UNIVERSIDAD DE LAS FUERZAS ARMADAS ESPE

UNIDAD DE GESTIÓN DE TECNOLOGÍAS

DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN

TRABAJO DE TITULACIÓN, PREVIO A LA OBTENCIÓN DEL TÍTULO DE TECNÓLOGA EN COMPUTACIÓN

TEMA:

“ANÁLISIS Y EVALUACIÓN DE RIESGOS DE SEGURIDAD INFORMÁTICA EN LA RED DE ÁREA LOCAL (LAN), DE LA UNIDAD DE GESTIÓN DE TECNOLOGÍAS ESPE, PARA PERMITIR ESTABLECER UN PLAN DE DEFENSA Y PROTECCIÓN”

AUTOR:

ORDOÑEZ VEINTIMILLA DIANA JAZMÍN

DIRECTOR:

ING. MOLINA PATRICIO

LATACUNGA

2019

UNIVERSIDAD DE LAS FUERZAS ARMADAS ESPE

UNIDAD DE GESTIÓN DE TECNOLOGÍAS

DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN

CERTIFICACIÓN

Certifico que el trabajo de titulación, "**ANÁLISIS Y EVALUACIÓN DE RIESGOS DE SEGURIDAD INFORMÁTICA EN LA RED DE ÁREA LOCAL (LAN), DE LA UNIDAD DE GESTIÓN DE TECNOLOGÍAS - ESPE, PARA PERMITIR ESTABLECER UN PLAN DE DEFENSA Y PROTECCIÓN**" realizado por la señorita **ORDÓÑEZ VEINTIMILLA DIANA JAZMÍN**, ha sido revisado en su totalidad y analizado por el software anti-plagio, el mismo cumple con los requisitos teóricos, científicos, técnicos, metodológicos y legales establecidos por la Universidad de Fuerzas Armadas ESPE, por lo tanto, me permito acreditar y autorizar a la señorita ORDÓÑEZ VEINTIMILLA DIANA JAZMÍN, para que lo sustente públicamente.

Latacunga, 13 de Febrero del 2019

_____

SR. ING. PATRICIO ALEJANDRO MOLINA PALMA

DIRECTOR DEL TRABAJO DE GRADUACIÓN

UNIVERSIDAD DE LAS FUERZAS ARMADAS ESPE

UNIDAD DE GESTIÓN DE TECNOLOGÍAS

DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN

AUTORÍA DE RESPONSABILIDAD

Yo, **ORDÓÑEZ VEINTIMILLA DIANA JAZMÍN,** con cédula de identidad N° **0202031076**, declaro que este trabajo de titulación **"ANÁLISIS Y EVALUACIÓN DE RIESGOS DE SEGURIDAD INFORMÁTICA EN LA RED DE ÁREA LOCAL (LAN), DE LA UNIDAD DE GESTIÓN DE TECNOLOGÍAS ESPE, PARA PERMITIR ESTABLECER UN PLAN DE DEFENSA Y PROTECCIÓN"** ha sido desarrollado considerando los métodos de investigación existentes, así como también se ha respetado los derechos intelectuales de terceros considerándose en las citas bibliográficas.

Consecuentemente declaro que este trabajo es de mi autoría, en virtud de ello me declaro responsable del contenido, veracidad y alcance de la investigación mencionada.

Latacunga, 13 de Febrero del 2019

_____

ORDÓÑEZ VEINTIMILLA DIANA JAZMÍN

CI: 0202031076

UNIVERSIDAD DE LAS FUERZAS ARMADAS ESPE

UNIDAD DE GESTIÓN DE TECNOLOGÍAS

DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN

AUTORIZACIÓN

Yo, **ORDÓÑEZ VEINTIMILLA DIANA JAZMÍN,** autorizo a la Universidad de las Fuerzas Armadas ESPE publicar en la biblioteca Virtual de la institución el presente trabajo de titulación **"ANÁLISIS Y EVALUACIÓN DE RIESGOS DE SEGURIDAD INFORMÁTICA EN LA RED DE ÁREA LOCAL (LAN), DE LA UNIDAD DE GESTIÓN DE TECNOLOGÍAS ESPE, PARA PERMITIR ESTABLECER UN PLAN DE DEFENSA Y PROTECCIÓN"** cuyo contenido, ideas y criterios son de mi autoría y responsabilidad.

Latacunga, 13 de Febrero del 2019

_____

ORDÓÑEZ VEINTIMILLA DIANA JAZMÍN

CI: 0202031076

DEDICATORIA

Dedico este proyecto de titulación principalmente a Dios, por haberme dado la vida. Por los triunfos y los momentos difíciles. Por haberme permitido llegar a este momento tan importante y por cada día, darme fortaleza para continuar en mi formación tanto personal como profesional.

A mi madre Sra. Silvia Veintimilla, por su amor, quien, a lo largo de mi vida, ha velado por mi bienestar y educación, por ser mi pilar más importante, y apoyo incondicional.

A mi hermana Ing. Jenny Baño por estar siempre presente, acompañándome a lo largo de esta etapa de mi vida.

A mis maestros, por brindarme sus conocimientos y sabiduría, en cada paso de mi carrera, de la misma forma por su incondicional apoyo en el desarrollo de mi formación profesional.

