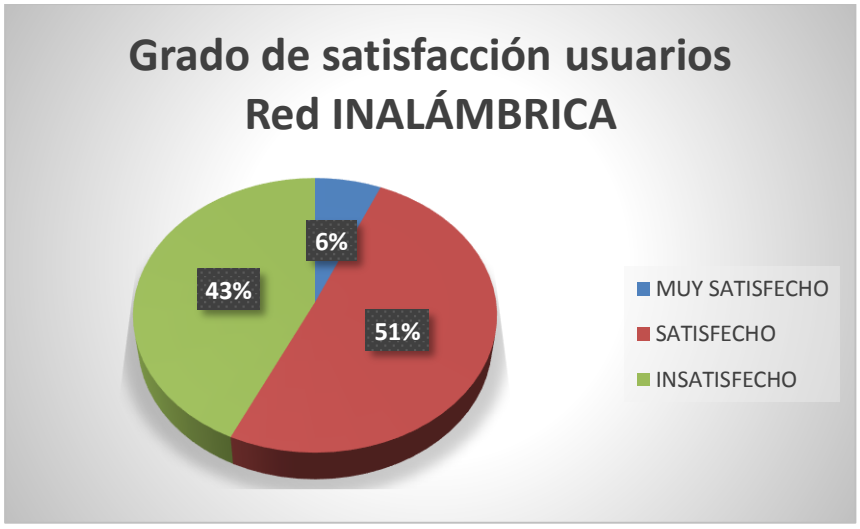


Gráfico 8. Grado de satisfacción de la Red INALÁMBRICA
Fuente: Propia del autor

Análisis:

Estos resultados dan la conclusión que la red LAN cumple con los parámetros solicitados para su buena operación y la red INALÁMBRICA presenta inconvenientes al momento de ser empleada.

PREGUNTA 3: Si usa los servicios web que brinda la PUCESE, por favor indique cuál de la lista a continuación:

Tabulación:

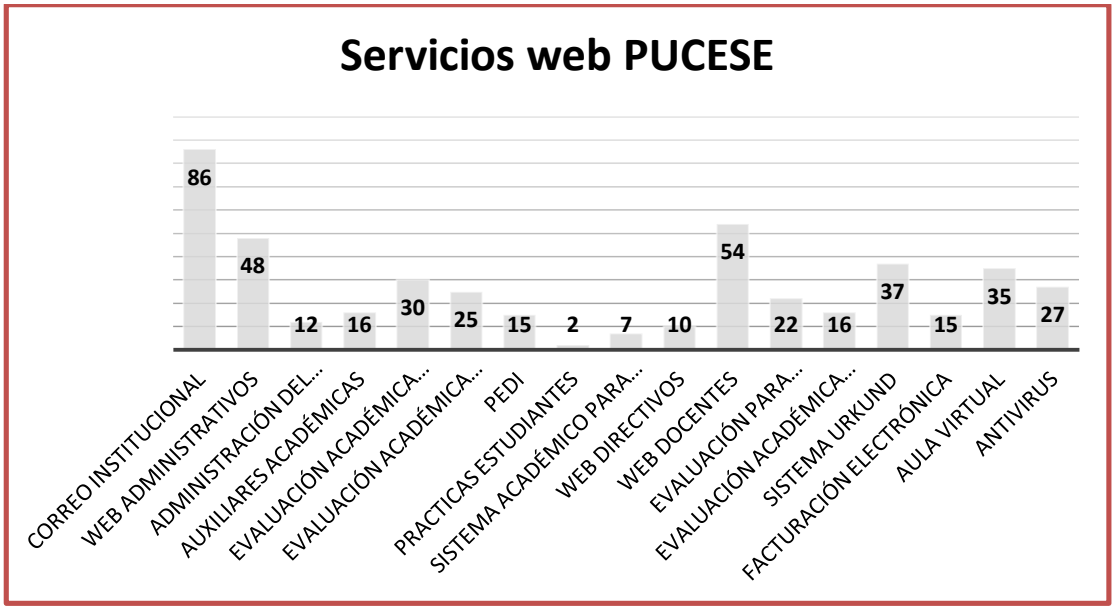


Gráfico 9. Servicios web que provee la PUCESE a sus usuarios
Fuente: Propia del autor

Análisis:

Entre los servicios más utilizados por los encuestados y que son provistos por el data center de la PUCESE esta Web Docente y Web Administrativos que son los sistemas considerados como críticos en la institución debido a la naturaleza de la información que se maneja en ellos.

PREGUNTA 4: ¿De los servicios web que usted utiliza, cuánta información cree se ha perdido?

Tabulación:

Gráfico 10. Percepción sobre la pérdida de información
Fuente: propia del investigador

Análisis:

La mayoría de los usuarios encuestados dice sentirse desconfiados de la protección de su información, aunque, existe una considerable cantidad de usuarios que indica lo contrario, se puede mencionar que el data center no cumple con parte de los requisitos de seguridad de la información exigidos para su operatividad.

PREGUNTA 5: Los servicios web están disponibles:

Tabulación:

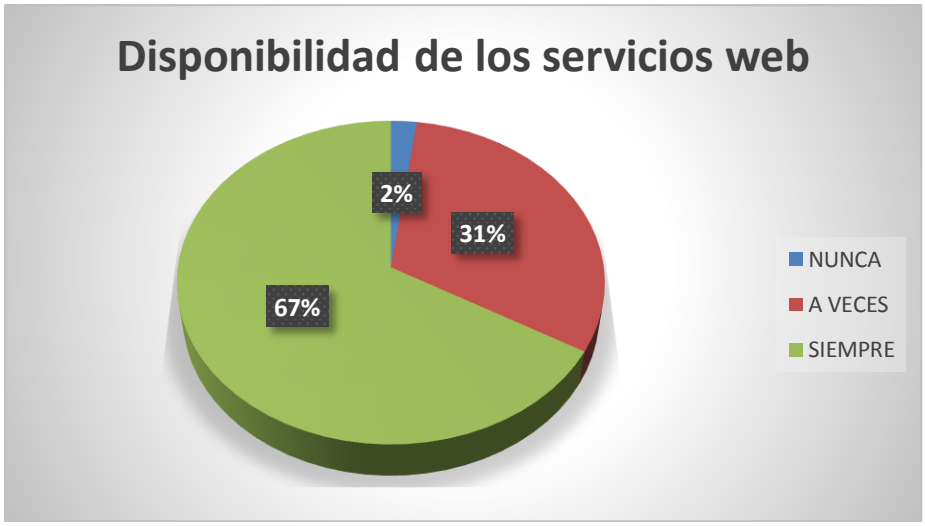


Gráfico 11. Disponibilidad de los servicios web
Fuente: propia del investigador

Análisis:

Esto refleja que la mayoría de usuarios no presentan mayores inconvenientes para disponer de los servicios web. Aunque, la función del data center es de mantener la disponibilidad de servicios siempre, la realidad es diferente tomando en cuenta la considerable cantidad de encuestados que no puede acceder a los servicios.

PREGUNTA 6: ¿La información que provee a los servicios web cree usted que se encuentra protegida?

Tabulación:

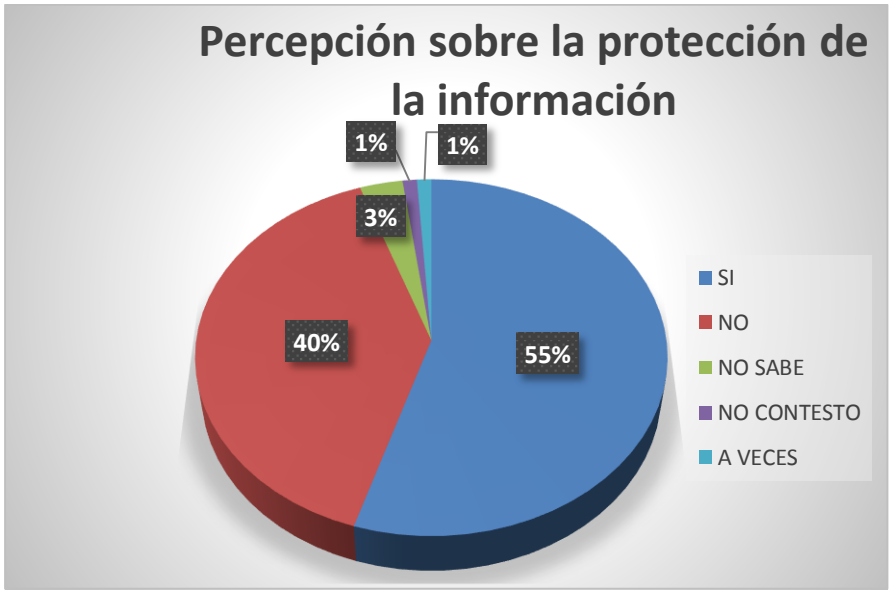


Gráfico 12. Percepción de los usuarios sobre la protección de su información
Fuente: Propia del autor

Análisis:

Existe una buena cantidad de usuarios insatisfechos, aunque la mayoría de población encuestada cuenta con la confianza que su información si está segura el data center debe hacer revisión en sus políticas de protección y aplicarlas.

2.8.2 Entrevistas

Entrevista realizada al Jefe del Departamento de TIC's: Lcdo. Marc Grob, Msc. **Ver anexo 25.**

Pregunta 1: ¿Cómo está estructurado el departamento?

Respuesta: Al momento, el departamento está estructurado en tres áreas: uno que abarca Soporte y Mantenimiento; Desarrollo y Administración de base de datos; Redes e Infraestructura en general. Son las tres áreas que tenemos por el momento.

Pregunta 2: Por favor indique los nombres de cada uno de los encargados de las áreas.

Respuesta: José Manuel Bernal es del área de Soporte, Kléber Posligua es de Desarrollo y Jhonny Quiñónez es parte de Redes e Infraestructura.

Pregunta 3: ¿Qué procesos administrativos se deben seguir en el departamento relacionados con el Data Center?

Respuesta: Es una muy buena pregunta. Se debería tener un plan de manejo en general de cómo se trata un Data Center. Debe existir un listado de qué actividades se hacen adentro y qué actividades se hacen afuera. Necesitamos una planificación de mantenimiento, cada cuánto se debe hacer el mantenimiento, se necesita también una planificación de respaldo de servidores de servicios que necesitan ser periódicamente respaldados, deberíamos tener un control de seguridad informática revisando los firewalls y locks, entre otros de manera constante. Estos son los procesos que deberían existir. Hay que definir primero los procesos porque no están formalmente delineados. Hay unos procesos definidos pero nunca se los aprobó y desconozco la razón de por qué no se ratificaron esos procesos.

Pregunta 4: ¿El departamento cuenta con un plan estratégico de TI?

Respuesta: No he visto un plan estratégico. Existe un plan estratégico de la universidad donde se estipulan cuatro puntos relacionados con el Departamento de Sistemas; pero en si para la estrategia del departamento y de la evolución de informática no existe.

Pregunta 5: ¿Se cuenta con un plan operativo?

Respuesta: No tenemos planes operativos. Hay ciertos roles y funcionarios definidos pero no existe una planificación.

Análisis

El Departamento de TIC's se encuentra estructurado de tal manera que hace frente a tres áreas críticas en la institución con respecto a tecnologías de la información pero no cuenta con un plan operativo en el que se marque de manera severa los procedimientos a seguir en cada área. A pesar de ello, el jefe del departamento cuenta con mucha predisposición para realizar las definiciones de procesos necesarios y establecimiento de estrategias para la correcta operación de funciones en la dependencia a su cargo, penosamente no se cuenta con procesos administrativos relacionados con el data center.

Entrevista realizada al Responsable del Data Center: Ing. Jhonny Quiñónez. **Ver anexo 2.**

Pregunta 1: ¿El ambiente del cuarto de telecomunicaciones cuenta con un ambiente físico apropiado para su buen funcionamiento?

Respuesta: La Universidad Católica en busca de proveer a los usuarios un buen servicio, ha hecho el esfuerzo para poder instalar un data center que tenga las condiciones mínimas para su funcionamiento. En este momento, contamos con un cuarto que tiene un aire acondicionado que se mantiene a 21°C, tenemos un piso falso para aislamiento del cableado estructurado que va por debajo del piso falso, tenemos unas conexiones a tierra, tenemos las protecciones eléctricas necesarias como es un TBSS, contamos con un respaldo de energía que nos ha dado un almacenamiento con capacidad para unas 8 horas de operación. Además de eso, tenemos una cámara de video vigilancia por la seguridad y consta una puerta con acceso tipo biométrico para que solo el personal apropiado pueda acceder a los equipos.

Pregunta 2: ¿Cuántas personas se encuentran registrados para ingresar al data center?

Respuesta: Solamente cinco personas registradas para el acceso a data center:

1. Jefe de desarrollo
2. Jefe de soporte
3. Técnico de desarrollo
4. Técnico de soporte
5. Mi persona (Johnny Quiñónez)

Pregunta 3: ¿Se cumple con las normas o estándares en el data center de la PUCESE?
Respuesta: Se ha tratado de cumplir con la mayor cantidad de requerimientos posibles al momento de la instalación del cableado estructurado, tanto de los equipos y de los servicios, para ello hemos hecho relevancia de estándares como son la ISO (sobre todo para cableado estructurado) y para los servicios se está empezando a estructurar orientados a ITIL para los procesos.
Pregunta 4: ¿Cómo se podría mejorar la situación actual del Data center en la PUCESE?
Respuesta: Como se había mencionado el data center está en vías de desarrollo, tenemos algunas implementaciones que se quiere hacer, por ejemplo, el monitoreo totalmente digital para que desde la parte externa del data center nosotros podemos ver cuál es la condición de funcionamiento y rendimiento de los equipos que están operando ahí adentro. Tenemos intención de comprar una consola KVM (Keyboard Video Mouse) que nos permitirá acceder vía remota con las seguridades debidas hacia los diferentes servidores. Estamos con algunos proyectos con respecto al crecimiento de equipos en cuanto a la tecnología y prestaciones de servicios en los servidores.
Pregunta 5: ¿En el plan de tratamiento de riesgo se ha contemplado al Data Center?
Respuesta: A decir verdad, el departamento de TIC´s no tiene un plan de contingencia en el cual se contemplen los riesgos que se corren con los activos de información. Estamos preocupados y justamente si existiera un estudio que descubra las debilidades que se tiene para poderlas tratar, sería bienvenida.

Análisis

De la entrevista otorgada por el responsable de la infraestructura tecnológica se puede considerar que el data center cuenta con cableado estructurado que cumple normas establecidas por la ISO y en el ámbito físico se encuentra parcialmente funcional. El ingeniero menciona proyectos a cumplir para mejorar la administración de su dependencia y la predisposición de aceptar colaboración en la gestión.

Entrevista realizada al Encargado del área de Redes y Comunicaciones: Ing. Jhonny Quiñónez, **ver anexo 3**.

Pregunta 1: ¿El Data Center con qué sistemas cuenta?

Respuesta: Ahora solo se tiene el sistema de climatización, el sistema de aislamiento, el sistema de backup de energía y el acceso biométrico que no supone una bitácora, pero si es solo para activar el ingreso.

Pregunta 2: ¿De los recursos tecnológicos de su área que se encuentran en el Data Center han sufrido algún inconveniente en su funcionamiento?

Respuesta: Hemos tenido inconvenientes con sistema de climatización. El aire acondicionado a veces ha dejado de funcionar y se ha encontrado con gran cantidad de calor en el cuarto de comunicaciones lo que perjudica notablemente a los servicios y por ende a los equipos.

Pregunta 3: ¿Se tiene algún nivel de seguridad para el acceso?

Respuesta: Claro. El único nivel de seguridad es el biométrico. Tiene una chapa eléctrica especializada que tiene una cierta resistencia de presión y que solamente se activa bajo el requerimiento de la huella digital de las personas que están registradas.

Pregunta 4: ¿Para qué actividades del Data center la PUCESE ha contratado a terceros?

Respuesta: Hemos contratado a terceros para la instalación del piso falso, para instalación del sistema del ambiente, para el sistema de cableado estructurado e inclusive para el sistema eléctrico lo que se refiere a la protección, banco de baterías y el UPS como tal.

Análisis:

El encargado del área de Redes y Comunicaciones menciona que el Data Center se encuentra con el equipamiento básico y la seguridad necesaria brindada por el sistema biométrico empleado. Además, hace notar su preocupación por el sistema de climatización que ha presentado inconvenientes poniendo en riesgo al equipamiento.

Entrevista realizada al Encargado del área de Desarrollo de Software: Ing. Kléber Posligua,**ver anexo 4** .

Pregunta 1: ¿El Data Center con qué sistemas cuenta?

Respuesta: En realidad no soy la persona que podría dar el dato confiable. El responsable de esa área es Jhonny Quiñonez. De lo que conozco, sé que no tiene sistema de climatización, no tiene sistema contra incendios. No tiene esas cosas esenciales.

Pregunta 2: ¿De los recursos tecnológicos de su área que se encuentran en el Data Center han sufrido algún inconveniente en su funcionamiento?

Respuesta: No. Mientras ha existido el data center ha tenido un funcionamiento normal; salvo casos en los que la energía se ha ido más de 10 horas, aunque el soporte del data center es de unas 10 horas más o menos, es decir que soporta. Pero cuando hubo paros de energía largos, ahí si se apagaron los equipos. De ahí, el funcionamiento de los servidores es normal, de la base de datos es normal, de los sistemas que estas a disposición de los usuarios ha sido óptimo.

Pregunta 3: ¿Se tiene algún nivel de seguridad para el acceso?

Respuesta: El único nivel de seguridad que hay es de usar una puerta de acceso física con un control electrónico digital que nos permite ingresar a determinadas personas. En este caso los responsables o los que tenemos acceso somos Jhonny Quiñonez, Jose Manuel Bernal y mi persona (Kléber Posligua), hasta donde tengo conocimiento. Mediante la lectura de la huella digital a través de un dispositivo electrónico nos da acceso a aquellos usuarios que previamente fuimos registrados por el administrador que es Jhonny Quiñonez.

Pregunta 4: ¿Para qué actividades del Data center la PUCESE ha contratado a terceros?

Respuesta: Se ha contratado a terceros para mantenimiento del UPS, para ponerlo en buen estado, el funcionamiento, para chequearlo; para poner allí un sistema de almacenamiento masivo como es My Cloud y uno nuevo que se ha contratado Synology.

Análisis

El encargado de Desarrollo de Software menciona que falta los sistemas necesarios para la correcta administración del data center. A pesar de ello, cuando surgieron inconvenientes como la falta de energía se pudo seguir adelante con las funciones y los

equipos a su cargo sin problemas. En vista de la necesidad de actualización de tecnología en la institución, se hizo adquisiciones y el respectivo asesoramiento sobre ellas.