AGRADECIMIENTO

Agradezco de manera principal a Dios, por cada día protegerme, por darme fuerza para poder superar cada una de las dificultades a lo largo de mi vida.

A mi madre por la confianza y el apoyo que día a día me ha brindado en lo que me he propuesto y sobre todo corrigiendo mis errores.

A mi hermana por ser una gran amiga, pero sobre todo por los momentos inolvidables que hemos vivido juntas y por ser una de las personas más importantes en mi vida.

A mis profesores por cada uno de sus conocimientos brindados a lo largo de mi carrera universitaria.

ÍNDICE DE CONTENIDOS

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

RESUMEN

El Departamento de TICs de la Unidad de Gestión de Tecnologías ESPE, requiere de un análisis y evaluación de riesgos de la red LAN, que permita mantenerlos de manera segura, proporcionando los principios básicos para la evaluación de riesgos y amenazas, en pro de la integridad, confidencialidad y disponibilidad de la información; para su desarrollo se ha utilizado la herramienta de Análisis y Gestión de Riesgos Pilar, en conjunto con la Metodología Magerit; para mostrar de manera clara, posibles amenazas, nivel de degradación, y de la misma forma obtener salvaguardas para contrarrestar los efectos de las mismas. Y a su vez la realización de un plan de defensa y protección de seguridad informática, que mediante los resultados obtenidos se pueda especificar la importancia de los activos, responsabilidades tanto del personal de las TICs, como de los usuarios en general, medidas y procedimientos en caso de amenazas; la seguridad en las operaciones, robo de equipos y seguridad en redes, estableciendo pasos para poder contrarrestar los efectos de las mismas. El mismo que servirá como un complemento para el Departamento de TICs, brindando opciones de seguridad en cuanto al manejo y uso de cada uno de los activos de la red LAN de la institución.

PALABRAS CLAVES:

- **ANÁLISIS**
- **MAGERIT**
- **PILAR**
- **METODOLOGÍA**
- **ACTIVOS**

ABSTRACT

The ICT Department of the Unidad de Gestión de Tecnologías ESPE, requires an evaluation of risks and analysis of the LAN network, to keep them secure, providing the basic principles for risk and threat assessment, for the integrity, confidentiality and availability of information; for its development has been used the Pillar Risk Analysis and Management tool, in conjunction with the Magerit Methodology; to show clearly, possible threats, level of degradation, likewise to obtain safeguards to counteract the effects of them. At the same time, the accomplishment of a plan about defense and protection of computer security, in which specifies the importance of the assets, responsibilities from personnel of the TICs and also the users in general, measures and procedures in case of threats; the security in the operations, stealing of equipment and security in networks, establishing steps to be able to counteract their effects. In fact, the plan for defense and protection of computer security will serve as a complement to the Department of ICTs, providing security options for the management and use of each of the assets of the LAN of the institution.

KEYWORDS:

- **ANALYSIS**
- **MAGERIT**
- **PILLAR**
- **METHODOLOGY**
- **ASSETS**

CHECKED BY:

LIC. ENID QUEZADA

DOCENTE UGT

CAPÍTULO I

1.1. TEMA

ANÁLISIS Y EVALUACIÓN DE RIESGOS DE SEGURIDAD INFORMÁTICA EN LA RED DE ÁREA LOCAL (LAN), DE LA UNIDAD DE GESTIÓN DE TECNOLOGÍAS ESPE, PARA PERMITIR ESTABLECER UN PLAN DE DEFENSA Y PROTECCIÓN.

1.2. ANTECEDENTES

Según González Agudelo (2014), en su trabajo de investigación de Seguridad Informática manifiesta que:

La posibilidad de interconectarse a través de redes ha abierto nuevos horizontes a las empresas para mejorar su productividad y poder explorar más allá de las fronteras nacionales, lo cual lógicamente ha traído consigo la aparición de nuevas amenazas para los sistemas de información. Hoy es imposible hablar de un sistema 100% seguro, debido a que esta configuración no existe. Por eso las empresas asumen riesgos como perder un negocio o arriesgarse a ser hackeadas.

Según Jhon Erik Guanoluisa Huertas (2015) , en su trabajo de investigación de Análisis de Riesgos y Diseño de un Plan de Seguridad de la Información para el Consejo Nacional de Igualdad de Discapacidades “CONADIS” manifiestan que:

Hoy en día, hablar de Seguridad de la Información es hablar de una relación directamente proporcional con las amenazas y riesgos a los que una empresa u organización puede estar expuesta. Por este motivo, el proceso para establecer controles y medidas que ayuden a proteger la información puede resultar complicado pues dependerá del nivel de aplicación del mismo en la organización y es en ese momento en donde un Análisis de Riesgos cumple un papel fundamental en la optimización de este proceso.

Según (González Agudelo, 2014), en su trabajo de investigación de Seguridad Informática manifiesta que:

La seguridad informática es la disciplina que se ocupa de diseñar las normas, procedimientos, métodos y técnicas, orientados a proveer condiciones seguras y confiables, para el procesamiento de datos en sistemas informáticos. Consiste en asegurar que los recursos del sistema de información (material informático o programas) de una organización sean utilizados de la manera que se decidió y que el acceso a la información allí contenida, así como su modificación sólo sea posible a las personas que se encuentren acreditadas y dentro de los límites de su autorización.

Según Bermúdez Molina y Bailón Sánchez (2015) en su trabajo de investigación de Análisis en seguridad informática y seguridad de la información basado en la Norma ISO/IEC 27001- Sistemas de Gestión de Seguridad de la Información Dirigido a una empresa de servicios financieros manifiestan que:

Frente a situaciones adversas, las organizaciones e instituciones han tenido que optar por planes de acción, dirigidos a resguardar y proteger la integridad de los activos que conforman su red, tanto de hardware, software, instalaciones y el personal, como el caso del Instituto de Seguridad de Computadoras(CSI), el mismo que publicó, una Encuesta Mundial del Crimen y la Seguridad en las Computadoras, informando en su encuesta del 2005 que las pérdidas que sufrieron 186 de los encuestados, totalizan 378 millones de dólares; las mismas que están basadas en graves violaciones de seguridad.

La necesidad del Departamento de TICs de la Unidad de Gestión de Tecnologías ESPE, de identificar amenazas que puedan afectar a los activos de la red LAN, conlleva a la realización de un análisis de riesgos, por medio de metodologías y herramientas, con el fin de apoyar a la mejora de las actividades de la organización, de la misma manera la elaboración de un plan de defensa que ayude a generar salvaguardas para contrarrestar las afectaciones, de accesos no autorizados y pérdidas de equipos a los que se

encuentran actualmente expuestos. (ROBAYO LÓPEZ & RODRÍGUEZ RODRÍGUEZ, 2015)

La Unidad de Gestión de Tecnologías ESPE, se encuentra ubicada en el Sector la FAE, Cantón Latacunga, Provincia Cotopaxi, Dirección Av. Javier Espinoza N3-47 y Av. Amazonas, dedicada principalmente a actividades académicas, cuenta con una edificación adecuada, la misma que consta de tres plantas, divididas cada una en secciones, como laboratorios, aulas educativas, oficinas para el personal administrativo y de servicio, así como también el Departamento de Tics en el que principalmente va enfocado el proyecto.

La carrera de Tecnología en Computación, forma estudiantes capacitados en el área de (TICs), con conocimientos necesarios para el desarrollo de proyectos de sistemas de gestión, seguridad de la información incluso el uso adecuado de recursos informáticos; motivo por el cual se ha planteado la realización de un Análisis y evaluación de riesgos de Seguridad informática en la red de área local (LAN), de la Unidad de Gestión de Tecnologías ESPE, mediante la Metodología Magerit en conjunto con la herramienta PILAR, con el fin de establecer un plan de defensa y protección, que disminuya la probabilidad de afectaciones en los activos de la red.

1.3. PLANTEAMIENTO DEL PROBLEMA

Actualmente el Departamento de TICs de la Unidad de Gestión de Tecnologías de la Universidad de las Fuerzas Armadas ESPE de la ciudad de Latacunga, se encuentra al servicio de la comunidad universitaria, contando con un número de 1700 estudiantes y 90 servidores públicos, pertenecientes a las distintas áreas como: administrativos, docentes, profesionales de servicios; que diariamente tienen acceso no controlado a las instalaciones y al servicio de internet; el libre acceso podría ocasionar desestabilización en las actividades, actos en contra de la seguridad de los activos de la red; incrementando los riesgos de accesos no autorizados, pérdidas de equipos o robos de información. Dentro de los principales inconvenientes, se encuentra la protección no adecuada de los recursos informáticos de la red, así como

también la omisión de las políticas de seguridad ya establecidas, que deben seguir los usuarios para el correcto uso de los activos.

La protección de los activos de red y de la información se ve afectada, debido a la falta de cumplimiento de políticas de seguridad de uso de los recursos informáticos por los usuarios; el desconocimiento es uno de los factores principales; aspectos que dan paso a incidentes como robos de información, pérdida de equipos, accesos no autorizados maliciosos; las mismas que fueron identificadas, mediante visitas técnicas realizadas al personal del Departamento de TICs y de la institución en general.

Las amenazas y riesgos pueden ser causantes de un bajo rendimiento o pérdida total del servicio de la red de la Unidad de Gestión de Tecnologías de la Universidad de las Fuerzas Armadas ESPE, cesando las actividades propias de la Institución. Tomando en cuenta cada uno de los inconvenientes identificados mediante visitas técnicas, se decide llevar acabo el desarrollo, del análisis y evaluación de los riesgos, mediante la herramienta PILAR, aplicando las normas de uso según la metodología Magerit. (Grajales Bartolo, 2011)

1.4. JUSTIFICACIÓN

En la actualidad, con el avance tecnológico, el uso de herramientas de gestión de riesgos y la incrementación de políticas de seguridad para la protección de recursos informáticos, etc., han sido medidas que han ido evolucionando día con día. En el Departamento de TICs de la Unidad de Gestión de Tecnologías de la Universidad de las Fuerzas Armadas ESPE, con el afán de proteger los activos que conforman la red, surge la necesidad de contar con un plan de defensa, el mismo que incluye procedimientos de seguridad, que apoyen al correcto uso de los activos e información. Por esta razón previo al análisis realizado en las visitas técnicas se identificó la ausencia de algunos procedimientos indispensables para asegurar la protección de los recursos, responsabilidades del personal, usuarios, seguridad física /ambiental, accesos no autorizados, operaciones, seguridad

ante programas malignos, seguridad en redes y gestión de incidentes de seguridad, por lo que se decide proporcionar pautas para efectuar un procedimiento correcto, las mismas que fueron determinadas posterior a la evaluación de las amenazas, realizada mediante la metodología Magerit y la herramienta Pilar.