Entrevista realizada al Encargado del área de Soporte Técnico: Ing. José Manuel Bernal, **ver anexo 5**

Pregunta 1: ¿El Data Center con qué sistemas cuenta?
Respuesta: En la actualidad, el data center se encuentra en un proceso de creación y todavía no está terminado. Según los expertos, dicen que está en un 70%. Creo que le hacen falta algunas cosas como el sistema contra incendio, sistema de ventilación automatizado, sistema de congelación; es decir, el único sistema con el que cuenta es de acceso que es huella digital, nada más.
Pregunta 2: ¿De los recursos tecnológicos de su área que se encuentran en el Data Center han sufrido algún inconveniente en su funcionamiento?
Respuesta: En el data center, bajo mi cargo hay tres equipos: un servidor para los estudiantes, un servidor para la parte administrativa que es el de Active Directory y un equipo My Cloud que es donde almacenamos todo los instaladores. El equipo de los estudiantes se reinició un par de veces por lo que los docentes no pudieron acceder, pero, normalmente funcionan todos bien.
Pregunta 3: ¿Por qué se dio esa eventualidad del reinicio del equipo de los estudiantes?
Respuesta: Hubo un problema con la tarjeta de red que causó un cortocircuito y se reinició. No fue un problema exactamente del data center sino del equipo como tal.
Pregunta 4: ¿Se tiene algún nivel de seguridad para el acceso?
Respuesta: Para entrar al data center primero debe pasar por la oficina de Sistemas, ahí contamos con una cámara de seguridad. Luego, en el data center está el sistema de huella que solo tiene acceso cinco personas, que somos los que trabajamos en el área de Sistemas y dentro del data center tenemos una cámara de seguridad que monitorea todos los cambios y todas las cosas que realizamos.
Pregunta 5: ¿Para qué actividades del Data center la PUCESE ha contratado a terceros?
Respuesta: Cuando empezamos la construcción del data center se contrató una empresa de Quito especializada en data center que fue la encargada de hacer le piso falso, luego para el sistema biométrico o el sistema de huella y para el aire acondicionado se ha contratado a terceros. Todas las conexiones y las puestas de las racks, switch y patch

panel lo hicimos aquí en la universidad. El encargado de esta tarea fue el Ing. Jhonny Quiñonez.

Análisis

El entrevistado considera que el data center le hace falta elementos importantes teniendo en cuenta que no se encuentra concluido en su totalidad. Los equipos servidores a su cargo operan dentro del parámetro normal; a pesar de eventualidades. Hace notar su conocimiento con respecto a la herramienta que brinda seguridad al data center y monitorea cada actividad en el mismo. Además indica la colaboración de terceros, mediante contratación, para la implementación de la infraestructura tecnológica y la instalación de la red bajo la directriz del Ing. Jhonny Quiñonez.

2.9 FODA Aplicada A Los Servicios Web De La Página De La PUCESE Y Data Center PUCESE

Fortalezas:

F1: Cumplimiento de estándar ISO para el cableado estructurado.

F2: Estructura organizacional del departamento de TI definida.

F3: Disponibilidad de los servicios web.

Oportunidades:

O1: Metodología de gestión de riesgos tecnológico.

O2: Existencia de estándares para la administración del data center.

O3: Empresas asesoras para implementación del data center.

O4: Certificaciones internacionales.

Debilidades:

D1: Ambiente físico implemento del data center.

D2: Falta personal especializado en Seguridad Informática y Riesgos de TI.

D3: No hay plan de tratamiento de riesgo del data center.

D4: Falta de seguridad.

Amenazas:

A1: Falta de credibilidad sobre la protección brindada a la información.

A2: Ataques informáticos.

A3: Falla de energía eléctrica de manera repentina.

2.10 Estrategias FA, FO, DO, DA

	AMENAZAS	OPORTUNIDADES
FORTALEZAS	• Asignar un responsable de la administración de riesgos. **(F2, A1, A2)** • Implementar medidas preventivas para que la disponibilidad de servicios no sea afectada por fallas de energía eléctrica. **(F3, A3)**	• Evaluar el estado del data center con respecto a los estándares. **(F2, O2)** • Acceder a certificaciones internacionales para mejorar la administración del data center. **(F2, O4)**
DEBILIDADES	• Aplicación de metodología de Gestión de Riesgos Tecnológicos **(D1, D4, A2, A3)** • Establecer protocolos de seguridad de la información para hacer frente a ataques informáticos. **(D4, A2)**	• Recibir asesoría para implementar en su totalidad al data center del equipamiento necesario. **(O3,D1)**

Tabla 3. Matriz FODA
Fuente: propia del investigador

2.11 Determinación del problema Diagnóstico

Una vez concluido el estudio de la situación actual del Data Center de la PUCESE, se determina que la infraestructura y los servicios no son suficientes al hacer frente a los riesgos que está atravesando. No hay personal asignado para la mitigación de los riesgos y no hay procedimientos relacionados con el Data Center. Las eventualidades suscitadas descritas por el personal en las entrevistas evidencian la necesidad implementar medidas para contrarrestar a los riesgos.

CAPÍTULO III

3 PROPUESTA: GESTIÓN DE RIESGOS DEL DATA CENTER DE LA PUCESE HACIENDO USO DE LA NORMA ICREA STD-131-2013 E ISO/IEC 27001

3.1 Antecedentes

La Pontificia Universidad Católica del Ecuador Sede Esmeraldas (PUCESE) cuenta con un data center que opera con un rendimiento bajo debido a las carencias que tiene con respecto a la seguridad de infraestructura tecnológica. El centro de procesamiento de datos fue construido sin los requerimientos básicos e incluso se puede considerar incompleto. Además, no brinda la seguridad mínima para mantener la información a salvo ante una grave eventualidad debido a la falta de un plan de tratamiento de riesgo. Por eso, se presenta la propuesta de gestión de riesgos aplicando ICREA Std-131-2013 e ISO/IEC 27001.

3.2 Objetivos de propuesta

1. Identificar los procesos relacionados con el data center.
2. Evaluar la infraestructura y los procesos del data center.
3. Implementación de una metodología de Gestión de Riesgos.

3.3 Alcance

Se realizó el proceso de auditoría a la infraestructura de data center de la Pontificia Universidad Católica del Ecuador Sede Esmeraldas del 30 de mayo del 2016 al 17 de junio del 2016. La responsabilidad asumida al momento de la inspección es de emitir un criterio con respecto a los controles del data center, basándose en el desarrollo de esta propuesta.

El proceso de análisis de riesgo fue efectuada de acuerdo a las normas ICREA Std-131-2013 e ISO 27001. Estas normas requieren que se planifique y se realice el trabajo con el objetivo de lograr un razonable grado de seguridad. El proceso comprende una inspección del espacio del data center considerando, recabar pruebas de las observaciones, evaluar los procedimientos de control usados y políticas. Se considera que las pruebas y procedimiento seguido constituya una base aceptable para fundamentar las conclusiones obtenidas.

3.4 Evaluación de riesgos

3.4.1 El proceso

La evaluación de riesgos se implementa a través del cuadro de evaluación de riesgos. El proceso de evaluación de riesgos se lo realizó identificando las amenazas y vulnerabilidades. Seguido, la evaluación de consecuencias y probabilidades. Parte del procedimiento de mitigación es la aceptación de riesgos apoyándose en una escala que califica de 1 a 5 siendo 1 considerado insignificante y 5 como catastrófico. Una vez identificados los riesgos se elabora el plan de tratamiento.

3.4.2 Activos, vulnerabilidades y amenazas

El primer paso en la evaluación de riesgos es la identificación de todos los activos dentro del alcance del Sistema de Gestión de Seguridad de Información; es decir todos los activos que pueden afectar la confidencialidad, integridad y disponibilidad de la información en la organización. Se hizo uso de la Norma ICREA Std-131-2013 para elaborar un listado considerando todos los aspectos de Data Center: eléctrico, climatización, seguridad, cableado estructurado y obra civil. Se realizó un cuadro que contiene a cada ítem que plantea cada requerimiento de la norma para un data center de Nivel I.

En la **tabla 4** se expresa en porcentaje los requerimientos cubiertos por el data center de la PUCESE según el Nivel I de la Norma ICREA Std-131-2013. Con respecto a la sustentabilidad presenta un porcentaje bajo 16,67%; proporciones nulas del aire acondicionado y seguridad (0%); y en instalaciones eléctricas 72,73 %, comunicaciones 66,72% y obra civil 70 %. Con esta información se demuestra que el data center no cuenta con las especificaciones mínimas para operar con total seguridad para garantizar la continuidad de los servicios, es decir, no puede hacer frente a los riesgos inherentes que tiene un data center.

Ítems	**Cumplimiento**	
	SI	**NO**
Instalaciones Eléctricas		
Energía eléctrica con alimentadores independientes de otras cargas		X
Sistemas de puesta a tierra aislada	X	
Sistemas de puestas a tierra de seguridad	X	
Interconexión entre los diferentes sistemas de puesta a tierra	X	
Supresión de transistorios de sobre tensiones en zonas de tableros de distribución y PDUs	X	
Protección contra descargas atmosféricas		X
Sistemas de energía ininterrumpible que soporte el 120 % de la carga existente, mas un 30 % para crecimiento	X	
Circuitos derivados de energía ininterrumpible	X	
No mas de cinco dispositivos por circuito		X
Toma corrientes con sistemas de puesta a tierra aislada	X	
Cables de sistema eléctrico identificados en ambos extremos	X	
Resultado (%)	72,73	27,27
Sistema de Aire Acondicionado		
Aire acondicionado de precisión independiente de otras cargas.		X
Resultado (%)	0	100
Instalaciones de Seguridad		
Detección y extinción sencilla de conato de incendio dentro del data center		X
Resultado (%)	0	100
Instalaciones de Comunicaciones		
Conexiones entre equipos por medio de Cableado estructurado de par trenzado y/o fibra óptica.	X	
No debe haber conexiones entre gabinetes excepto aquellos que tengan paso directo para cables	X	
Al menos una interfaz de red externa	X	
No debe haber empalmes de ningún tipo de cables de comunicaciones		X
Los cables deben terminar en ambos extremos con sus conductores o fibras en las posiciones respectivas de los conectores	X	

No deben realizarse conexiones derivadas en serio o paralelo, en ningún punto del trayecto ni en la terminación de cables	X	
Salidas de equipo ubicadas cerca a los equipos activados que conectan	X	
Cableado clase D/categoría 6a, con o sin blindaje, en instalaciones preexistentes	X	
Cableado de fibra óptica multimodo OM1 u OM2 sólo en instalaciones preexistentes	X	
Longitudes de cableado adecuadas		X
No debe haber daños ni deformaciones en los cables, cordones, adaptadores o conectores de comunicaciones	X	
Canalizaciones, estructuras, gabinetes, y demás elementos metálicos deben estar conectados al sistema de puesta a tierra de seguridad		X
Penetraciones realizadas en muros y losas para el paso del cableado deben tener sellos que utilicen materiales para barreras contra fuego	X	
Los espacios y canalizaciones deben estar protegidos contra: el ingreso de contaminantes, la exposición a agentes que deterioren y condiciones ambientales y mecánicas que puedan afectar la integridad del Cableado Estructurado.		X
Las instalaciones de Comunicaciones deben tener canalizaciones dedicadas, es decir, no podrán compartirse con otras instalaciones del CPD	X	
Las canalizaciones para comunicaciones deben ser metálicas		X
Cualquier tipo de canalizaciones metálica no debe exceder una capacidad máxima del 50% de llenado de cables	X	
La capacidad mínima de canalizaciones por gabinete o rack es de 12 cables de par trenzado y 2 cables del 12 fibras ópticas	X	
Sistema de administraciones basado en documentación impresa		X
Sistema de administraciones elaborado en computadora	X	
Deben estar identificados todos los enlaces del cableado en ambos extremos, dentro de los primeros 30 cm de su terminación	X	
Todos los racks o gabinetes deben estar identificados en las partes superior e inferior, tanto de la cara frontal como posterior		X
Las etiquetas deben tener durabilidad que garantice la identificaciones del componente durante todo el ciclo de vida del cableado	X	
Todas las canalizaciones deben estar identificadas		X
Resultado (%)	66,65	33,36
Ámbito u Obra Civil		
Acceso controlado al Data Center	X	
Las puertas se deben cerrar automáticamente		X
Abatimiento de la puerta hacia el exterior	X	
Barra de pánico instalada en la puerta en caso de emergencia		X
Piso técnico (piso falso o elevado)	X	
El piso verdadero o losa no podrá ser menor resistencia a 250 Kg/m^2	X	
Iluminación adecuada para ambientes de TIC	X	
Mantenerse dentro de los límites de vibración marcados en la Norma	X	

Los muros no deberán estar construidos con material de fácil destrucción		X
Ausencia de tuberías hidráulicas y sanitarias dentro del CPD	X	
Resultado (%)	70	30
Sustentabilidad		
Tecnologías tendientes a mejorar la eficiencia energéticas	X	
Procesos de virtualización		X
Aire acondicionado de precisión de capacidad variable		X
Pasillos fríos y calientes		X
Chimeneas en los gabinetes para conducir eficientemente el aire caliente		X
Uso de leds para sistema de iluminación		X
Resultado (%)	16,67	83,33

Tabla 4. Ítems de acatamiento para Nivel I de Data Center de ICREA 2013 (Onofre, 2015)

Para empezar con el proceso de valoración y mapeo de riesgo que indica la metodología de ISO 27001, se debía identificar la infraestructura y gestión del data center a evaluar. Se procedió a elaborar una tabla en la que conste la infraestructura o activos identificados y observaciones que se aprecien durante la inspección. En la **tabla 5** a continuación, la matriz de riesgos desarrollada en base a las observaciones.

TIPIFICACIÓN RIESGO	INFRAESTRUCTURA Y GESTION DEL DATA CENTER	OBSERVACIÓN EN CAMPO
R1	Tablero principal	No tiene su propio tablero principal, usa el de la universidad**. Ver anexo 31.**
R2	Tablero de by pass	Si esta. **Ver anexo 32**
R3	Tablero de distribución red regulada	Si esta. **Ver anexo 33**
R4	Red eléctrica data center	Al momento de la inspección no estaba listo el plano de la red eléctrica de data center.
R5	Generador eléctrico	El data center no cuenta con generador eléctrico.
R6	Tablero de transferencia automática	Si esta.
R7	UPS	No existe redundancia de UPS. **Ver anexo 34**
R8	Aire acondicionado	El aire acondicionado no es de precisión, no existe redundancia, se debe reubicar. **Ver anexo 35**
R9	Condensador vertical	No es un aire acondicionado de precisión.
R10	Paneles	Están elaborados con material resistente y antiestático. **Ver anexo 36**
R11	Paneles perforados	Los paneles perforados son de material resistente antiestático y no están segmentadas. **Ver anexo 36**
R12	Ventosa	Se encuentra dentro del espacio del data center y junto a la puerta de acceso. **Ver anexo 37**
R13	Hermetización de pasos de cables	El paso de los cables por el piso falso no se encuentran hermetizado. **Ver anexo 38**
R14	Malla de alta frecuencia	No hay malla de alta frecuencia. **Ver anexo 39**

R15	Aterrizaje de los pedestales	No existe debido de a la ausencia de la malla de alta frecuencia. **Ver anexo 39**
R16	Sistema de puesta a tierra	La instalación del sistema se encuentra bajo los lineamientos establecidos. **Ver anexo 40**
R17	Pintura antiestática	A decir del encargado del data center, solo racks fueron cubiertos con esta pintura.
R18	Cableado	Se encuentra bajo las normas establecidas aunque existen cables expuestos. Existe holgura. **Ver anexo 41**
R19	Puntos de cobre	Óptimas condiciones.
R20	Racks y accesorios	Los racks se encuentran mal ubicados en data center. **Ver anexo 42**
R21	Fibra óptica	El sistema se encuentra bajo las exigencias establecidas. **Ver anexo 43**
R22	Canalización y tuberías	Existen tramos del cableado expuesto por falta de canaletas.
R23	Sistema de control de acceso	Sistema biométrico con acceso de cinco funcionarios en el data center. No genera bitácora de acceso. **Ver anexo 44**
R24	Sistema de gestión y monitoreo	No existe.
R25	Sistema de detección y extinción de incendios	Se cuenta con extintor, no está empotrado en la pared y se encuentra caducado. **Ver anexo 45**
R26	Sistema de video seguridad	Cámara IP desconectada de la red eléctrica. **Ver anexo 46**
R27	Puerta de seguridad	Puerta de vidrio. **Ver anexo 47**
R28	Puerta de aluminio	Es usada como puerta de seguridad.
R29	Licencia de servidores	A razón del encargado si tiene servidores licenciados. Se pidió documentación que avalará y no se entregó.

R30	Respaldos de base de los servidores	El proceso de respaldo se lo realiza automáticamente con el equipo servidor Synology. **Ver anexo 48**
R31	Tecnología servidores(fecha de compra)	Todos los servidores tienen su fecha de garantía vencida. Se encuentran operando, menos dos que a razón del encargado del data center están de reserva.
R32	Servicios tercializados	Falta de acuerdos de nivel de servicios.
R33	Capacitación del personal	El ingeniero a cargo del data center cuenta con certificados de configuración de equipos, cableado estructurado y fibra óptica
R34	Administración de recursos del data center	No se rigen al manual de funciones
R35	Informes de monitoreo	El monitoreo se realiza mediante página web que proveen de ese servicio, MikroTik y NRTG (no se entregaron). Los resultados obtenidos del monitoreo externo demuestran indisponibilidad por largos intervalos de tiempo. **Ver anexo 49**
R36	Documentación	Existe documentación técnica del equipo de Synology y UPS. Se solicitó doc. en Adquisiciones, no constaban todo equipamiento
R37	Políticas	Políticas y procedimientos en estado de revisión por parte del personal de TI. **Ver anexo 50**

Tabla 5. Matriz de riesgos
Fuente: propia del investigador

El siguiente paso fue identificar todas las amenazas y vulnerabilidades relacionadas con cada activo. Las amenazas y vulnerabilidades se identifican utilizando los catálogos otorgados dentro de la metodología. El proceso se puede apreciar a continuación en la **tabla 6**:

TIPIFICACIÓN RIESGO	INFRAESTRUCTURA Y GESTION DEL DATACENTER	VULNERABILIDAD	IMPACTO
R1	Tablero principal	Susceptibilidad del equipamiento a alteraciones en el voltaje	Daño de servidores
R2	Tablero de by pass	N/A	N/A
R3	Tablero de distribución red regulada	N/A	N/A
R4	Red eléctrica data center	N/A	N/A
R5	Generador eléctrico	Susceptibilidad del equipamiento a alteraciones en el voltaje	Fallas en equipos
R6	Tablero de transferencia automática	N/A	N/A
R7	UPS	Mantenimiento inadecuado	Fallas en equipos eléctricos
R8	Aire acondicionado		Sobrecalentamiento de los servidores

R9	Condensador vertical	Susceptibilidad del equipamiento a la temperatura	
R10	Paneles	N/A	N/A
R11	Paneles perforados	N/A	N/A
R12	Ventosa	Equipamiento móvil proclive a ser robado	Robo
R13	Hermetización de pasos de cables	No hay estanqueidad de la temperatura	Sobrecalentamiento de los equipos
R14	Malla de alta frecuencia	Posibilidades de interferencias en los equipos	Fallas en equipos
R15	Aterrizaje de los pedestales		
R16	Sistema de puesta a tierra	N/A	N/A
R17	Pintura antiestática	Posibilidades de estática por fricción	Que se apaguen los equipos
R18	Cableado	Inadecuada gestión de redes	Susceptible a daños
R19	Puntos de cobre	N/A	N/A
R20	Racks y accesorios	Inadecuada ubicación del rack	Deterioro de soportes
R21	Fibra óptica	N/A	N/A
R22	Canalización y tuberías	Cableado expuesto	Susceptibilidad a daños

R23	Sistema de control de acceso	Falta de registro y monitoreo de bitácora de acceso	Perdida de información y omisión de responsabilidad
R24	Sistema de gestión y monitoreo	Susceptibilidad del equipamiento a la temperatura	Susceptibilidad a daños
R25	Sistema de detección y extinción de incendios	Equipamiento móvil proclive a ser robado	Incendio
R26	Sistema de video seguridad	Falta de mecanismo de acercamiento y baja resolución	Falta de identificación de intruso
R27	Puerta de seguridad	Inexistencia de seguridad en el acceso físico	Robo
R28	Puerta de aluminio	Equipamiento móvil proclive a ser robado	Robo
R29	Licencia de servidores	Inadecuada o falta de implementación de auditoría interna	Uso no autorizado de materiales patentados
R30	Respaldos de base de los servidores	Única copia, sólo una copia de la información	Perdida de información
R31	Tecnología servidores(fecha de compra)	Uso de equipamiento obsoleto	Incendio
R32	Servicios tercializados	Falta de acuerdo de servicios para la disponibilidad de los mismo	Incumplimiento de relaciones contractuales

R33	Capacitación del personal	No se tiene un plan de capacitación	Uso erróneo de sistemas de información
R34	Administración de recursos del data center	Inadecuada separación de tareas	Repudio de responsabilidad
R35	Informes de monitoreo	Susceptibilidad a ataques	Ataques cibernético
R36	Documentación	Falta de manuales de configuración de equipos	Indisponibilidad del servicio
R37	Políticas	Falta de lineamientos para el trabajo de desarrollo de TI	Perdida de información

Tabla 6. Asignación de las vulnerabilidades y amenazas según las observaciones.
Fuente: propia de investigador

N/A: No Aplica

3.4.3 Probabilidad e impacto

El análisis cualitativo es el proceso de valorar el impacto y la probabilidad de ocurrencia de los riesgos identificados, utilizando una calificación apreciativa general tanto para la probabilidad como para el impacto. Las **tablas 7 y 8** se muestran la manera cómo es evaluado el riesgo del activo:

Nivel	Cuantificativa	Descripción
Insignificante	1	La pérdida de confidencialidad, disponibilidad o integridad no afecta las finanzas, las obligaciones legales o contractuales o el prestigio de la organización.
Menor	2	
Moderado	3	La pérdida de confidencialidad, disponibilidad o integridad causa gastos y tiene consecuencias bajas o moderadas sobre obligaciones legales o contractuales o sobre el prestigio de la organización.
Mayor	4	La pérdida de confidencialidad, disponibilidad o integridad tiene consecuencias importantes y/o inmediatas sobre las finanzas, las operaciones, las obligaciones legales o contractuales o el prestigio de la organización.
Catastrófico	5	

Tabla 7. Impacto
Fuente: propia del investigador

Nivel	Cuantificativa	Descripción
Raro	1	Los controles de seguridad existentes son seguros y hasta el momento han suministrado un adecuado nivel de protección. En el futuro no se esperan incidentes nuevos.
Improbable	2	
Posible	3	Los controles de seguridad existentes son moderados y en general han suministrado un adecuado nivel de protección. Es posible la ocurrencia de nuevos incidentes, pero no muy probable.
Probable	4	Los controles de seguridad existentes son bajos o ineficaces. Existe una gran probabilidad de que haya incidentes así en el futuro
Casi seguro	5	

Tabla 8. Probabilidad
Fuente: propia del investigador

3.5 Criterios para la aceptación de riesgos

Los valores 1 y 2 son riesgos aceptables, mientras que los valores 3, 4 y 5 son riesgos no aceptables. Los riesgos no aceptables deben ser tratados y por ello, se establecen controles para mitigarlos.

Este criterio de calificación fue aplicado, dando como resultado la siguiente **tabla 9**:

TIPIFICACIÓN RIESGO	INFRAESTRUCTURA Y GESTION DEL DATACENTER	RIESGO DEL ACTIVO
R1	Tablero principal	Alto
R2	Tablero de by pass	Bajo
R3	Tablero de distribución red regulada	Bajo
R4	Red eléctrica data center	Bajo
R5	Generador eléctrico	Alto

R6	Tablero de transferencia automática	Bajo
R7	UPS	Medio
R8	Aire acondicionado	Alto
R9	Condensador vertical	
R10	Paneles	Bajo
R11	Paneles perforados	Bajo
R12	Ventosa	Bajo
R13	Hermetización de pasos de cables	Bajo
R14	Malla de alta frecuencia	Medio
R15	Aterrizaje de los pedestales	
R16	Sistema de puesta a tierra	Bajo
R17	Pintura antiestática	Bajo
R18	Cableado	Medio
R19	Puntos de cobre	Bajo
R20	Racks y accesorios	Bajo
R21	Fibra óptica	Bajo
R22	Canalización y tuberías	Alto
R23	Sistema de control de acceso	Medio
R24	Sistema de gestión y monitoreo	Alto
R25	Sistema de detección y extinción de incendios	Alto
R26	Sistema de video seguridad	Medio
R27	Puerta de seguridad	Alto
R28	Puerta de aluminio	Alto

R29	Licencia de servidores	Bajo
R30	Respaldos de base de los servidores	Alto
R31	Tecnología servidores(fecha de compra)	Bajo
R32	Servicios tercializados	Medio
R33	Capacitación del personal	Alto
R34	Administración de recursos del data center	Medio
R35	Informes de monitoreo	Alto
R36	Documentación	Alto
R37	Políticas	Alto

Tabla 9. Calificación del riesgo
Fuente: propia del investigador

Al finalizar la calificación se puede apreciar que la mayoría de los activos del data center corren un riesgo alto. Después de determinar cuáles son los riesgos no aceptados, se emplea el mecanismo de tratamiento de riesgo mediante la definición de controles.

3.5.1 Mapa de Calor Riesgo Inherente

En el **gráfico 13** se representa el nivel de impacto que tendría cada riesgo considerando la vulnerabilidad del activo auditado. Este es el mapa de riesgo inherente como resultado de este proceso de análisis de riesgo.

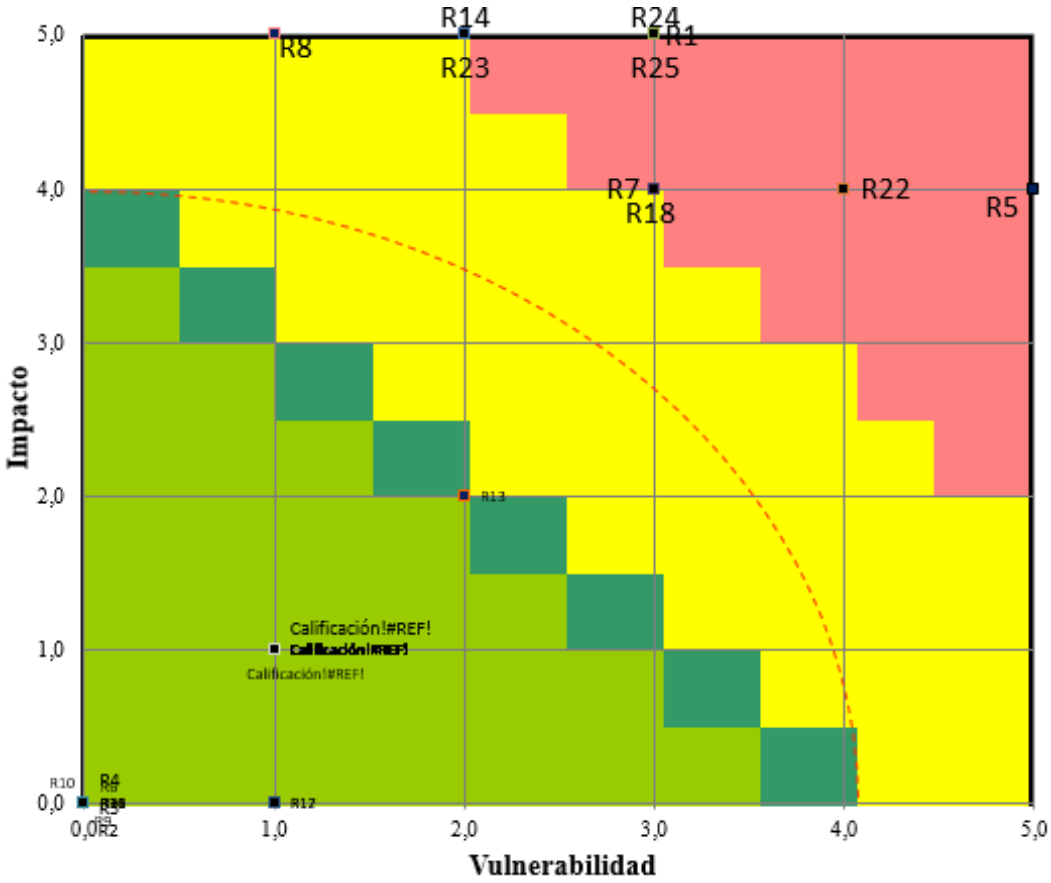


Grafico 13. Mapa de calor del riesgo inherente
Fuente: propia del investigador

Los valores que sobrepasan la curvatura representan aquellos riesgos de activos que después de la evaluación obtuvieron valoraciones altas.

3.6 Cuadro de Tratamiento del riesgo

El tratamiento de riesgos se implementa mediante el cuadro de tratamiento de riesgos, copiando desde el cuadro de evaluación de riesgos todos los riesgos identificados como no aceptables. En la **tabla 10** se puede apreciar el cuadro de tratamiento de riesgos.

TIPIFICACIÓN RIESGO	INFRAESTRUCTURA Y GESTION DEL DATACENTER	RIESGO DEL ACTIVO	PROBABILIDAD QUE LA AMENAZA EXPLOTE LA VULNERABILIDAD	IMPACTO DE MATERIALIZACIÓN DE LA AMENAZA	CONTROL
R1	Tablero principal	Alto	3,0	5,0	Instalación del tablero principal para el data center
R5	Generador eléctrico	Alto	5,0	4,0	Instalación de generador eléctrico
R7	UPS	Medio	3,0	4,0	Adquisición de UPS
R8	Aire acondicionado	Alto	2.5	5,0	Adquisición e instalación de aire acondicionado de precisión
R14	Malla de alta frecuencia	Medio	2,0	5,0	Instalación de malla de alta frecuencia

R18	Cableado	Medio	3,0	4,0	Cubierta de protección para el cable de red
R22	Canalización y tuberías	Alto	4,0	4,0	Cubierta de protección para el cable de red
R23	Sistema de control de acceso	Medio	2,0	5,0	Sistema biométrico con consulta web de acceso.
R24	Sistema de gestión y monitoreo	Alto	3,0	5,0	Implementación de un sistema de monitoreo que permita controlar la temperatura
R25	Sistema de detección y extinción de incendios	Alto	3,0	5,0	Implementar un sistema de agente limpio para detección de incendio para data center
R27	Puerta de seguridad	Alto	3,0	5,0	Instalar una puerta de seguridad
R28	Puerta de aluminio	Alto	3,0	5,0	Retiro de puerta por falta de garantías de seguridad
R30	Respaldos de base de los servidores	Alto	5,0	5,0	Desarrollar políticas de respaldo de información

R33	Capacitación del personal	Alto	5,0	5,0	Desarrollar plan capacitación para el personal
R34	Administración de recursos del data center	Alto	5,0	3,0	Cumplimiento de rol de funciones de acuerdo a contrato
R35	Informes de monitoreo	Alto	3,0	5,0	Definición de políticas de seguridad informática
R36	Documentación	Alto	4,0	5,0	Desarrollo de un repositorio de la documentación técnica.
R37	Políticas	Alto	4,00	5,00	Definición e implementación de políticas con respecto al data center

Tabla 10. Cuadro de tratamiento de riesgos
Fuente: propia del investigador

Para los riesgos calificados en 4 y 5 se ha seleccionado controles.

3.6.1 Observaciones

3.6.1.1 No contar con un tablero principal.

No se dispone de un tablero principal para protección de los equipos alojados en el data center, exponiéndolos a daños por cortocircuito durante un corte de energía eléctrico.

3.6.1.2 No contar con un generador eléctrico.

No se cuenta con un generador eléctrico que garantice la continuidad de los servicios del data center a pesar de cortes de energía eléctrica. Esto provoca la paralización de servicios importantes como el aula virtual.

3.6.1.3 No contar con un UPS en óptimas condiciones.

No se dispone de un UPS en buenas condiciones que garantice el tiempo indicado para salvaguardar los equipos servidores lo que provoca daños en los mismos representando gastos en mantenimiento correctivo. Si se tiene un óptimo sistema de respaldo de energía la infraestructura del data center se encontrará asegurada y no habrá indisponibilidad de los servicios.

3.6.1.4 No contar con un aire acondicionado de precisión.

Se dispone de un aire acondicionado de confort que no es indicado para el data center lo que impide la correcta propagación del aire frio entre los racks y eso conlleva al sobrecalentamiento de los servidores. Además, el equipo que se tiene para climatización es viejo y amerita el cambio prontamente. Existen antecedentes negativos con respecto a su rendimiento.

3.6.1.5 No contar con una malla de alta frecuencia.

No se tiene una malla de alta frecuencia que impida la interferencia electromagnética lo que provoca mal funcionamiento en los equipos de telecomunicaciones. La malla de alta frecuencia debe estar conectada con el sistema de puesta a tierra, si no se cuenta con ella los equipos no se encuentran totalmente seguros.

3.6.1.6 No tener el cableado estructurado protegido adecuadamente.

No se dispone de las canaletas suficientes para la protección del cableado haciéndolo susceptible a daños externos. En versión del encargado, la fibra óptica fue afectada por ataque de roedores representado un gasto en reposición del segmento afectado a pesar de que la eventualidad podría haberse evitado. Además, evidenció que el data center no cumple con uno de sus requerimientos importantes, ser hermético.

3.6.1.7 No contar con sistema de control de acceso.

No se dispone de un sistema de control de acceso que permita la identificación y validación de la identidad del personal que ingresa al data center. No existe una bitácora en que se registren los accesos al espacio del data center para mayor control. Durante el proceso de auditoría, se pudo evidenciar que al encargado de data center le sustrajeron una tarjeta que también permite el acceso. Esta eventualidad vulnera notablemente la seguridad considerando que la cámara se encontraba desconectada de la red eléctrica en el momento de la auditoria.

3.6.1.8 No contar con sistema de gestión y monitoreo.

No se dispone de un sistema de gestión y monitoreo que vigile las condiciones de temperatura de los equipos servidores alojados y del sistema de climatización en el data center haciéndolos susceptibles a sobrecalentamiento. Se tiene versiones que el aire acondicionado con el que cuenta ha dejado de funcionar exponiendo a daño los equipos por sobrecalentamiento. Si se hubiera contado con el sistema de monitoreo no se expondría a ese riesgo.

3.6.1.9 No contar con sistema de detección y extinción de incendios.

No se dispone de un sistema de detección temprana y extinción de incendios haciéndolo notablemente vulnerable ante un siniestro de esa magnitud teniendo la pérdida total de activos considerando que la política de respaldo no opera aun. Por el momento en el data center hay un extintor con su fecha de caducidad vencida.

3.6.1.10 No se cuenta con puerta de seguridad

En el data center se tiene una puerta de aluminio que no brinda las seguridad que necesita; vulnera la integridad y confidencialidad que debe tener el data center. Se necesita de una puerta de acero que cumpla con todas las medidas de seguridad, es decir, para los equipos servidores y en casos de presentarse eventualidades.

3.6.1.11 Respaldos de base de los servidores

No se tiene dispositivos magnéticos que sirvan como respaldo. Se cuenta solamente con equipamiento de respaldo masivo (Synology) en donde se encuentran alojada la información de toda la universidad, es decir se tiene solo una copia. En caso de presentarse una catástrofe que afecte a las instalaciones del data center esa información se perdería.

3.6.1.12 Capacitación del personal

El responsable del data center cuenta con cursos y certificaciones que las realizo de manera autofinanciada, pero no como parte de un plan de capacitación definido por el departamento. Si se planifican las capacitaciones se pueden establecer prioridades con respecto a las necesidades del data center y realizar cursos de certificaciones que en verdad amerite progreso para la infraestructura.

3.6.1.13 Mala administración de recursos de Data Center

Los roles de función no son asumidos por el personal correcto. El encargado del data center supervisa el desempeño del equipamiento que no está a su cargo.

3.6.1.14 Informes de monitoreo

Se realiza el monitoreo de los servicios web usando páginas que proveen del servicio. Además, el encargado del data center usa herramientas provistas por Mikrotik y para vigilar el ancho de banda usa NRTG que fue dado por el proveedor de Internet.

3.6.1.15 Falta documentación

Falta documentación técnica de los equipos alojados en el data center. Cuando se realizó la auditoria, se solicitaron documentos y entregaron del equipo de almacenamiento masivo Synology y del UPS, teniendo claro que en el data center existe más equipos alojados como el equipo de fibra óptica, switch, routers MikroTik y equipos My Cloud.

3.6.1.16 No hay políticas vigentes.

Las actividades que se realizan con respecto al data center durante la auditoria no se encuentran amparadas bajo ninguna política ni procedimientos debido a que están en restructuración de los mismo. Cuando se solicitó la documentación el personal dijo que no están vigentes y entregaron documentación antigua.