Es necesario mencionar que además de brindar solución en gran parte a los inconvenientes presentados, en cuanto a seguridad y uso de recursos informáticos, surge la necesidad de utilización de herramientas que puedan facilitar conocer de manera puntual las amenazas a las que se encuentran expuestos, por esta razón, el análisis de riesgos se realizó a través de la herramienta Pilar, en conjunto con la Metodología Magerit, la misma que fue elaborada por el Consejo Superior de Administración Electrónica de España; tienen como propósito de proveer información de riesgos y amenazas, valorarlos de manera cualitativa, conocer el impacto que pueden causar y medidas de seguridad necesarias para lograr contrarrestarlos. Los mismos que tienen un nivel de efectividad del 80%, en cuanto a solución, en medida de la aplicabilidad de las salvaguardas que la institución tome en cuenta frente a los riesgos encontrados.

El personal del Departamento de las TICs de la Unidad de Gestión de Tecnologías ESPE (UGT-ESPE), podrá conocer el resultado del análisis realizado a los activos de la red, ya que contará con un Plan de defensa y protección de Seguridad informática, en el que se describen los activos con mayor riesgo, procedimientos de control de los recursos informáticos, instalaciones, e instrucciones en caso de suscitarse un evento. El mismo que se desarrolló con el objetivo de lograr una correcta aplicación de las medidas de seguridad informática necesarias para proteger la integridad de cada uno de los recursos con que cuenta la institución.

1.5. OBJETIVO GENERAL

Analizar y evaluar riesgos de seguridad informática en la red de área local (LAN), de la unidad de gestión de tecnologías ESPE, para permitir establecer un plan de defensa y protección.

1.6. OBJETIVOS ESPECÍFICOS

- Identificar los requerimientos de la metodología Magerit y la herramienta Pilar, especificando las características de operación necesarias, para la realización del análisis de riesgos.
- Establecer un análisis de carácter cualitativo en los activos más críticos de la red LAN de la institución, para la identificación y valoración de amenazas.
- Proponer un plan de defensa y protección de seguridad informática para la red LAN de la Unidad de Gestión de Tecnologías ESPE, proporcionando lineamientos para precautelar la seguridad de la información, y toma de acciones para salvaguardar la integridad de los activos de la misma.

1.7. ALCANCE

Con el siguiente proyecto se busca realizar el análisis y evaluación de riesgos de seguridad informática en la red de área local LAN, el mismo que se desarrollará en el Departamento de TICs de la Unidad de Gestión de Tecnologías de la Universidad de las Fuerzas Armadas ESPE de la ciudad de Latacunga, basado en la Metodología Magerit apoyada con la herramienta Pilar, permitiendo identificar las principales amenazas a los que se encuentran expuestos los activos tanto de hardware, software, instalaciones y personal.

El análisis por desarrollar será de carácter cualitativo, en donde los niveles de evaluación serán de carácter probabilístico. La identificación de los activos y amenazas será realizada de forma general, considerando los equipos principales de la red; las salvaguardas serán definidas en base a la detección de los riesgos de mayor prioridad. Por lo tanto, solo servirán como guía para

que el personal encargado del Departamento de TICs evalúe la posibilidad de implementación o mejoramiento de la seguridad en los equipos.

Finalmente logrando la elaboración de un plan de defensa y protección de seguridad informática, para garantizar la integridad de los activos de la red, en un escenario donde los riesgos se encuentran siempre presentes y si no son adecuadamente controlados pueden producir daños graves.

CAPÍTULO II

MARCO TEÓRICO

2.1. Información

Según Tixilima Cisneros (2015) , en su trabajo de investigación de Elaboración de políticas y normas de seguridad de la información en base a la norma de seguridad ISO/IEC 27001, y al análisis de riesgos realizado aplicando la metodología Magerit y la herramienta Pilar, manifiesta que:

La información es todo grupo organizado de datos que puede manejar una organización, y que tenga valor para la misma, independientemente de la manera en la cual se la puede almacenar, procesar o transmitir como también su origen o fecha de elaboración.

Según Álvarez Edison Oswaldo Rosero (2014), en su trabajo de investigación de Análisis de riesgos de la seguridad de la red de área local (LAN) de la matriz de la Contraloría General del Estado, manifiesta que:

La información es uno de los componentes activos de mayor importancia, es por esta razón que necesita tener una protección adecuada. Un activo es necesariamente cualquier cosa que tenga valor para las Tecnologías de la Información, existe información en diferentes formas, ya sea impresa, escrita en un papel, almacenada electrónicamente, transmitida por correo, utilizando medios electrónicos, mostrada en películas o hablada en una conversación.

Cualquiera que sea la forma que tome la información o el medio por el cual sea almacenada o compartida, siempre deberá estar adecuadamente protegida.

2.2. Importancia de la Seguridad de la información

Según Amutio Gómez, Candau, & Mañas (2012) en su trabajo de manifiestan que:

Seguridad es la capacidad de las redes o de los sistemas de información para resistir, con un determinado nivel de confianza, los accidentes o acciones ilícitas o malintencionadas que comprometan la disponibilidad, integridad y confidencialidad de los datos almacenados o transmitidos y de los servicios que dichas redes y sistemas ofrecen o hacen accesibles.

Según Amutio Gómez, Candau, & Mañas (2008) en su trabajo de manifiesta que:

La seguridad ha pasado de ser utilizada para preservar los datos clasificados del gobierno en cuestiones militares o diplomáticas, a tener una aplicación de dimensiones inimaginables y crecientes que incluye transacciones financieras, acuerdos, información personal, domótica y computación. Por ello, se hace imprescindible que las necesidades de seguridad potenciales sean tenidas en cuenta y se determinen para todo tipo de aplicaciones.

2.3. Metodología MAGERIT V3.0 (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información)

Según Rodríguez, Peralta, & Consejo Superior de Administración Electrónica (2013), en su trabajo de investigación de Gestión de Riesgos Magerit, indican que:

MAGERIT es la metodología de análisis y gestión de riesgos elaborada por el Consejo Superior de Administración Electrónica, que permite: estudiar los riesgos que soporta un sistema de información y el entorno asociado a él.

Según Rodríguez, José María y Peralta, Ignacio (2013), en su trabajo de investigación de Gestión de Riesgos Magerit, indican que:

MAGERIT propone la realización de un análisis de los riesgos que implica la evaluación del impacto que una violación de la seguridad tiene en la organización; identificando las amenazas que acechan al sistema de información, y determina la vulnerabilidad.

Los resultados del análisis de riesgos permiten a la Gestión de Riesgos recomendar las medidas apropiadas que deberían adoptarse para conocer, prevenir, impedir, reducir o controlar los riesgos identificados y así reducir al mínimo su potencialidad o sus posibles perjuicios. MAGERIT es un instrumento para facilitar la implantación y aplicación del Esquema Nacional de Seguridad proporcionando los principios básicos y requisitos mínimos para la protección adecuada de la información.

Según Rodríguez, José María y Peralta, Ignacio (2013), en su trabajo de investigación de Magerit, indican que:

El análisis de riesgos considera los siguientes elementos:

1. **Activos:** Elementos del sistema de información (o estrechamente relacionados con este) que soportan la misión de la Organización.
2. **Amenazas:** Cosas que les pueden pasar a los activos causando un perjuicio a la Organización.
3. **Salvaguardas:** (o contra medidas), medidas de protección desplegadas para que aquellas amenazas no causen tanto daño.

Con estos elementos se puede estimar:

1. **El impacto**: lo que podría pasar en los activos en caso de materializarse una amenaza que afecte de manera potencial.
2. **El riesgo**: lo que probablemente pase (Rodríguez, Peralta, & Consejo Superior de Administración Electrónica, 2013)

2.3.1. Análisis de Riesgos

El análisis de riesgos es una aproximación metódica para determinar el riesgo siguiendo los siguientes pasos:

1. Determinar los activos relevantes para la Organización, su interrelación y su valor, en el sentido de qué perjuicio (coste) supondría su degradación.

2. Determinar a qué amenazas están expuestos aquellos activos.

3. Determinar qué salvaguardas hay dispuestas y cuán eficaces son frente al riesgo.

4. Estimar el impacto, definido como el daño sobre el activo derivado de la materialización de la amenaza.

5. Estimar el riesgo, definido como el impacto ponderado con la tasa de ocurrencia de la amenaza. (Rodríguez, Peralta, & Consejo Superior de Administración Electrónica, 2013)

Figura 1 Aproximación Metódica Activos, Amenazas y Salvaguarda.

Fuente: (Rodríguez, Peralta, & Consejo Superior de Administración Electrónica, 2013)

2.3.2. Activos

Según Rodríguez, José María y Peralta, Ignacio (2013), en su trabajo de investigación Gestión de Riesgos Magerit, indican que:

Componente o funcionalidad de un sistema de información susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización.

Estos pueden ser:

1. Aplicaciones informáticas (software) que permiten manejar los datos.
2. Equipos informáticos (hardware) y que permiten hospedar datos, aplicaciones y servicios.
3. Soportes de información que son dispositivos de almacenamiento de datos.
4. Equipamiento auxiliar que complementa el material informático.
5. Redes de comunicaciones que permiten intercambiar datos.
6. Instalaciones que acogen equipos informáticos y de comunicaciones.

¿Cuál es el valor de los activos?

Según Rodríguez, José María y Peralta, Ignacio (2013), en su trabajo de investigación de Magerit indican que:

La valoración se debe realizar desde la perspectiva de la necesidad de proteger. Cuanto más valioso es un activo, mayor nivel de protección requeriremos en la dimensión (o dimensiones) de seguridad que sean pertinentes.

2.3.3. OBJETIVOS MAGERIT:

Magerit persigue los siguientes objetivos:

1. Concienciar a los responsables de las organizaciones de información de la existencia de riesgos y de la necesidad de gestionarlos.
2. Ofrecer un método sistemático para analizar los riesgos derivados del uso de tecnologías de la información y comunicaciones (TIC).