3.6.2 Conclusiones y recomendaciones

En virtud de lo expuesto, se considera que el data center de la PUCESE presenta debilidades en cuanto a seguridad en infraestructura e información; por falta de políticas de mitigación de riesgos, que pueden afectar la integridad y disponibilidad de los servicios que se manejan desde el data center de la institución, por tanto se sugiere trabajar en la implementación de los controles que minimicen el riesgo antes que se materialicen las vulnerabilidades anteriormente citadas.

3.6.2.1 Es primordial la implementación de un sistema de detección y extinción de incendio para asegurar a la infraestructura y equipamiento del data center en el caso de que suceda un incendio **3.6.1.9**.

3.6.2.2 Se debe instalar un tablero principal de distribución eléctrica para el data center para salvaguardar la integridad del equipamiento alojado en él. Además, se estaría cumpliendo un requerimiento de la Norma ICREA 2013. Será necesaria su instalación si se realiza la compra del generador eléctrico. **3.6.1.1**.

3.6.2.3 Se debe realizar la compra del generador eléctrico para garantizar que los servicios críticos que se administran desde el data center no se paralicen. **3.6.1.2**.

3.6.2.4 Se sugiere la compra de un nuevo UPS que brinde seguridad a los equipos servidores durante un corte energía y el que se dispone actualmente usarlo como redundancia N+1. **3.6.1.3**.

3.6.2.5 Se debe realizar la adquisición de un aire acondicionado de precisión que es el indicado para uso en data center para que las condiciones de climatización dentro del cuarto de equipos sea la correcta **3.6.1.4**.

3.6.2.6 Se debe instalar la malla de alta frecuencia para evitar que los equipos de telecomunicaciones fallen en su funcionamiento **3.6.1.5**.

3.6.2.7 Para evitar los daños por exposición de cableado estructurado en el data center se debe comprar las canaletas para proteger de eventualidades **3.6.1.6**.

3.6.2.8 Se debe adquirir un sistema de control de acceso que sea confiable en la identificación y que registre los ingresos al espacio del data center para evitar incidentes **3.6.1.7**.

3.6.2.9 Se debe adquirir un sistema que permita mantener la temperatura adecuada dentro del data center y evitar inconvenientes por sobrecalentamiento en equipos servidores **3.6.1.8**

3.6.2.10 Para garantizar la seguridad en el data center se debe hacer la adquisición de una puerta de acero denominada "puerta de seguridad"; porque además de cumplir el requerimiento de ser hermético, también protege la vida del personal en caso de presentarse un conato de incendio en el interior del data center. **3.6.1.10**

3.6.2.11 Se recomienda definir las políticas de respaldo de información con la finalidad de garantizar la integridad de la información. No se debe confiar a que solo exista una copia de los datos guardados en los equipos del data center por ello, se sugiere implementar una biblioteca de respaldos y su ubicación fuera del departamento por seguridad. **3.6.1.11**

3.6.2.12 Se debe elaborar un plan de capacitación del personal del departamento que tiene equipamiento a su cargo del data center. Cuando el personal se encuentra bien capacitado, ejerce sus funciones a cabalidad. **3.6.1.12**

3.6.2.13 Se debe respetar el manual de funciones que reposa en el Departamento de Recursos Humanos con respecto a los roles de funciones de Departamento de TIC´s. No se puede asumir responsabilidades ajenas al cargo asignado porque afectaría la eficiencia del Data Center. **3.6.1.13**

3.6.2.14 Debe tomarse decisiones con respecto a los informes obtenidos del monitoreo de la página web de la PUCESE. Se monitorea la disponibilidad y si se obtiene resultado negativo se debe activar un control que contrarreste la eventualidad. **3.6.2.14**

3.6.2.15 Se debe tener en las dependencia de la Jefatura de TIC´s la documentación sobre las adquisiciones de equipamiento, los equipos y planos de la red eléctrica instalada en el data center. **3.6.1.15**

3.6.2.16 Se debe contar con políticas establecidas en el menor tiempo posible y procedimientos correctamente definidos relacionados con el data center. **3.6.2.16**

3.7 Plan de tratamiento del riesgo

Se preparó el plan de tratamiento de riesgos que implementará los controles. En la **tabla 11** se visualiza en plan de tratamiento.

Descripción de actividades	Recursos generales y financieros necesarios	Persona responsable	Plazos de inicio y finalización	Método para evaluación de resultados
Adquisición de tablero principal	3.423,64	Jefe de TIC´s	Anual	Verificar compra
Adquisición de generador eléctrico	27.060,00	Jefe de TIC´s	Anual	Verificar compra
Adquisición de UPS	13.936,36	Jefe de TIC´s	Anual	Verificar compra
Adquisición de aire acondicionado de precisión	18.251,00	Jefe de TIC´s	Anual	Verificar compra
Adquisición de malla de alta frecuencia	5.400,00	Jefe de TIC´s	Anual	Verificar compra
Adquisición de cubierta de protección para la red	734,95	Jefe de TIC´s	Anual	Verificar compra
Adquisición de sistema biométrico	2.280,00	Jefe de TIC´s	Anual	Verificar compra
Adquisición de sistema de monitoreo de temperatura	2.280,00	Jefe de TIC´s	Anual	Verificar compra
Adquisición de sistema de detección de incendios	33.512,97	Jefe de TIC´s	Anual	Verificar compra
Adquisición de una puerta de seguridad	3.556,00	Jefe de TIC´s	Anual	Verificar compra
Adquisición de discos externos	524.00	Jefe de TIC´s	Anual	Verificar compra
Desarrollo de plan de capacitación para el personal	7.000,00	Jefe de TIC´s	Anual	Verificar documentación
Desarrollo de un repositorio de la documentación técnica.		Jefe de TIC´s	Anual	Verificar documentación
Definición e implementación de políticas con respecto al data center	1.000,00	Jefe de TIC´s	Anual	Verificar documentación

Tabla 11. Cuadro de plan de tratamiento de riesgos
Fuente: Metodología de análisis de riesgos ISO/IEC 27001

Cada actividad es presentada con los costos estimados para su implementación. Se asigna como responsable al Jefe de TIC´s e indicando como plazo cada actividad a un año. Los métodos de evaluación de resultados son la actividad de verificación de compra que hará seguimiento con respecto adquisición e instalación del activo necesario para el tratamiento del riesgo; y verificación de documentación aprobada para controlar los riesgos con respecto a las políticas y planes.

CAPITULO IV

4 ANÁLISIS DE IMPACTOS

4.1 ANTECEDENTES

Finalizada la Gestión de Riesgo del Data Center de la PUCESE basados en Estándares Internacionales, se han determinados algunos impactos en el aspecto: Tecnológico, Administrativo y Económico.

Para poder interpretarlos existen los siguientes niveles:

Valor	Equivalencia
3	Impacto Alto Positivo
2	Impacto Medio Positivo
1	Impacto Bajo Positivo
0	No causa impacto
-1	Impacto Bajo Negativo
-2	Impacto Medio Negativo
-3	Impacto Alto Negativo

Tabla 12. Matriz de impactos
Fuente: propia del investigador

4.2 Impacto Tecnológico

Niveles de impacto / Indicadores	-3	-2	-1	0	1	2	3
Salvaguarda de activos del data center							**X**
Implementación de sistemas para data center							**X**
Controles tecnológicos							**X**
Impacto = Sumatoria de Impactos							
							9

$\Sigma = 9$

$$\text{Nivel de impacto tecnológico} = \frac{\Sigma}{\textbf{número de indicadores}}$$

$$NI = \frac{9}{3} = 3$$

Nivel de Impacto Tecnológico = Alto Positivo

Tabla 13. Impacto Tecnológico
Fuente: propia del autor

Análisis:

- Salvaguarda de activos del data center se lo considera como alto positivo porque cumplió con los requerimientos de seguridad establecidos para la protección de infraestructura, los equipos servidores y la información alojada en él.

- Implementación de sistemas para data center se lo considera como alto positivo porque el empleo de la tecnología en las actividades implica gran influencia sobre el trabajo cotidiano.

- Controles tecnológicos se lo considera como un alto impacto positivo después de que se implementen las mejoras sugeridas al data center. Será el modo de medir el desempeño de la infraestructura.

4.3 Impacto Administrativo

Niveles de impacto / Indicadores	-3	-2	-1	0	1	2	3
Aplicación de estándares							**X**
Definición de responsable de administración de riesgo						**X**	
Metodología de Gestión de Riesgos							**X**
Mejora continua de la gestión de riesgo							**X**
Impacto = Sumatoria de Impactos							
						2	**9**

$$\Sigma = 11$$

$$\text{Nivel de impacto administrativo} = \frac{\Sigma}{\text{número de indicadores}}$$

$$\text{NI} = \frac{11}{4} = 2.75 \approx 3$$

Nivel de Impacto Administrativo = Alto Positivo

Tabla 14. Impacto Administrativo
Fuente: propia del investigador

Análisis:

- Aplicaciones de estándares fue considerada como un impacto alto positivo porque fue aplicada en su totalidad considerando el nivel de madurez y fiabilidad que podía aplicar.

- Definición de responsable de administración de riesgos se lo considera dentro de medio positivo considerando que puede ser el Jefe del Departamento de TIC´s como encargado de vigilar que los riesgos sean mitigados en su totalidad.

- Metodología de Gestión de Riesgo es calificada como alto positivo porque fue aplicada en su totalidad.

- Mejora continua de la gestión de riesgo está catalogada como impacto alto positivo pues si se aplica el análisis de riesgo de manera periódica se garantiza que aquellos riesgos que se calificaron como medio puedan bajar y evitar vulnerabilidades.

4.4 Impacto Económico

Niveles de impacto / Indicadores	-3	-2	-1	0	1	2	3
Compra de infraestructura	**X**						
Disminución de costos						**X**	
Impacto = Sumatoria de Impactos							
	-3					**2**	

$$\Sigma = -1$$

$$\text{Nivel de impacto económico} = \frac{\Sigma}{\text{número de indicadores}}$$

$$\text{NI} = \frac{-1}{2} = -0.5 \approx -1$$

Nivel de Impacto Económico = Bajo Negativo

Tabla 15. Impacto Económico
Fuente: propia del investigador

Análisis:

- Compra de infraestructura está considerada como alto negativo debido a que debe hacer adquisiciones con un presupuesto considerable para que el data center se encuentre en óptimas condiciones para hacer frente a los riesgos de TI.

- Disminución de costos seria de impacto medio alto considerando la notable disminución de riesgos a los que haría frente en caso que se implementen las medidas expuestas para el tratamiento de riesgos.

4.5 Impacto General

Niveles de impacto / Indicadores	-3	-2	-1	0	1	2	3
Impacto Tecnológico							**X**
Impacto Administrativo							**X**
Impacto Económico			**X**				
Impacto = Sumatoria de Impactos							
			-1				**6**

$$\Sigma = 5$$

$$\text{Nivel de impacto general} = \frac{\Sigma}{\textbf{número de indicadores}}$$

$$\text{NI} = \frac{5}{3} = 1.67 \approx 2$$

Nivel de Impacto General = Medio Positivo

Tabla 16. Impacto General
Fuente: propia de investigador

Análisis:

La implementación del presente proyecto tendrá un impacto general medio positivo considerando los tres campos de impacto: Tecnológico, Administrativo y Económico. Toda implementación para mejoramiento de la infraestructura

tecnológica significa inversión justificada, sobre todo si se refiere al tratamiento de riesgos. La Gestión de Riesgos para el Data Center contempla adquisiciones que salvaguarda los equipos servidores y la información.

CONCLUSIONES

- La situación en la que se encuentra la infraestructura tecnológica de la PUCESE, muestra que no alcanza los requerimientos mínimos de un centro de procesamiento de datos del Nivel I a pesar de que brinda servicios de TI de importancia.

- Debido a la falta de plan de tratamiento de riesgos el Data Center de la PUCESE es vulnerable a eventualidades, generando incomodidades en la comunidad universitaria. La adquisición del equipamiento solicitado en el cuadro de tratamiento de riesgos ayudaría de manera significativa al buen desempeño.

- La gestión de riesgos de TI es el manejo de los riesgos tecnológicos con el fin de plantear acciones para contrarrestar los posibles efectos que produzcan.

- El uso de estándares para la seguridad de la infraestructura tecnológica y seguridad de la información debe mantenerse para alcanzar los requerimientos más importantes con respecto al manejo de información bajo los criterios confidencialidad, integridad y disponibilidad.

- La gestión del data center con respecto a los riesgos y los procedimientos de control, no son aceptables en todos los aspectos considerados, de acuerdo a las normas ICREA Std-131-2013 e ISO 27001.

RECOMENDACIONES

- Ejecutar el plan de Tratamiento de Riesgos para mitigar los riesgos inherentes.

- Asignar a un responsable para la administración de riesgos que se encargue de vigilar los activos que están en riesgo inherente, contrarrestarlos y garantizar que la mejora continua de los servicios de TI no sean afectados.

- Desarrollar el Plan Anual de Capacitación con presupuesto aprobado por el Pro-rectorado y elaborado por el Departamento de TIC´s en base a las necesidades que presenta el Data Center.

- Al realizar las adquisiciones para el Data Center se recomienda analizar los riesgos junto con asesoría de un especialista en ambientes de TI.

- Elaborar posteriormente plan de tratamiento de riesgos para que mitigue los riesgos residuales que pueden presentarse en los siguientes años.

- Considerar las recomendaciones obtenidas de la auditoria basada en Gestión de Riesgos para desarrollar un plan de contingencia ante los riesgos latentes que tenga el Data Center.

BIBLIOGRAFÍA

27001Academy. (2016). *¿Qué es norma ISO 27001?* Obtenido de ¿Qué es norma ISO 27001?: http://advisera.com/27001academy/es/que-es-iso-27001/

27001Academy. (2016). *Cuadro de Evaluacion de riesgos*. Obtenido de http://advisera.com/27001academy/es/documentation/cuadro-y-catalogos-de-evaluacion-del-riesgo/

27001Academy. (2016). *Cuadro de tratamiento de riesgos*. Obtenido de http://advisera.com/27001academy/es/documentation/cuadro-de-tratamiento-del-riesgo/

27001Academy. (2016). *Informe sobre evaluación y tratamiento de riesgos*. Obtenido de http://advisera.com/27001academy/es/documentation/informe-sobre-la-evaluacion-de-riesgos/

27001Academy. (2016). *Metodología de evaluación y tratamiento de riesgos*. Obtenido de http://advisera.com/27001academy/es/documentation/metodologia-de-evaluacion-y-tratamiento-de-riesgos/

ADRFORMACION. (2014). Obtenido de http://www.adrformacion.com/cursos/wserver082/leccion1/tutorial6.html

Aguirre, H. (25 de Mayo de 2014). *Introducción a COBIT* . Obtenido de https://chaui201411700722390.wordpress.com/2014/05/25/introduccion-a-cobit-4-1/

AlambrixIT. (28 de mayo de 2012). *Como armar uun cable de red cruzado*. Obtenido de https://www.youtube.com/watch?v=jphv4zfKBcs

ALCAGLAS. (2015). *ALCAGLAS*. Obtenido de http://www.alcaglas.com/infer.php?gr=accesorios-vidrio&sg=herramientas-vidrio&vista=cuadricula

ALEGSA. (2016). *Definición de UPS*. Obtenido de http://www.alegsa.com.ar/Dic/ups.php

Alvarado, C., Yáñez, I., & Vásquez, J. (16 de Marzo de 2009). *COBIT- Sistema de Investigación.* Obtenido de http://es.slideshare.net/Jasik/c-o-b-i-t-sistema-de-investigacin

Amaya, C. G. (14 de MAYO de 2013). *MAGARET: metogología práctica para gestionar riesgos*. Obtenido de http://www.welivesecurity.com/la-es/2013/05/14/magerit-metodologia-practica-para-gestionar-riesgos/

AMPER. (2016). *CyberAir*. Obtenido de http://www.amperonline.com/marca/stulz

Andrade, J. F. (2013). Propuesta de Gestión del Riesgo de Infraestructura Tecnológica basada en COBIT, para la empresa Soft Warehouse S.A.

AprendaRedes.com. (7 de Junio de 2013). *¿Qué es un data center?* Obtenido de http://www.aprendaredes.com/blog/que-es-un-data-center-4/

AreaData. (2015). *Monitoreo Ambiental*. Obtenido de http://www.areadata.com.ar/Monitoreo_Ambiental.html

Artilec. (2015). *LECTOR BIOMETRICO PIN*. Obtenido de http://www.artilec.cl/lector-biometrico-pin.html

auditoriasistemas. (2016). *Tabla comparativa*. Obtenido de https://auditoriasistemas.wikispaces.com/TablaComparativa

Avellaneda, J. C. (10 de Junio de 2008). *Apuntes de seguridad de la información*. Obtenido de http://seguridad-de-la-informacion.blogspot.com/2008/06/publicada-la-iso-270052008.html

Baquero, K., Calle, L., Guamán, K., & Villalva, J. (2012). *COBIT (Objetivos de Control para la Información y Tecnologías Relacionadas)*. Obtenido de http://www.monografias.com/trabajos93/cobit-objetivo-contro-tecnologia-informacion-y-relacionadas/cobit-objetivo-contro-tecnologia-informacion-y-relacionadas.shtml

Cadavid, C. A. (24 de Agosto de 2015). *¿Qué es ITIL?* Obtenido de http://teinco2015-que-esittil.blogspot.com/2015_08_01_archive.html

Casa Navia. (2014). *Canalización*. Obtenido de http://www.casanavia.cl/canalizacion.html

Castro, A. R. (4 de Septiembre de 2012). *Riesgo tecnológico y su impacto parra las organizaciones parte I*. Obtenido de http://revista.seguridad.unam.mx/numero-14/riesgo-tecnol%C3%B3gico-y-su-impacto-para-las-organizaciones-parte-i

Chavez, R. (15 de Septiembre de 2013). *Gestión del riesgos de seguridad de la información*. Obtenido de http://es.slideshare.net/roberth.chavez/gestin-del-riesgos-de-seguridad-de-la-informacin

Cibertec. (2015). *¿Qué es COBIT?* Obtenido de http://www.cibertec.edu.pe/formacion-continua/certificaciones-internacionales/cursos-cobit/que-es-cobit/

Comstor. (3 de Junio de 2014). *¿Qué es un data center?* Obtenido de http://blogmexico.comstor.com/%C2%BFqu%C3%A9-es-un-data-center

Cummins. (2016). *Generadores electricos*. Obtenido de http://generadoreselectricos.info/

Decomsa. (2015). *Varillas para tierra.* Obtenido de http://decomsa.net/productos/sistemas-de-tierra/

Devia, G. A., & Pardo, C. J. (2014). *Hacia un modelo para la gestión de riesgos de TI* . Obtenido de http://www.redalyc.org/comocitar.oa?id=411534000003

Diesel Service Generation. (2015). *¿Qué es tablero de transferencia?* Obtenido de http://venta-deplantasdeluz.com.mx/que-es-tablero-de-transferencia.html

ElectrostatEx. (2012). *Industria Electrónica*. Obtenido de http://www.electrostatex.com/Productos-Antiestaticos/Industria-Electronica.php

Emerson Network Power. (2016). *ASCO Series 300SE Service Entrance Power Transfer Switch*. Obtenido de http://www.emersonnetworkpower.com/es-EMEA/Products/PowerSwitchingandControls/PowerTransferSwitches/Pages/ASCOSeries300SEServiceEntrancePowerTransferSwitch.aspx

Equipo 4. (27 de Julio de 2015). *Data Center*. Obtenido de https://datacenterequipo4.wordpress.com/2015/07/27/hola-mundo/

Espinoza, P. (29 de Marzo de 2012). *Estándar TIA 942.* Obtenido de http://es.slideshare.net/PatrickEspi/estndar-tia-942

FibreMex. (2916). *Fibra óptica*. Obtenido de http://fibremex.com/fibraoptica/index.php?mod=contenido&id=3&t=3

Garcia, A. (2015 de Noviembre de 2015). *Servicio de TI*. Obtenido de http://armando-garcia-cesareo.blogspot.com/2015/11/itil-ve-2011-y-cobit-5.html

Google. (2016). *Centro de Datos*. Obtenido de https://www.google.com/about/datacenters/inside/locations/douglas-county/working-here.html

GUÍA DE SOLUCIOINES TIC. (2011). *HSS Ingeniería Piso Falso - Técnico*. Obtenido de http://www.guiadesolucionestic.com/centros-de-computo-data-centers-centro-de-datos-/pisos-falsos-pisos-tecnicos-pisos-elevados/390-hss-ingenieria-piso-falso-tecnico

Guilarte, M. (14 de Marzo de 2013). *¿Qué es Tier?* Obtenido de http://www.muycomputerpro.com/2013/03/14/que-es-un-tier

IAN Ingeniería Aplicada del Norte. (2016). *IAN Presentacion Comercial*. Obtenido de http://ianmexico.com.mx/wp-content/uploads/2015/06/Presentacion-IAN.pdf

Indeo. (2016). *EATON EX 1000 MINI TORRE*. Obtenido de http://grupoindeo.es/sai-para-servidores/1112-eaton-ex-1000-mini-torre-3553340681813.html

Innovación Energética Inga. (15 de Diciembre de 2013). *EQUIPAMIENTO ELÉCTRICO PARA DISEÑO DE DATA CENTER.* Obtenido de http://es.slideshare.net/cesaringazapata/presentacin-data-center-telecomunicaciones

International Computer Room Experts Assotiation. (2013). Norma Internacional para la Construcción e Instalación de Equipamiento de Ambientes para el Equipo de Manejo de la Información y Similares. Ciudad de México.

IT Process Maps GbR. (2010). *Introducción a ITIL Versión 3 y al Mapa de Procesos ITIL V3.* Obtenido de https://albinogoncalves.files.wordpress.com/2011/03/introduccion-mapa-de-procesos-itil-v3.pdf

Jack Power. (2016). *Generadores*. Obtenido de http://spanish.genset-dieselgenerator.com/china-48kw_65kva_cummins_diesel_generators_with_24v_alternator-1133656.html

LASER CENTRO DE MANTENIMIENTO ELÉCTRICO. (2015). *Ingeniería y construccion de tableros automáticos*. Obtenido de http://www.cmelaser.com/ingenieriacutea-y-construccioacuten-de-tableros-automaacuteticos.html

Mariana Arroyo, A. B. (15 de SEPTIEMBRE de 2015). *Gobierno de TI*. Recuperado el 2014, de https://www.youtube.com/watch?v=SrflumuGzzE

Mink Bursten. (2015). *Cepillos de Listón / paso de cables*. Obtenido de https://www.mink-buersten.com/es/productos-tienda/cepillos-de-liston/paso-de-cables.html

Mundo HVACR. (20 de Enero de 2014). *AA de precisión vs AA de confort*. Obtenido de https://www.mundohvacr.com.mx/mundo/2014/01/aa-de-precision-vs-aa-de-confort/

Onofre, D. (2015). DISEÑO DE LA INFRAESTRUCTURA FÍSICA DEL DATA CENTER EN EL GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DE SAN PEDRO DE PIMAMPIRO BASADO EN LA NORMA INTERNACIONAL ICREA-STD-131-2013.

Oriente, J. (2014 de Enero de 2014). *Apuntes ITIL 2011: Ciclo de vida de un servicio*. Obtenido de http://joaquinoriente.com/2014/01/24/apuntes-itil-2011-ciclo-de-vida-de-un-servicio/

Osores, M. (Julio de 2014). *Principios de COBIT 5 para el gobierno efectivo de TI*. Obtenido de http://searchdatacenter.techtarget.com/es/cronica/Principios-de-COBIT-5-para-el-gobierno-efectivo-de-TI

Panduit. (2014). *Productos.* Obtenido de http://www.panduit.com/wcs/Satellite?c=Page&childpagename=Panduit_Global%2FPG_Layout&cid=1345575866705&packedargs=classification_id%3D2320%26locale%3Des_es&pagename=PG_Wrapper

Pascual, Alberto Escudero. (Octubre de 2010). *Estándares en Tecnologías Inalámbricas.* Recuperado el 2014, de http://www.itrainonline.org/itrainonline/mmtk/wireless_es/files/02_es_estandares-inalambricos_guia_v02.pdf

PEDI-PUCESE. (17 de Septiembre de 2012). *www.pucese.edu.ec*. Recuperado el 27 de mayo de 2014, de PUCESE: http://www.pucese.edu.ec/index.php/features/mision-y-vision

PeopleCert. (2015). *Qué es ITIL*. Obtenido de http://www.peoplecert.org/es/ITIL_V3/Que_es_ITIL%C2%AE/Pages/Que_es_ITIL%C2%AE.aspx

Perez, A. (2 de Noviembre de 2012). *Presentación COBIT.* Obtenido de http://es.slideshare.net/antonyamd9/presentacion-cobit-14998980

PowerHost Data Center. (2016). *Conectividad & Estructura de Red*. Obtenido de http://www.powerhost.cl/datacenter

Ríos, F. D. (28 de MAYO de 2014). *Gestión de Continuidad del Negocio.* Recuperado el 09 de junio de 2014, de http://es.slideshare.net/fernandelos/gestin-de-continuidad-del-negocio-35243888

Rubio, J. (2012). malla hecha con láminas de cobre que se utiliza para asegurar el aterrizaje de las desviaciones de alta frecuencia, generados por los equipos eléctricos. Obtenido de http://dspace.ups.edu.ec/bitstream/123456789/3537/1/UPS-ST000821.pdf

Segarra, S. (11 de Julio de 2011). *COBIT 5 tanteando el terreno*. Obtenido de http://www.securityartwork.es/2011/07/11/5745/

Solano, M., & Zúñiga, A. (18 de Octubre de 2013). *Riesgos de TI*. Obtenido de http://es.slideshare.net/LeoGomez3/riesgo-de-ti

Soporte Remoto Mexico. (2008). *¿Qué es ITIL? Ventajas y desventajas*. Obtenido de http://www.soporteremoto.com.mx/help_desk/articulo04.html

Tapia, A. M. (2 de Octubre de 2015). *COBIT*. Obtenido de http://anamatapi.blogspot.com/

Tecniases. (2012). *Proyectos*. Obtenido de http://www.tecniases.com/proyectos.php

Telepartes. (2012). *Racks*. Obtenido de http://www.telepartes.com.pe/productos/c/rack**s**

ANEXOS

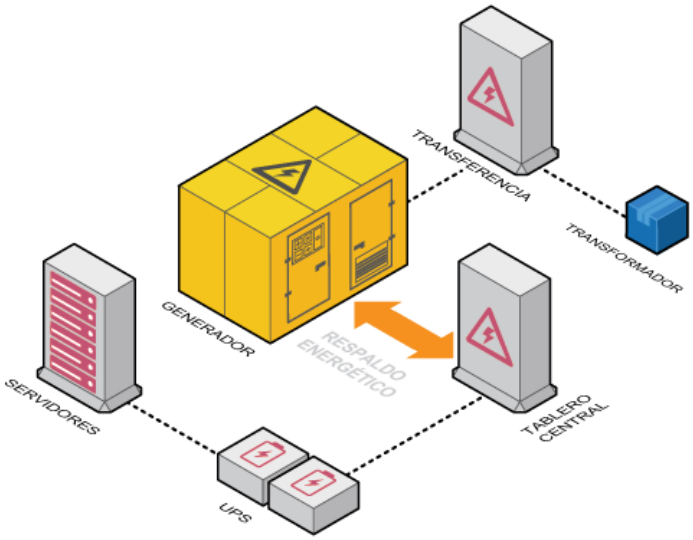
ANEXO 1

Gráfico 14. Tablero Principal (Tecniases, 2012)

ANEXO 2

Gráfico 15. Tablero de By Pass (LASER CENTRO DE MANTENIMIENTO ELÉCTRICO, 2015)

ANEXO 3



Gráfica 16. Red eléctrica de data center. (PowerHost Data Center, 2016)

ANEXO 4

Gráfico 17. Generador eléctrico. (Jack Power, 2016)

ANEXO 5

Gráfico 18. Tablero de transferencia automática (Emerson Network Power, 2016)

ANEXO 6

Gráfico 19. UPS (Indeo, 2016)

ANEXO 7

Gráfico 20. Aire acondicionado de precisión. (AMPER, 2016)

ANEXO 8

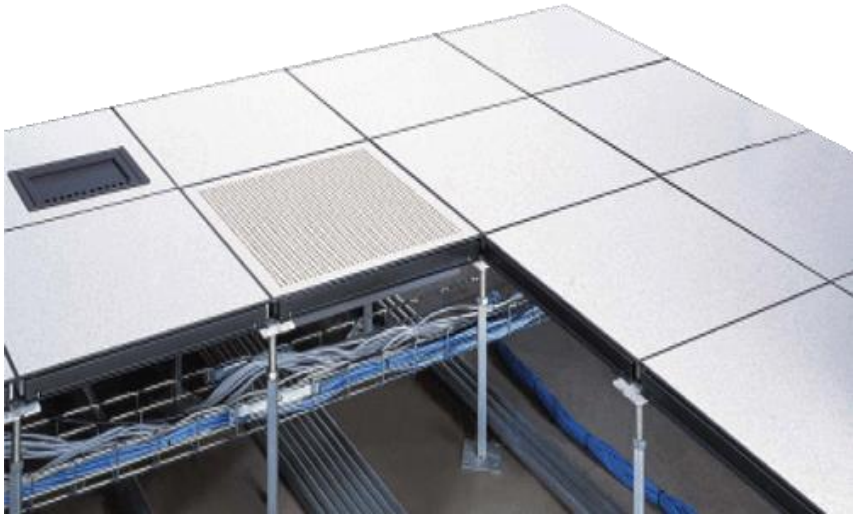


Gráfico 21. Piso falso (IAN Ingeniería Aplicada del Norte, 2016)

ANEXO 9

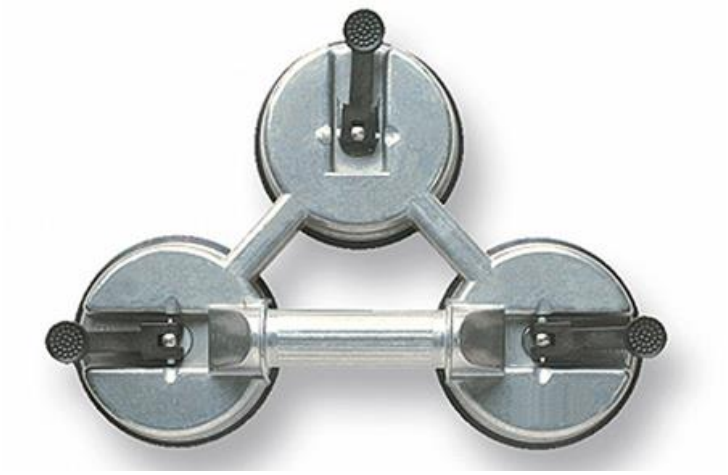


Gráfico 22. Ventosa (ALCAGLAS, 2015)

ANEXO 10

Gráfico 23. Paso de cables (Mink Bursten, 2015)

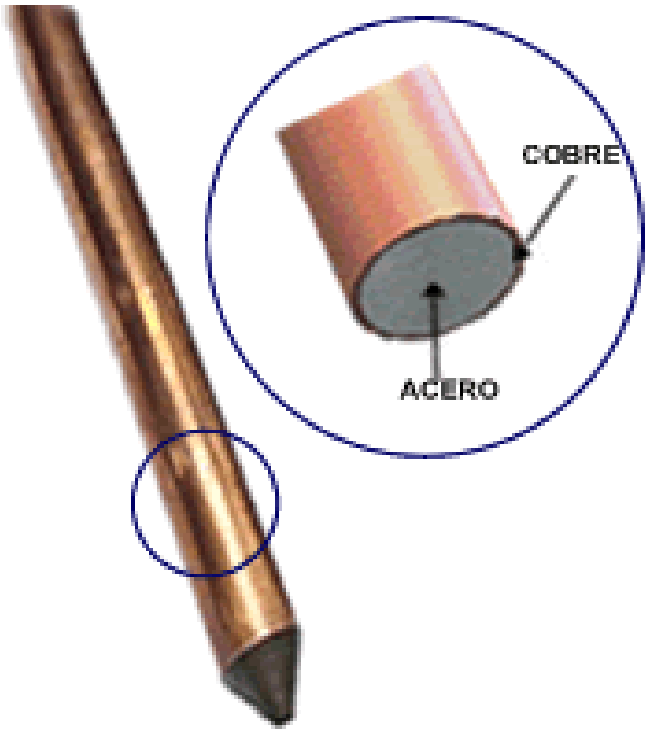
ANEXO 11

Gráfico 24. Malla de alta frecuencia (Innovación Energética Inga, 2013)

ANEXO 12

Gráfico 25. Abrazadera para aterrizaje de pedestales (Panduit, 2014)

ANEXO 13



Grafica 26. Varillas de cobre para la puesta de tierra (Decomsa, 2015)

ANEXO 14

Gráfico 27. Pintura antiestática (ElectrostatEx, 2012)

ANEXO 15

Grafica 28. Cableado (Google, 2016)

ANEXO 16

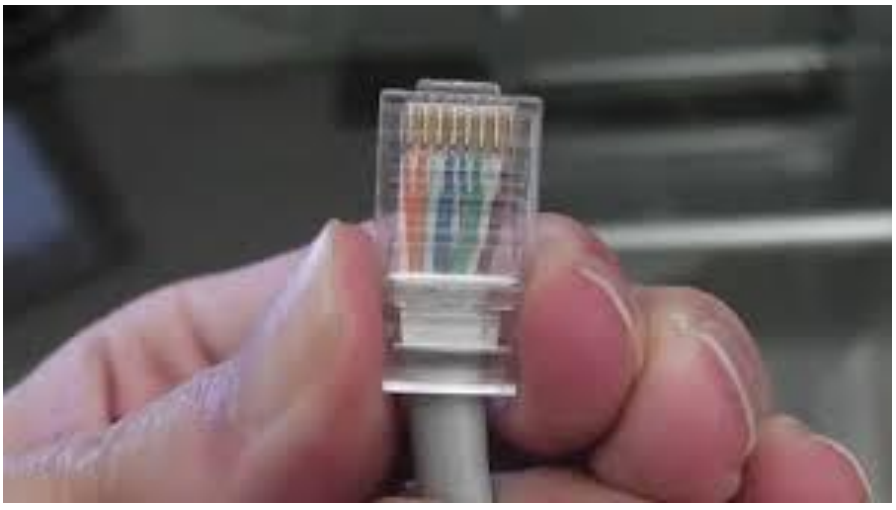


Grafico 29. Puntos de cobre (AlambrixIT, 2012)

ANEXO 17

Grafico 30. Racks (Telepartes, 2012)

ANEXO 18

Grafico 31. Fibra óptica (FibreMex, 2916)

ANEXO 19

Grafico 32. Canaletas (Casa Navia, 2014)

ANEXO 20

Grafico 33. Sistema biométrico (Artilec, 2015)

ANEXO 21

Grafico 34. Unidad de monitoreo ambiental (AreaData, 2015)

ANEXO 22

Gráfico 35. Sistema inteligente detección de incendio (SCI Seguridad Contra Incendios, 2016)

ANEXO 23

Grafico 36. Sistema de video vigilancia (ELECYTEL S.A.C., 2015)

ANEXO 24

Grafico 37. Puerta de seguridad contra incendio (ACECO TI, 2013)

ANEXO 25

PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR SEDE EN ESMERALDAS

ESCUELA DE INGENIERÍA EN SISTEMAS Y COMPUTACIÓN

Guía Para Entrevista Jefe Del Departamento De TIC´S

Proyecto de Tesis: *"Gestión de Riesgo del Data Center de la PUCESE basada en estándares internacionales"*

Objetivo: Identificar la gestión administrativa del data center de la PUCESE.

a. **¿Cómo está estructurado el departamento?**

b. **Por favor indique los nombres de cada uno de los encargados de las áreas.**

c. **¿Qué procesos administrativos se deben seguir en el departamento relacionados con el Data Center?**

d. **¿El departamento cuenta con un plan estratégico de TI?**

e. **¿Se cuenta con un plan operativo?**

ANEXO 26

PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR SEDE EN ESMERALDAS

ESCUELA DE INGENIERÍA EN SISTEMAS Y COMPUTACIÓN

Guía Para Entrevista Responsable del Data Center

Proyecto de Tesis: *"Gestión de Riesgo del Data Center de la PUCESE basada en estándares internacionales"*

Objetivo: Reconocer las vulnerabilidades de los recursos tecnológicos disponibles en el data center de la PUCESE.

1. **¿El ambiente del cuarto de telecomunicaciones cuenta con un ambiente físico apropiado para su buen funcionamiento?**

2. **¿Cuántas personas se encuentran registrados para ingresar al data center?**

3. **¿Se cumple con las normas o estándares en el data center de la PUCESE?**

4. **¿Cómo se podría mejorar la situación actual del Data center en la PUCESE?**

5. **¿En el plan de tratamiento de riesgo se ha contemplado al Data Center?**

ANEXO 27

PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR SEDE EN ESMERALDAS

ESCUELA DE INGENIERÍA EN SISTEMAS Y COMPUTACIÓN

Guía Para Entrevista Encargado Redes y Comunicaciones

Proyecto de Tesis: *"Gestión de Riesgo del Data Center de la PUCESE basada en estándares internacionales"*

Objetivo: Reconocer las vulnerabilidades de los recursos tecnológicos disponibles en el data center de la PUCESE.