También se ha buscado la uniformidad de los informes que recogen los hallazgos y las conclusiones de las actividades de análisis y gestión de riesgos:

1. **Modelo de valor:** Es la caracterización del valor en el cual representan cada uno de los activos de la Organización.
2. **Evaluación de salvaguardas:** Se evalúa la eficacia que puedan tener las salvaguardas encontradas.
3. **Estado de riesgo:** Obtención de la caracterización de los riesgos encontrados.
4. **Informe de insuficiencias:** Verificación si las amenazas pueden ayudar a contrarrestar los riesgos encontrados
5. **Cumplimiento de normativa:** Satisfacción de unos requisitos. Declaración de que se ajusta y es conforme a la normativa correspondiente.
6. **Plan de seguridad:** Conjunto de procedimientos y políticas de seguridad que disminuir las afectaciones en caso de aparición de un riesgo. (MAGERIT, 2012)

2.4. Descripción y Justificación de la Metodología MAGERIT

Según Amutio Gómez, Miguel Angel; Candau, Javier; Mañas, José Antonio (2012), en su trabajo de investigación de Magerit, manifiesta que:

MAGERIT persigue algunos objetivos de manera directa como también indirecta:

1. Concientizar a los responsables de las organizaciones de información de la existencia de riesgos y de la necesidad de gestionarlos.
2. Ofrecer un método sistemático para analizar los riesgos.
3. Buscar la uniformidad de los informes que recogen los hallazgos y las conclusiones de las actividades.

2.4.1. Descripción Metodología Magerit

La Metodología Magerit, se encuentra dividida en dos libros y una guía de técnicas:

Libro I Método

El primer libro de Magerit, se refiere al Método, en el cual se puede encontrar el método de análisis de riesgos, como se realiza el proceso de gestión de riesgos. De la misma manera el plan de seguridad como se debe realizarlo teniendo en cuenta el desarrollo de los sistemas de información y por último consejos prácticos para la aplicación de la metodología. (Amutio Gómez, Candau, & Mañas, 2012)

Libro II Catálogo de Elementos

El segundo Libro de Magerit, habla sobre los tipos de activos, las dimensiones y criterios de valoración, amenazas, salvaguardas y modelos en los cuales se puede especificar cada uno de ellos acorde a lo que establece la metodología. (Amutio Gómez, Candau, & Mañas, 2012)

Libro III Guía de Técnicas

El tercer Libro de Magerit, se refiere a las técnicas específicas, análisis mediante tablas, modelos cualitativos y técnicos generales que se pueden utilizar en salvaguardas, amenazas, riesgos, medición de impacto en los activos. (Amutio Gómez, Candau, & Mañas, 2012)

2.5. Proyecto Análisis de Riesgos

Para realizar un proyecto de Análisis de Riesgos se debe tener en cuenta pasos esenciales para obtener un resultado efectivo, en cuanto a poder identificar amenazas, salvaguardas y cada uno de los estados de dicho riesgo representa, con esto al final lograr tomar decisiones, elaborar un plan de seguridad efectivo y la ejecución del mismo. (Quintero Villarroya & SDG TIC. Ministerio de Defensa, 2012)

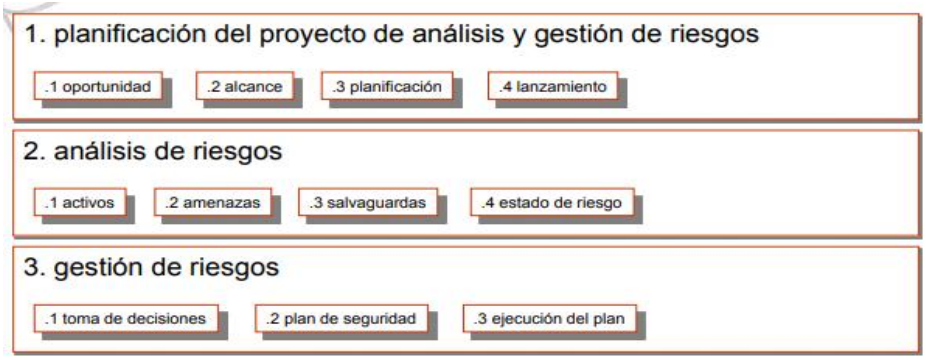


Figura 2 Proyecto Análisis de Riesgos

Fuente: (Quintero Villarroya & SDG TIC. Ministerio de Defensa, 2012, pág. 16)

2.6. Fases de Desarrollo de la Metodología Magerit

2.6.1. Fase 1 Activos

Según Álvarez Edison Oswaldo Rosero (2014), en su trabajo de investigación de Análisis de riesgos de la seguridad de la red de área local (LAN) de la matriz de la Contraloría General del Estado, indica que:

En esta etapa se identifican los activos más relevantes de la organización. Entre los activos con mayor relevancia para la metodología Magerit muestra las siguientes categorías:

- [HW] Hardware
- [SW] Software
- [AUX] Equipamiento Auxiliar
- [L] Instalaciones
- [P] Personal

Valoración de los Activos

Según Álvarez Edison Oswaldo Rosero (2014), en su trabajo de investigación de Análisis de riesgos de la seguridad de la red de área local (LAN) de la matriz de la Contraloría General del Estado, indica que

El valor que se establece a un activo es la estimación del coste que causaría, en caso de que se materializará una amenaza de dicho activo.

Para facilitar la valoración, se debe considerar el daño total cuando la amenaza afecta contundentemente al activo y lo destroza completamente en una cierta dimensión. Después, para cada amenaza, se estimará en qué medida el daño es completo o parcial. El valor del activo, junto con la degradación, permite para estimar el impacto de una amenaza sobre un activo. (Álvarez Edison Oswaldo Rosero, 2014, pág. 15)

Impacto = valor x degradación

Según Álvarez Edison Oswaldo Rosero (2014), en su trabajo de investigación de seguridad informática indica que:

El Riesgo también es un indicador de lo que posiblemente suceda por causa de las amenazas.

Riesgo = impacto * degradación

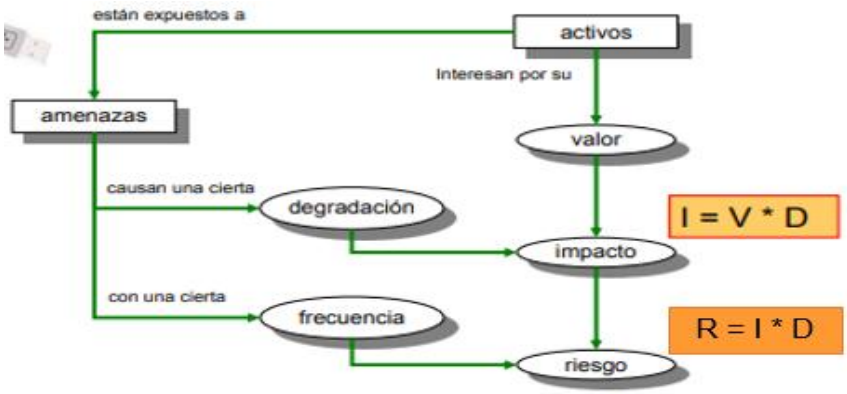


Figura 3 Valoración Activos, Análisis de Riesgo

Fuente: (Quintero Villarroya & SDG TIC. Ministerio de Defensa, 2012, pág. 37)

2.6.2. Fase 2 Amenazas

Según Álvarez Edison Oswaldo Rosero (2014), en su trabajo de investigación de Análisis de riesgos de la seguridad de la red de área local (LAN) de la matriz de la Contraloría General del Estado indica que:

En esta fase se procede a identificar las amenazas a los cuales los activos pueden verse afectados.

- **Frecuencia:** cada cuánto se materializa una amenaza.
- **Degradación:** impacto que tiene la materialización de la amenaza en el activo.

2.6.3. Fase 3 Salvaguardas

Según Álvarez Edison Oswaldo Rosero (2014), en su trabajo de investigación de Análisis de riesgos de la seguridad de la red de área local (LAN) de la matriz de la Contraloría General del Estado indica que:

Las salvaguardas son las contras medidas que se definen como aquellos procedimientos o mecanismos tecnológicos que reducen el riesgo.

2.6.4. Fase 4 Impacto Residual

Luego de efectuar las salvaguardas, los activos a los cuales se los aplica quedan en una situación en la cual es posible que el impacto sea disminuido de un valor potencial a un valor residual. El cálculo del impacto residual se realiza midiendo la magnitud de la degradación que sufre el activo. (Álvarez Edison Oswaldo Rosero, 2014, pág. 16)

2.7. EAR/PILAR

PILAR conjuga los activos TIC de un sistema con las amenazas posibles, calcula los riesgos y permite incorporar salvaguardas para reducir el riesgo a valores residuales aceptables. Esto permite fundamentar la confianza en el sistema. (PAE Portal Administración Electrónica, 2004)

Dicho software también permite introducir las amenazas posibles en los aspectos de disponibilidad, integridad, confidencialidad, autenticidad y trazabilidad, para derivar los riesgos potenciales sobre el sistema. (PAE Portal Administración Electrónica, 2004)

Según Quintero Villarroya (2012), en su trabajo de investigación de Análisis y Gestión de Risgos Pilar, dice que:

La herramienta EAR/PILAR soporta el análisis y la gestión de riesgos de un sistema de información siguiendo la Metodología Magerit.

Figura 4 Esquema EAR / PILAR

Fuente: (Quintero Villarroya & SDG TIC. Ministerio de Defensa, 2012)

Según Quintero Villarroya (2012), en su trabajo de investigación de Análisis y Gestión de Risgos Pilar, indica que:

PILAR dispone de una biblioteca estándar de propósito general, y es capaz de realizar calificaciones de seguridad respecto de normas ampliamente conocidas como son:

- Esquema Nacional de Seguridad. - ISO/IEC 27001:2013. (2012)

2.7.1. Análisis de Impacto y Continuidad de Operaciones

Según Quintero Villarroya (2012), en su trabajo de investigación de Análisis y Gestión de Risgos Pilar, dice que:

Se analiza el efecto de las interrupciones de servicio teniendo en cuenta la duración de la interrupción. Para tratar el riesgo se proponen:

- Salvaguardas.