1. **¿El Data Center con qué sistemas cuenta?**

2. **¿De los recursos tecnológicos de su área que se encuentran en el Data Center han sufrido algún inconveniente en su funcionamiento?**

3. **¿Se tiene algún nivel de seguridad para el acceso?**

4. **¿Para qué actividades del Data center la PUCESE ha contratado a terceros?**

ANEXO 28

PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR SEDE EN ESMERALDAS

ESCUELA DE INGENIERÍA EN SISTEMAS Y COMPUTACIÓN

Guía Para Entrevista Encargado Desarrollo de Software

Proyecto de Tesis: *"Gestión de Riesgo del Data Center de la PUCESE basada en estándares internacionales"*

Objetivo: Reconocer las vulnerabilidades de los recursos tecnológicos disponibles en el data center de la PUCESE.

1. **¿El Data Center con qué sistemas cuenta?**

2. **¿De los recursos tecnológicos de su área que se encuentran en el Data Center han sufrido algún inconveniente en su funcionamiento?**

3. **¿Se tiene algún nivel de seguridad para el acceso?**

4. **¿Para qué actividades del Data center la PUCESE ha contratado a terceros?**

ANEXO 29

PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR SEDE EN ESMERALDAS

ESCUELA DE INGENIERÍA EN SISTEMAS Y COMPUTACIÓN

Guía Para Entrevista Encargado del Área de Soporte Técnico

Proyecto de Tesis: *"Gestión de Riesgo del Data Center de la PUCESE basada en estándares internacionales"*

Objetivo: Reconocer las vulnerabilidades de los recursos tecnológicos disponibles en el data center de la PUCESE.

1. **¿El Data Center con qué sistemas cuenta?**

2. **¿De los recursos tecnológicos de su área que se encuentran en el Data Center han sufrido algún inconveniente en su funcionamiento?**

3. **¿Por qué se dio esa eventualidad del reinicio del equipo de los estudiantes?**

4. **¿Se tiene algún nivel de seguridad para el acceso?**

5. **¿Para qué actividades del Data center la PUCESE ha contratado a terceros?**

ANEXO 30

PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR SEDE EN ESMERALDAS

ESCUELA DE INGENIERÍA EN SISTEMAS Y COMPUTACIÓN

GUIA PARA ENCUESTA Usuarios de Servicios Web PUCESE

Proyecto de Tesis: *"Gestión de Riesgo del Data Center de la PUCESE basada en estándares internacionales"*

Objetivo: Identificar a las funciones de los usuarios del servicio web que ofrece el data center de la PUCESE.

Reciba un cordial saludo, actualmente estoy desarrollando mi proyecto de tesis y le pido su colaboración con la siguiente encuesta.

1.- ¿Qué tipo de usuario es?

a) Docente
c) Trabajadores Administrativos ☐

2.- ¿Cuan satisfecho está Ud. con el servicio de red que ofrece la PUCESE?

RED LAN

a) Muy Satisfecho
b) Satisfecho
c) Insatisfecho ☐

RED INALÁMBRICA

a) Muy Satisfecho
b) Satisfecho
c) Insatisfecho ☐

3.- Si usa los servicios web que brinda la PUCESE, por favor indique cuál de la lista a continuación:

Correo institucional ☐
Web administrativos
Administración del proceso de inscripciones y admisiones ☐
Auxiliares académicas ☐
Evaluación académica para docentes
Evaluación académica para directores de escuela ☐
PEDI
Practicas estudiantes

Sistema académico para nivelación ☐
Web directivos
Web docentes ☐
Evaluación para dirección académica
Evaluación académica para estudiantes ☐
Sistema Urkund
Facturación electrónica ☐
Aula virtual
Antivirus ☐

4.- ¿De los servicios web que usted utilizada, cuánta información cree se ha perdido?

ada ☐
Muy poco ☐
Poco ☐
Mucho ☐
Toda ☐

5.- Los servicios web están disponibles:

Nunca ☐
A veces ☐
Siempre ☐

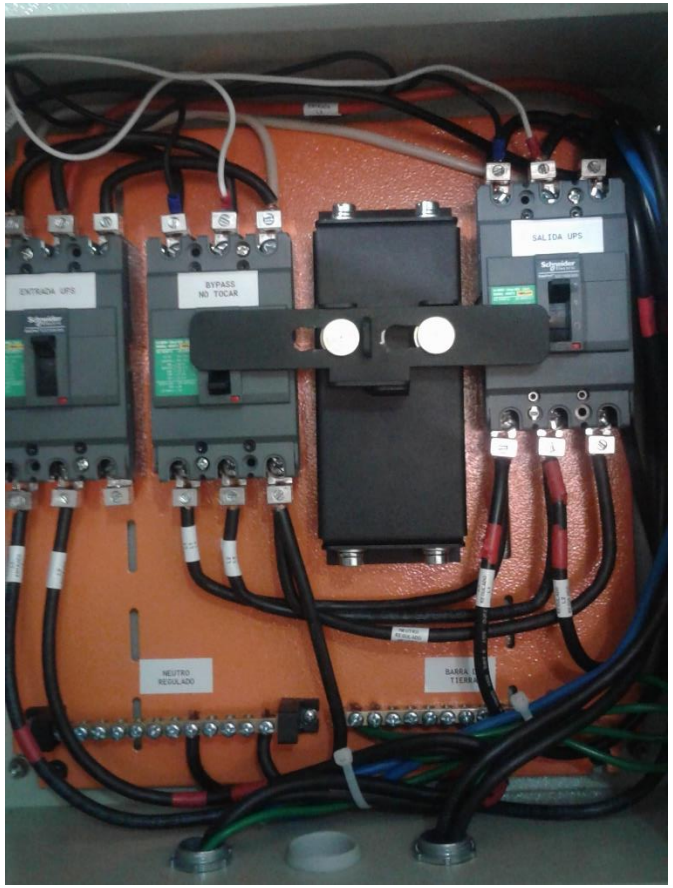
6.- ¿La información que provee a los servicios web cree usted que se encuentra protegida?

Si ☐
No ☐

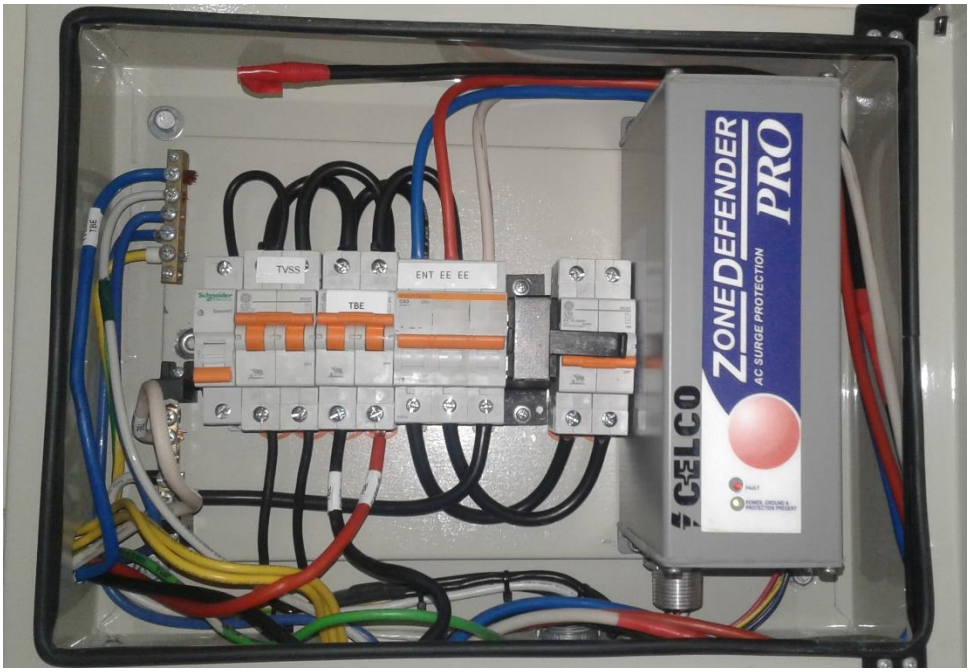
Gracias por su comprensión.

ANEXO 31: Tablero principal

ANEXO 32: Tablero de bypass



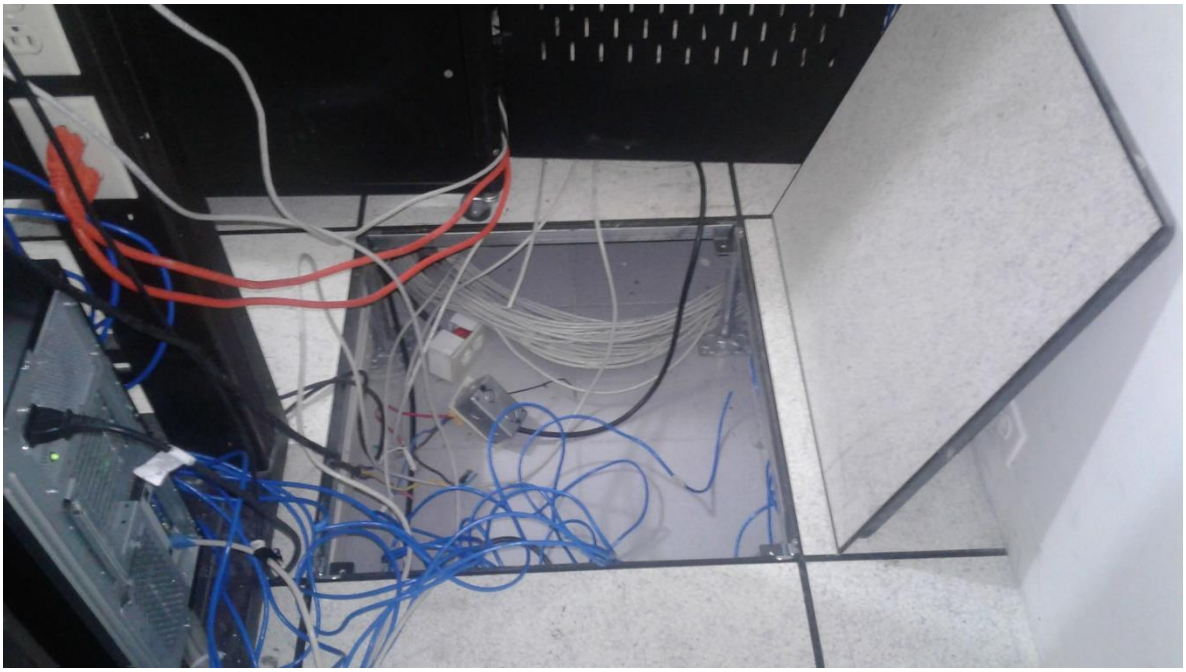
ANEXO 33: TABLERO DE DISTRIBUCIÓN REGULADA

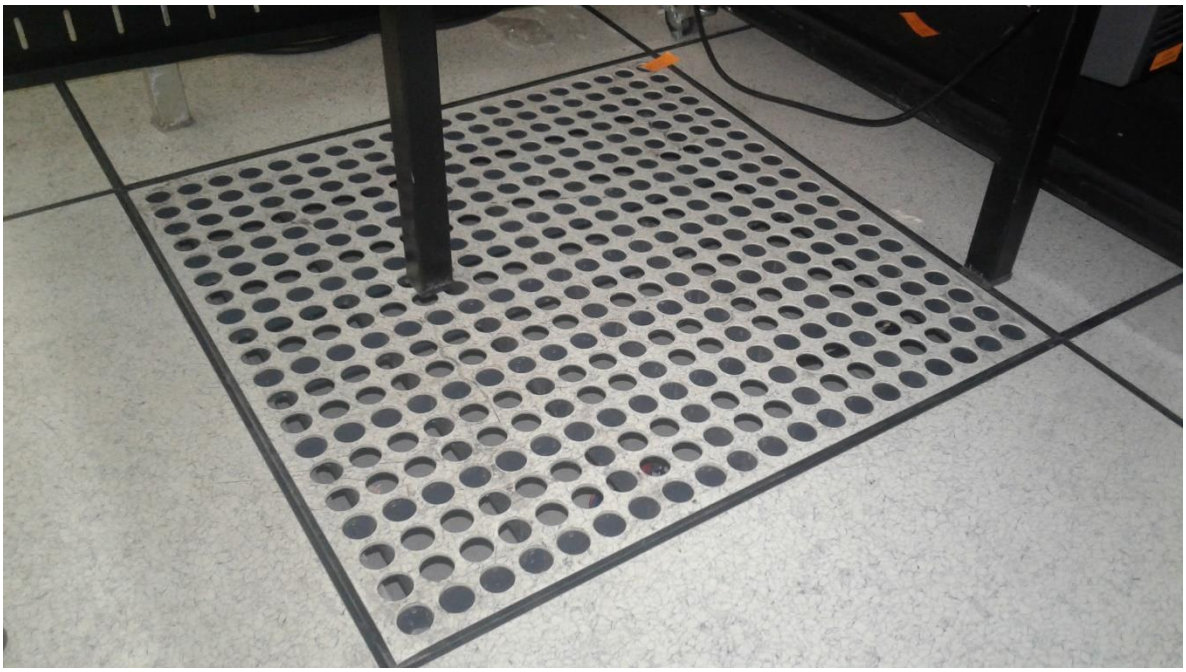


ANEXO 34: UPS

ANEXO 35: AIRE ACONDICIONADO

ANEXO 36: PISO FALSO





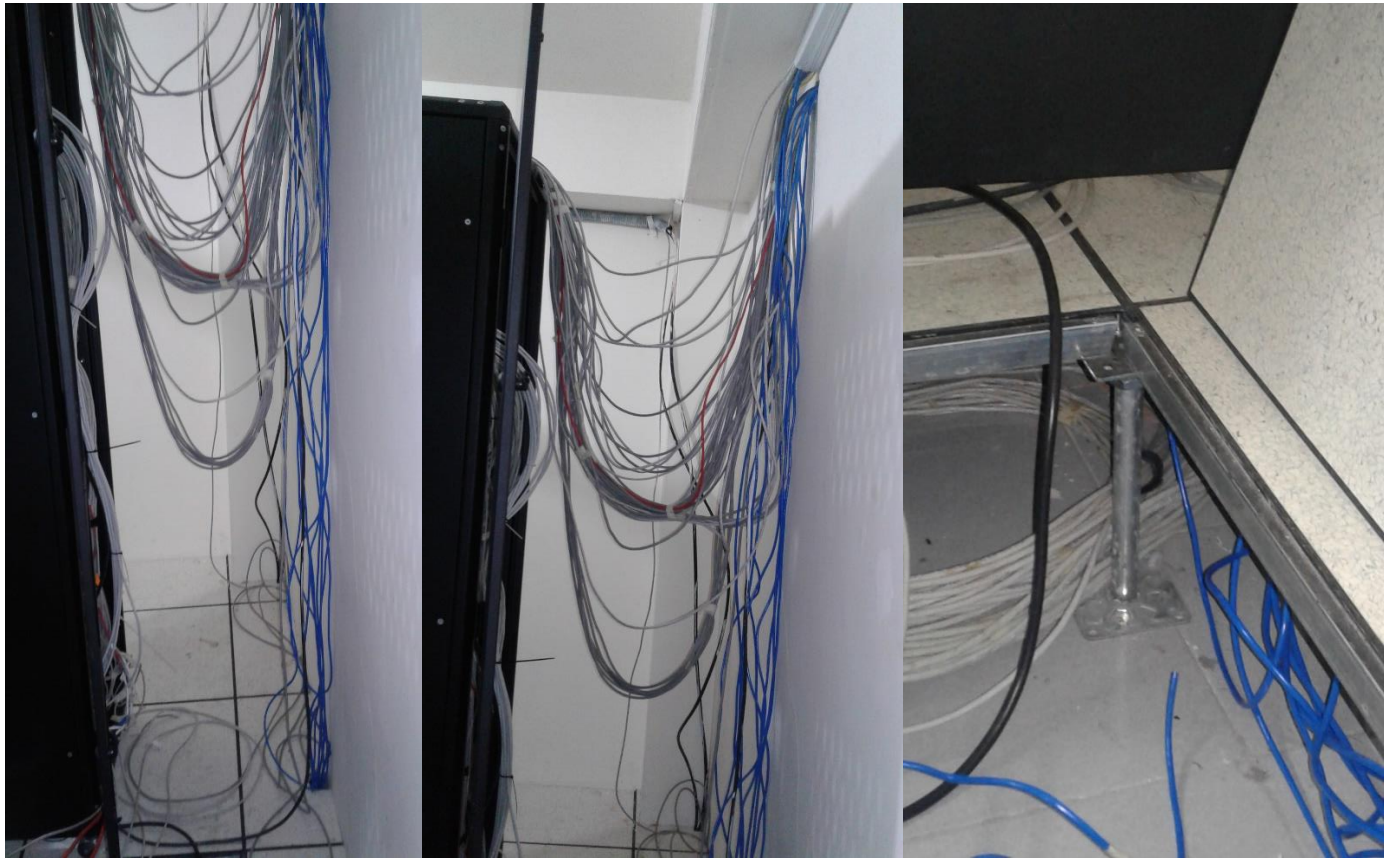
ANEXO 37: VENTOSA

ANEXO 38: HERMETIZACIÓN PASO DE CABLES

ANEXO 39: MALLA DE ALTA FRECUENCIA

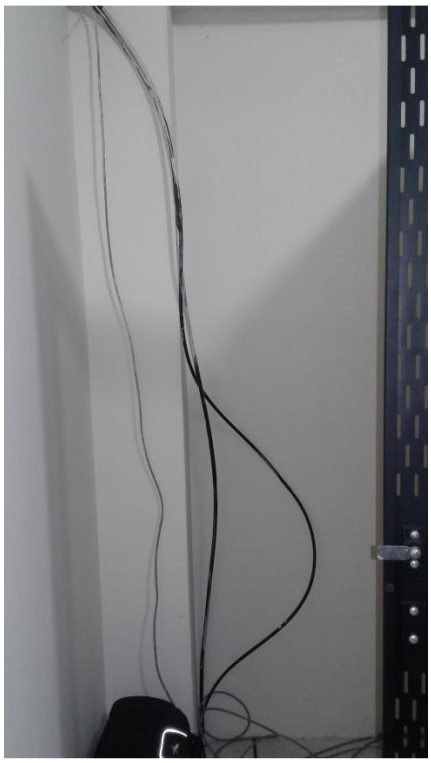
ANEXO 40: SISTEMA DE PUESTA A TIERRA

ANEXO 41: CABLEADO



ANEXO 42: RACKS

ANEXO 43: FIBRA ÓPTICA



ANEXO 44: SISTEMA DE CONTROL DE ACCESO

ANEXO 45: SISTEMA DE DETECCIÓN Y EXTINCION DE INCENDIOS

ANEXO 46: SISTEMA DE VIDEOSEGURIDAD

ANEXO 47: PUERTA DE SEGURIDAD

ANEXO 48: RESPALDO DE BASE DE LOS SERVIDORES

ANEXO 49: INFORMES MONITOREO

Site24x7 - Availability Summary Report

2 de mayo de 2016 0:00 ECT hasta 9 de mayo de 2016 18:00 ECT

Site24x7

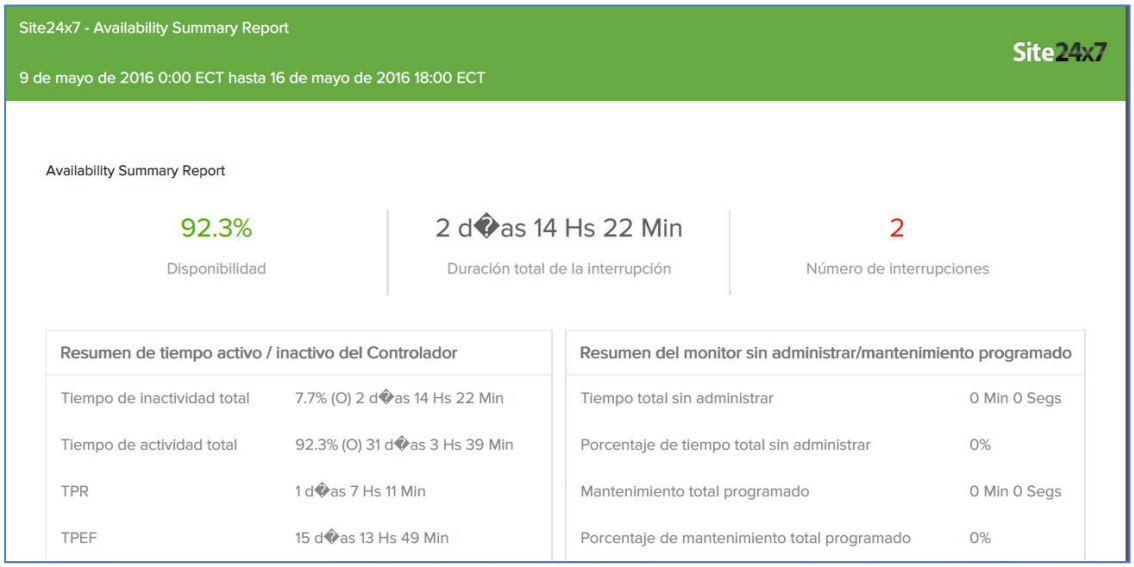
Availability Summary Report

100%	0 Min 0 Segs	0
Disponibilidad	Duración total de la interrupción	Número de interrupciones

Resumen de tiempo activo / inactivo del Controlador	
Tiempo de inactividad total	0% (O) 0 Min 0 Segs
Tiempo de actividad total	100% (O) 4 d&#65533;as 9 Hs 39 Min
TPR	0 Min 0 Segs
TPEF	4 d&#65533;as 9 Hs 39 Min

Resumen del monitor sin administrar/mantenimiento programado	
Tiempo total sin administrar	0 Min 0 Segs
Porcentaje de tiempo total sin administrar	0%
Mantenimiento total programado	0 Min 0 Segs
Porcentaje de mantenimiento total programado	0%

Tendencia de porcentajes de disponibilidad



Site24x7 - Availability Summary Report

9 de mayo de 2016 0:00 ECT hasta 16 de mayo de 2016 18:00 ECT

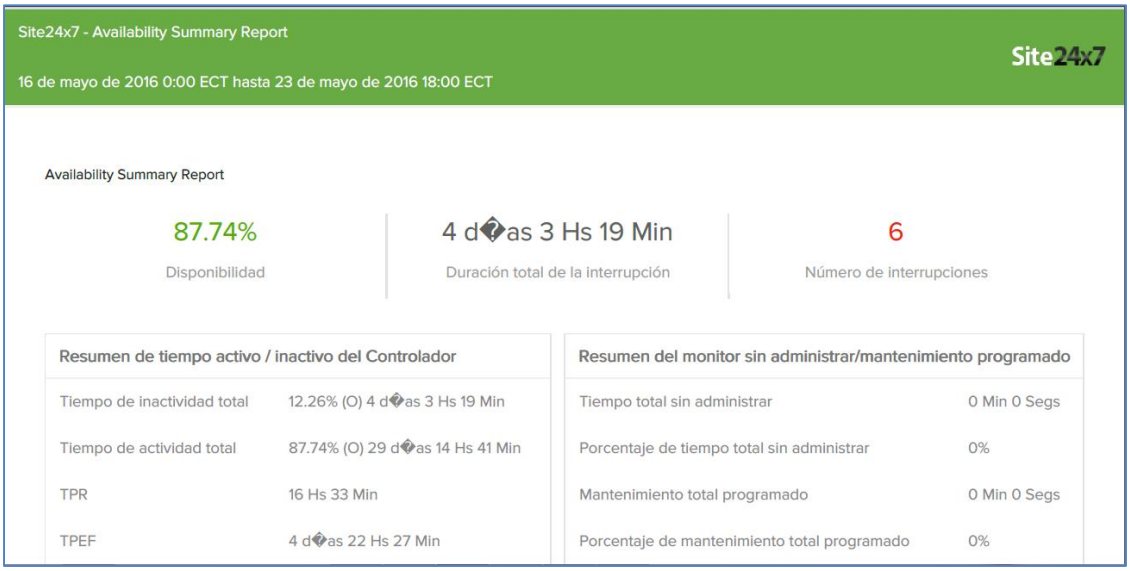
Site24x7

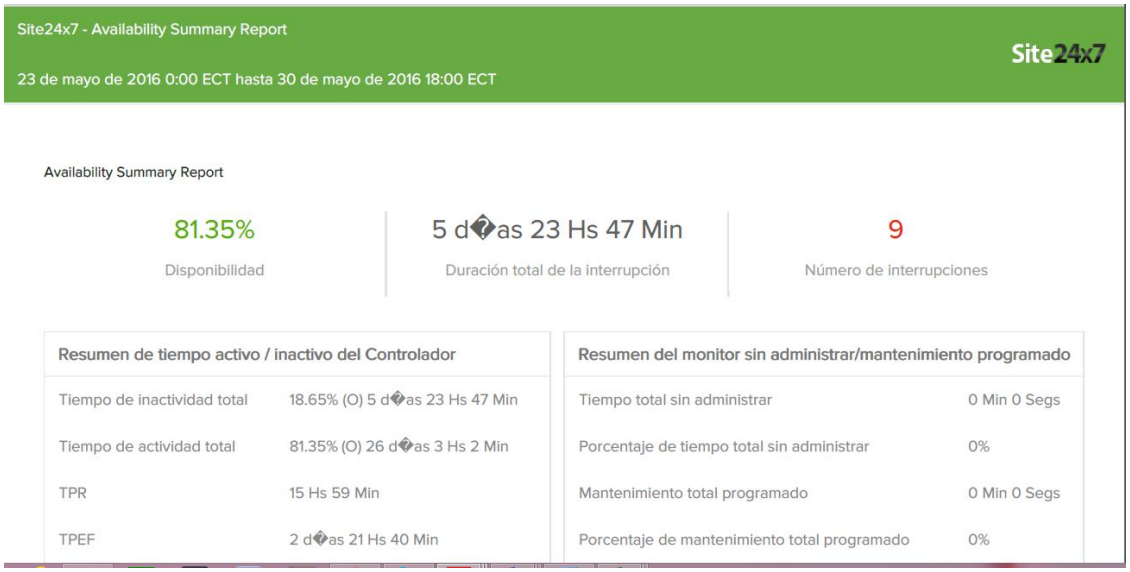
Availability Summary Report

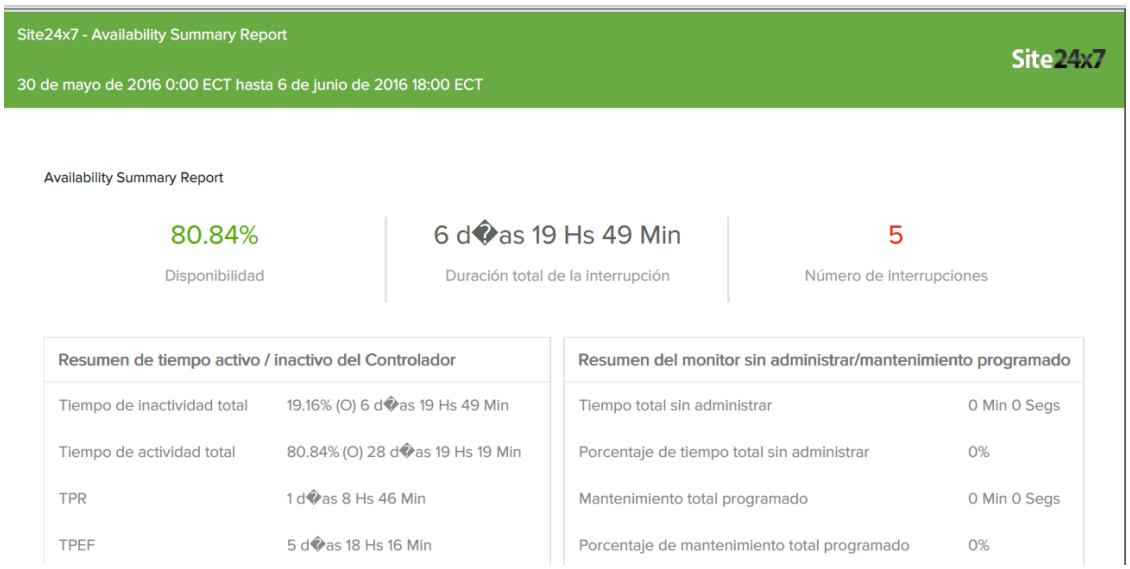
92.3%	2 d&#65533;as 14 Hs 22 Min	2
Disponibilidad	Duración total de la interrupción	Número de interrupciones

Resumen de tiempo activo / inactivo del Controlador	
Tiempo de inactividad total	7.7% (O) 2 d&#65533;as 14 Hs 22 Min
Tiempo de actividad total	92.3% (O) 31 d&#65533;as 3 Hs 39 Min
TPR	1 d&#65533;as 7 Hs 11 Min
TPEF	15 d&#65533;as 13 Hs 49 Min

Resumen del monitor sin administrar/mantenimiento programado	
Tiempo total sin administrar	0 Min 0 Segs
Porcentaje de tiempo total sin administrar	0%
Mantenimiento total programado	0 Min 0 Segs
Porcentaje de mantenimiento total programado	0%


Site24x7 - Availability Summary Report
16 de mayo de 2016 0:00 ECT hasta 23 de mayo de 2016 18:00 ECT
Site24x7
Availability Summary Report
87.74%
Disponibilidad
4 d&#65533;as 3 Hs 19 Min
Duración total de la interrupción
6
Número de interrupciones
Resumen de tiempo activo / inactivo del Controlador
Tiempo de inactividad total 12.26% (O) 4 d&#65533;as 3 Hs 19 Min
Tiempo de actividad total 87.74% (O) 29 d&#65533;as 14 Hs 41 Min
TPR 16 Hs 33 Min
TPEF 4 d&#65533;as 22 Hs 27 Min
Resumen del monitor sin administrar/mantenimiento programado
Tiempo total sin administrar 0 Min 0 Segs
Porcentaje de tiempo total sin administrar 0%
Mantenimiento total programado 0 Min 0 Segs
Porcentaje de mantenimiento total programado 0%


Site24x7 - Availability Summary Report
23 de mayo de 2016 0:00 ECT hasta 30 de mayo de 2016 18:00 ECT
Site24x7
Availability Summary Report
81.35%
Disponibilidad
5 d&#65533;as 23 Hs 47 Min
Duración total de la interrupción
9
Número de interrupciones
Resumen de tiempo activo / inactivo del Controlador
Tiempo de inactividad total 18.65% (O) 5 d&#65533;as 23 Hs 47 Min
Tiempo de actividad total 81.35% (O) 26 d&#65533;as 3 Hs 2 Min
TPR 15 Hs 59 Min
TPEF 2 d&#65533;as 21 Hs 40 Min
Resumen del monitor sin administrar/mantenimiento programado
Tiempo total sin administrar 0 Min 0 Segs
Porcentaje de tiempo total sin administrar 0%
Mantenimiento total programado 0 Min 0 Segs
Porcentaje de mantenimiento total programado 0%


Site24x7 - Availability Summary Report
30 de mayo de 2016 0:00 ECT hasta 6 de junio de 2016 18:00 ECT
Site24x7
Availability Summary Report
80.84%
Disponibilidad
6 d&#65533;as 19 Hs 49 Min
Duración total de la interrupción
5
Número de interrupciones
Resumen de tiempo activo / inactivo del Controlador
Tiempo de inactividad total
19.16% (O) 6 d&#65533;as 19 Hs 49 Min
Tiempo de actividad total
80.84% (O) 28 d&#65533;as 19 Hs 19 Min
TPR
1 d&#65533;as 8 Hs 46 Min
TPEF
5 d&#65533;as 18 Hs 16 Min
Resumen del monitor sin administrar/mantenimiento programado
Tiempo total sin administrar
0 Min 0 Segs
Porcentaje de tiempo total sin administrar
0%
Mantenimiento total programado
0 Min 0 Segs
Porcentaje de mantenimiento total programado
0%

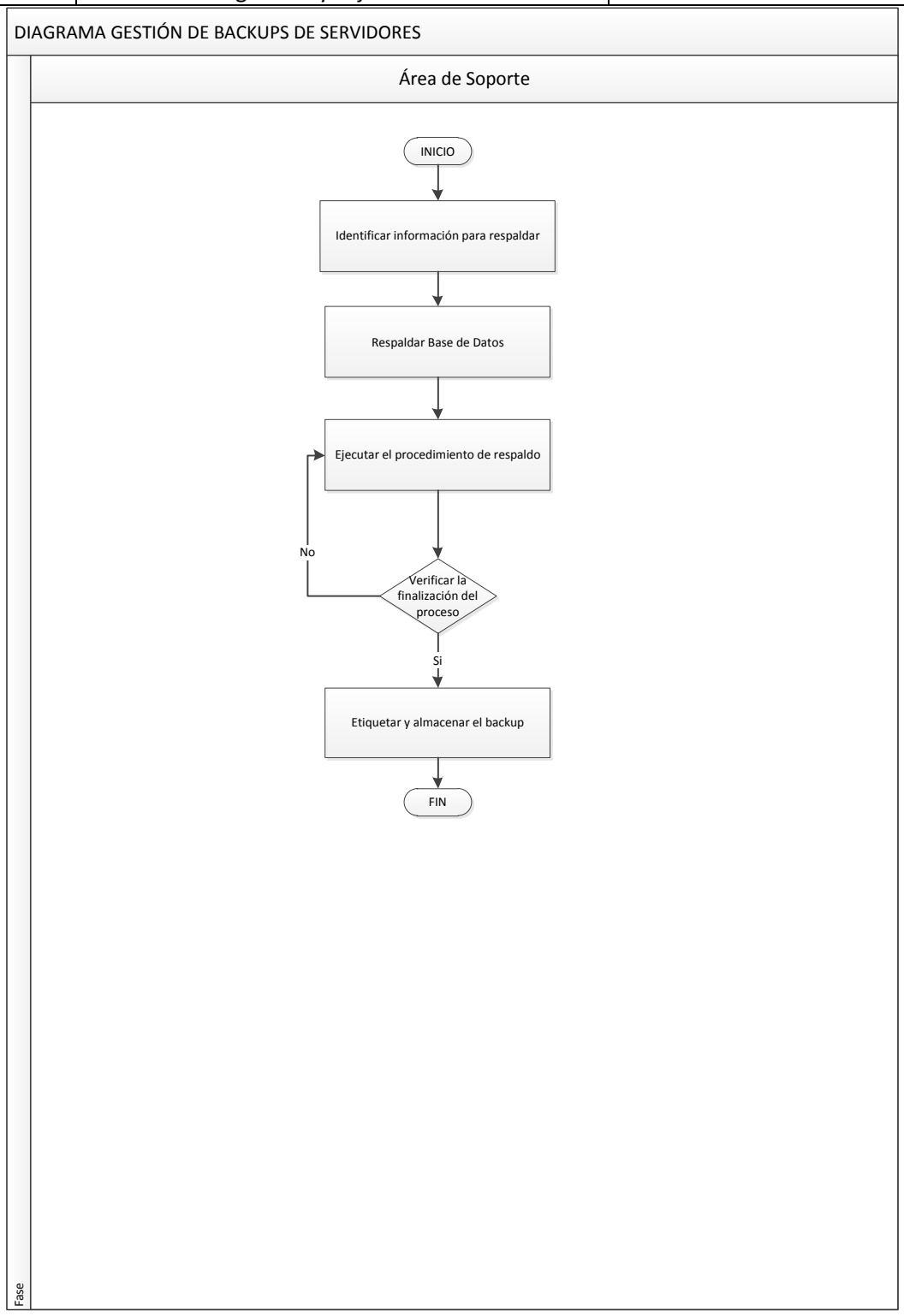
ANEXO 50: POLÍTICAS

	PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR	Manual de Procedimientos
	Proceso: Gestión de Backups de Servidores	
Nº Revisión: 00		

DESCRIPCIÓN DEL PROCEDIMIENTO:	
Nombre:	Gestión de Backups de Servidores
Objetivo:	Este procedimiento respalda la información de los aplicativos institucionales que están bajo la responsabilidad del Departamento de Tics.
Alcance:	
Frecuencia:	Semanalmente

Actividad	Descripción	Responsables
1	IDENTIFICAR INFORMACIÓN PARA RESPALDAR: El tipo de información se identifica por: - Servidor. En este caso, se identifican los archivos o particiones que se van a respaldar. Se continúa con la actividad 3. - Aplicación. En este caso se identifica si es la aplicación o los datos de la aplicación son los que se van a respaldar. - Si el respaldo es de aplicación, se continúa con la actividad 3. - Si el respaldo es de las bases de datos, se continúa con la actividad 2.	Área de Infraestructura y Servidores
2	RESPALDAR BASES DE DATOS: Se respaldan diariamente mediante la herramienta de backup del Administrador de Bases de Datos. Nota: Este respaldo se realiza en disco duro o medios magnéticos. Fin de procedimiento.	
3	EJECUTAR EL PROCEDIMIENTO DE RESPALDO: Se ejecuta el respaldo de la información.	
4	VERIFICAR LA FINALIZACIÓN DEL PROCESO: Si el proceso finaliza exitosamente, continuar con la siguiente actividad, de lo contrario y basado en el error reportado:	

	Reiniciar el proceso punto 1.	
5	ETIQUETAR Y ALMACENAR: Se especifica a que servidor o aplicación se le realizó el backup con la fecha en que se realizó. Almacenar en gavetas y caja fuerte.	



1. PROPÓSITO

Salvaguardar la información generada por los diferentes departamentos de la PUCESE, para contar con la información en caso de contingencia o desastre.

2. ALCANCE

Personal Administrativo y docentes investigadores de la PUCESE que contengan información propia de sus funciones o actividades encomendadas en los servidores del Departamento de TIC.

3. RESPONSABLE

Administrador de Servidores

4. DEFINICIONES

- **Conjunto de copias de seguridad:** Conjunto de archivos, carpetas y demás datos a los que se ha realizado una copia de seguridad y se ha almacenado en un archivo o en uno o varios medios (cintas, disquetes, DVD).
- **Métodos de copias de seguridad:** Es la la forma en que se realizara la copia y su tipo, define el medio que se utiliza para resguardar un grupo o conjunto de archivos de datos.
- **Servidor:** es un nodo que forma parte de una red, provee servicios a otros nodos denominados cliente. Puede ser un equipo de cómputo tradicional o un supercomputador.

Responsable del Proceso	Responsable de Gestión por Procesos	Jefe de Unidad
Fecha:	Fecha:	Fecha:

PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR SEDE ESMERALDAS	MANUAL DE PROCEDIMIENTOS
CODIGO MSO-10	Proceso: Respaldo y recuperación de archivos

5. POLÍTICAS

- El propietario de la información debe presentar por escrito la periodicidad y la información que deberá respaldar y el tiempo que se deberá conservar los respaldos.
- La aprobación de las solicitudes de respaldo está a cargo del Administrador de Servidores, con el aval del Líder en Redes y Telecomunicaciones (quien determina el método de copia).
- Para la restauración de la información respaldada, el propietario, deberá solicitar el servicio mediante la mesa de ayuda.
- Por cada respaldo, se debe realizar un informe técnico dirigido al Líder en Redes y Telecomunicaciones para su revisión y aprobación.

Métodos de copia

- Copia de seguridad normal: una copia de seguridad normal incluye todos los archivos seleccionados y pone a cada archivo una marca que indica que se ha hecho una copia de seguridad del mismo. En las copias de seguridad normales solo necesita la copia de seguridad mas reciente del archivo o la cinta que contiene la copia de seguridad para restaurar todos los archivos. Las copias de seguridad normales se suelen realizar al crear por primera vez un conjunto de copia.
- Copia de seguridad diaria: una copia de seguridad diaria incluye todos los archivos seleccionados que se hayan modificado el día en que se realizo la copia. Los archivos incluidos en la copia de seguridad no se marcan como tales.
- Copia de seguridad incremental: Una copia de seguridad incremental solo copia los archivos creados o modificados desde la última copia de seguridad normal o incremental. Marca los archivos como copiados

Responsable del Proceso	Responsable de Gestión por Procesos	Jefe de Unidad
Fecha:	Fecha:	Fecha:

6. INDICADORES

Código	Nombre			
Descripción				
Formula de calculo	Frecuencia	Estándar	Responsable del indicador	Responsable del análisis

7. DOCUMENTOS

Código	Nombre
MSO-S1	Solicitud de Acceso a recursos de red

Responsable del Proceso	Responsable de Gestión por Procesos	Jefe de Unidad
Fecha:	Fecha:	Fecha:

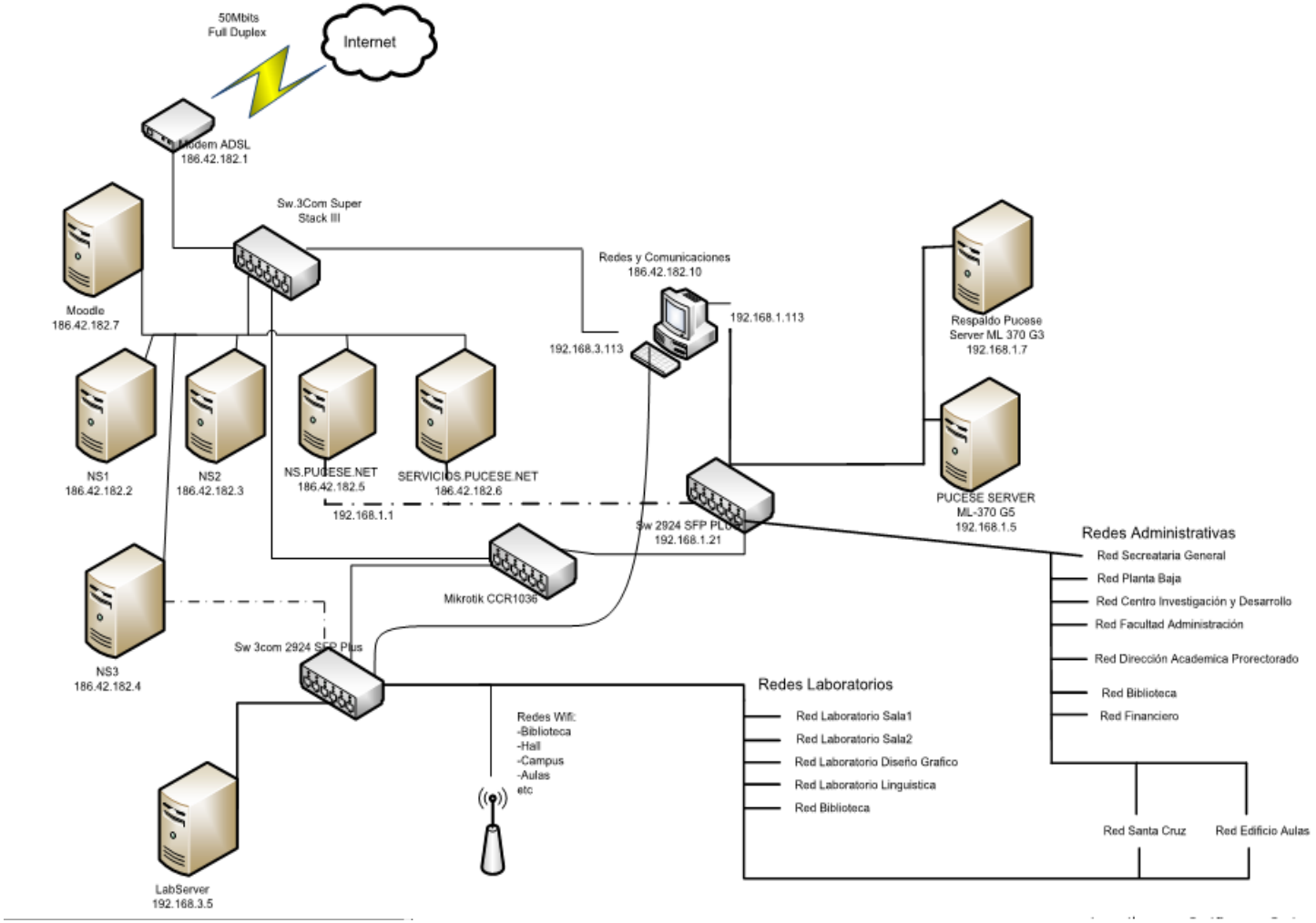


Grafico 38. Nivel 0 del Data Center PUCESE

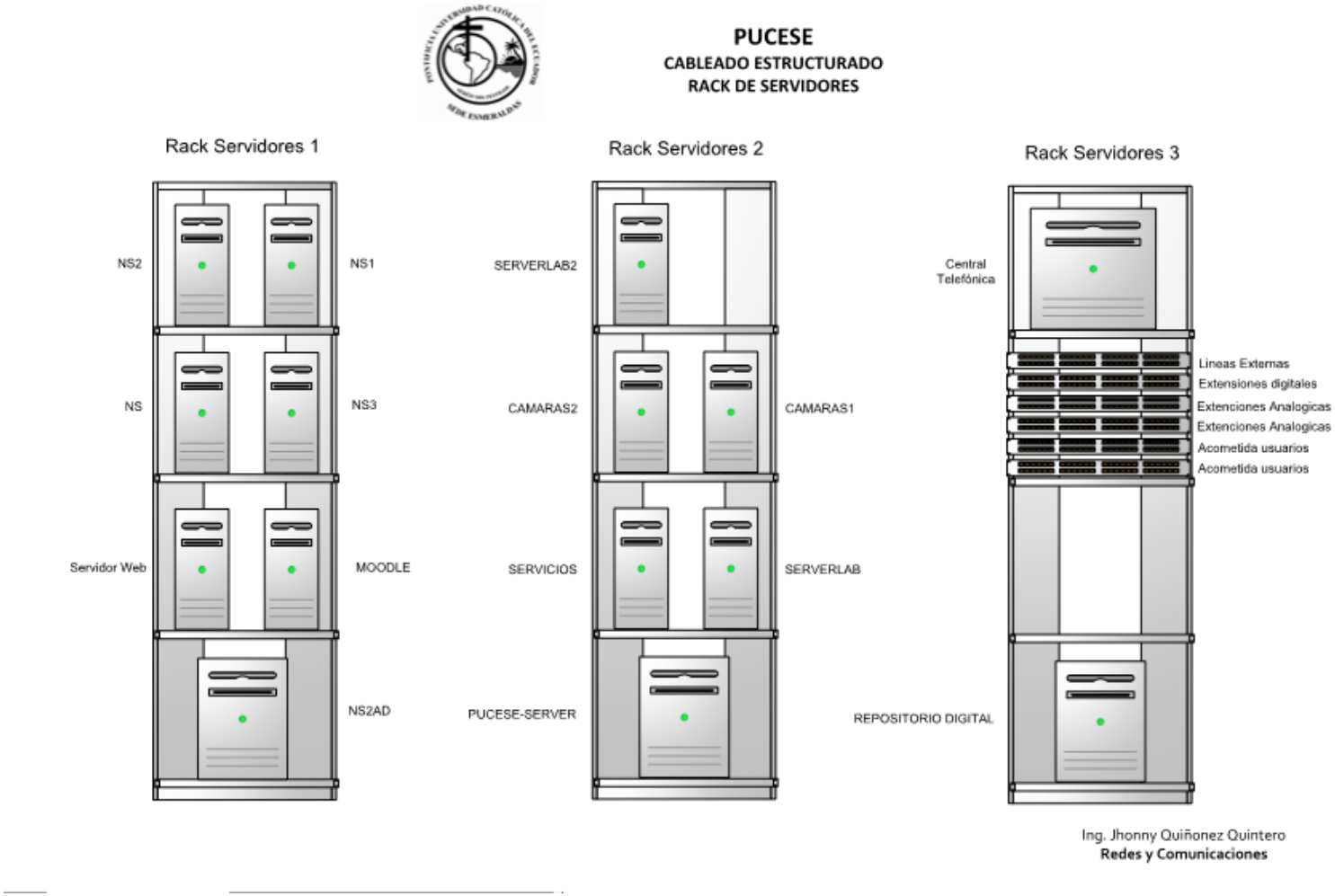


Gráfico 39. Rack Servidores Data Center PUCESE

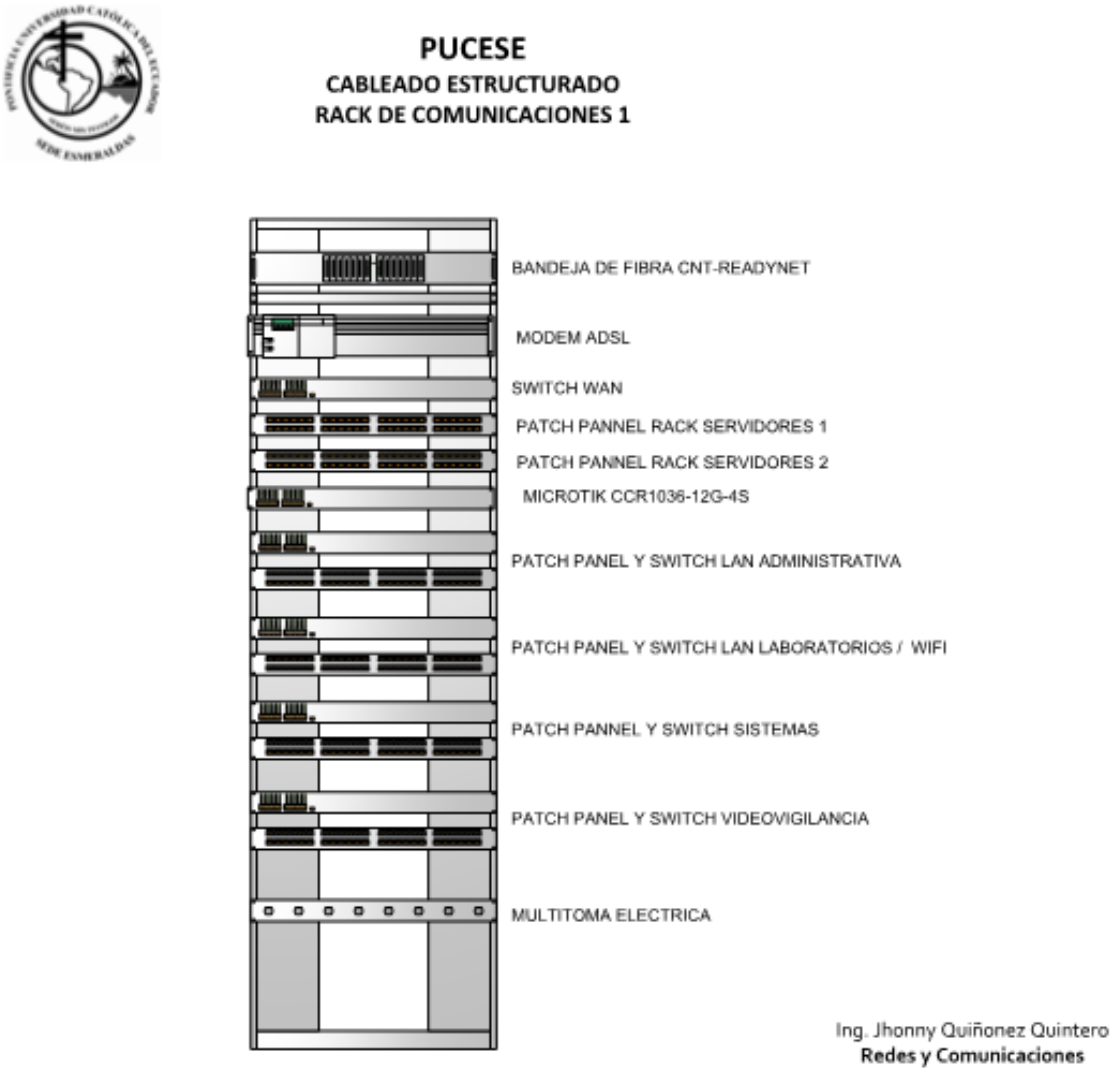


Grafico 40. Rack Comunicaciones Data Center PUCESE

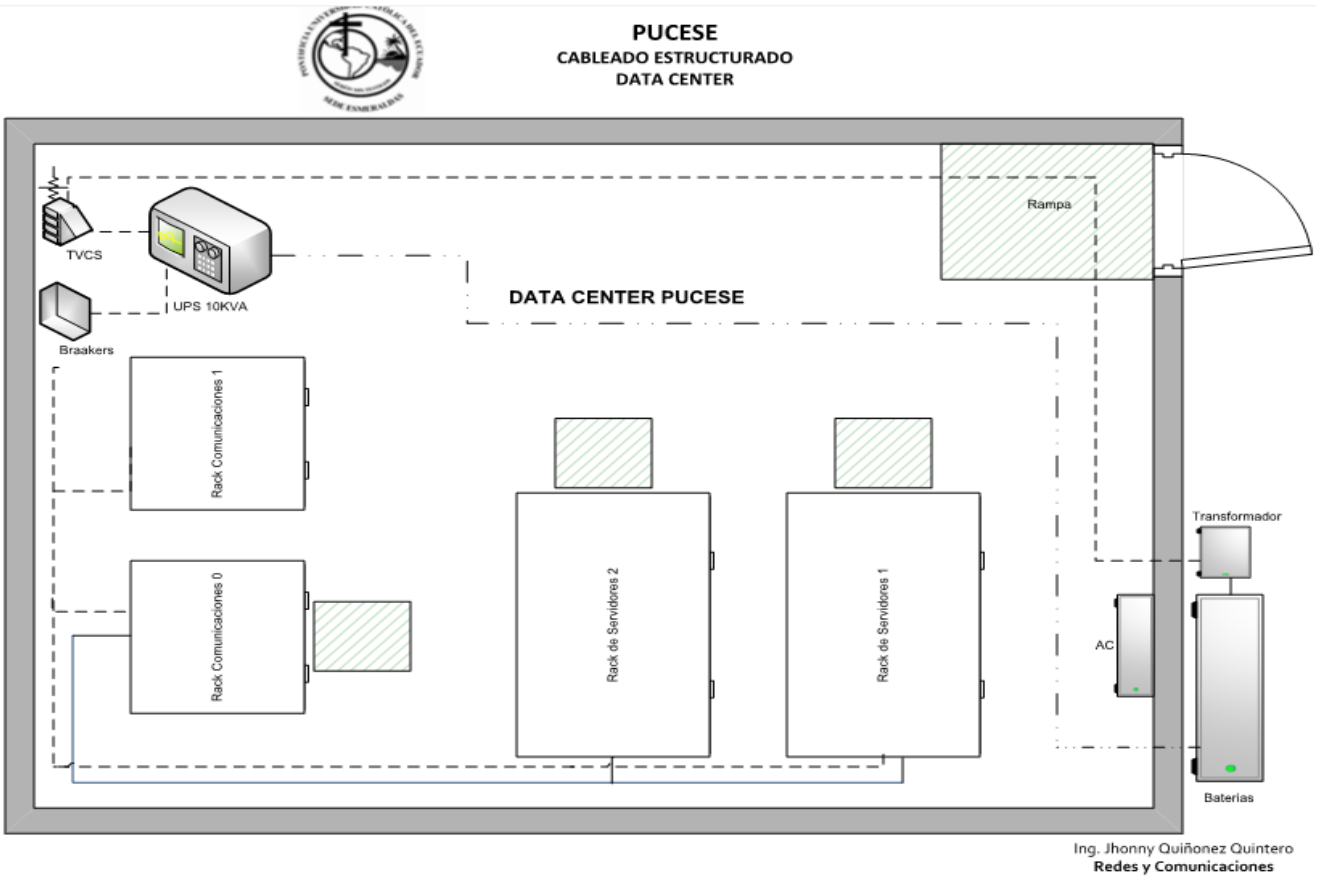


Grafico 41. Cableado Estructurado PUCESE