- Elementos de respaldo.
- Planes de recuperación de desastres analizándose el impacto residual a lo largo de diversas etapas de tratamiento. (Quintero Villarroya & SDG TIC. Ministerio de Defensa, 2012)

Figura 5 Análisis de Impacto y Continuidad de Operaciones

EAR / Pilar es una herramienta gratuita, en donde permite generar una licencia de evaluación de 30 días para poder efectuar el proyecto, la misma que puede ser solicitada enviando un correo electrónico a la dirección de correo dispuesta en el mismo sitio web. (Quintero Villarroya & SDG TIC. Ministerio de Defensa, 2012)

2.8. NORMA ISO/IEC 27001/2013

El Plan de defensa y protección de seguridad informática, consiste en proporcionar una opción para el Sistema de Gestión de la Seguridad de la Información, la Norma ISO/IEC 27001, su eje central es proteger la confidencialidad, integridad y disponibilidad de la información en una empresa. (Antonio Jose Segovia, 2019)

ISO 27001 es una norma internacional emitida por la Organización Internacional de Normalización (ISO) y describe cómo gestionar la seguridad de la información en una empresa. La revisión más reciente de esta norma

fue publicada en 2013 y ahora su nombre completo es ISO/IEC 27001:2013, la primera revisión se publicó en 2005. (Antonio Jose Segovia, 2019)

La elaboración del Plan de defensa y protección de seguridad informática para la Unidad de Gestión de Tecnologías ESPE, se encuentra enfocado en el uso del estándar ISO/IEC 27001/2013, ya que en el mismo se proporciona cada uno de los lineamientos para la gestión de la seguridad de la información, el mismo que cubre únicamente la parte planificación, mientras que para la implementación y mejora se da como una recomendación. (Jhon Erik Guanoluisa Huertas, 2015)

Según Jhon Erik Guanoluisa Huertas (2015) , en su trabajo de investigación de Análisis de Riesgos y Diseño de un Plan de Seguridad de la Información para el Consejo Nacional de Igualdad de Discapacidades “CONADIS” manifiestan que:

De esta manera demandará la gestión de múltiples políticas, procedimientos, personas, bienes, etc., ISO 27001 ha detallado cómo amalgamar todos estos elementos dentro del sistema de gestión de seguridad de la información (SGSI).

Por eso, la gestión de la seguridad de la información no se acota solamente a la seguridad de TI (por ejemplo, cortafuegos, antivirus, etc.), sino que también tiene que ver con la gestión de procesos, de los recursos humanos, con la protección jurídica, la protección física, etc. (Antonio Jose Segovia, 2019)

ISO 27001 puede ser implementada en cualquier tipo de organización, con o sin fines de lucro, privada o pública, pequeña o grande. La filosofía principal de la norma ISO 27001 se basa en la gestión de riesgos: investigar dónde están los riesgos y luego tratarlos sistemáticamente. (Antonio Jose Segovia, 2019)

Figura 6 Estructura ISO 27001

Fuente: (Antonio Jose Segovia, 2019)

2.9. Información elaboración del Plan de Seguridad Informática

Según Jhon Erik Guanoluisa Huertas (2015) , en su trabajo de investigación de Análisis de Riesgos y Diseño de un Plan de Seguridad de la Información para el Consejo Nacional de Igualdad de Discapacidades “CONADIS” manifiestan que:

El Plan de Seguridad Informática proporciona pautas necesarias para gestionar de manera correcta la seguridad tanto de la información, como el uso de los activos, proponiendo ideas para mejorar en el momento de su implementación.

Es por esta razón que la propuesta del Plan de seguridad Informática para la Unidad de Gestión de Tecnologías ESPE, servirá como una propuesta objetiva, que sirva como guía, para lograr proteger a los activos e información de posibles amenazas. Cabe recalcar que el presente proyecto de titulación está centrado en la base de planificación, es decir que la implementación, verificación y mejoramiento del plan ya establecido por la institución, queda a total criterio de los directivos. Dicha fase consiste en definir procedimientos para la gestión de riesgos y la mejora de la seguridad de la información. (Jhon Erik Guanoluisa Huertas, 2015)

2.9.1. Documentos Entregables

Los documentos entregables, ayudarán a reducir los riesgos en los mismos, se procede a proponer políticas de seguridad que pueden ayudar a

concientizar sobre la protección de los activos y el manejo correcto de la información. (Jhon Erik Guanoluisa Huertas, 2015)

Según Jhon Erik Guanoluisa Huertas (2015) , en su trabajo de investigación de Análisis de Riesgos y Diseño de un Plan de Seguridad de la Información para el Consejo Nacional de Igualdad de Discapacidades “CONADIS” manifiestan que:

Los documentos entregables para este proyecto ver Anexo J del Plan de defensa y protección de Seguridad Informática son las siguientes:

- Procedimiento para control de Documentos y Registros
- Seguridad de la Información. (Jhon Erik Guanoluisa Huertas, 2015)

2.10. Hipótesis del Proyecto Planteado

Con la utilización de la Metodología Magerit y la herramienta EAR / PILAR 7.2.1, se puede proceder a realizar un análisis y evaluación de riesgos de la red de área local (LAN) de la Unidad de Gestión de Tecnologías ESPE, el mismo que permitirá identificar cada uno de los activos que se encuentran en utilización y los riesgos que pueden sufrir los mismo. Realizando identificación de cada uno de los activos de hardware, software, instalaciones y el personal que se encuentran en la institución; y al final poder conocer los riesgos y amenazas potenciales y encontrar acciones y recomendaciones efectivas al momento de que alguna amenaza pueda hacerse efectiva. De esta manera también poder establecer un plan de defensa.

CAPÍTULO III

3.1. Situación Actual de la Red LAN de la Unidad de Gestión de Tecnologías ESPE (UGT-ESPE).

Mediante la realización de una visita técnica ejecutada al Departamento de TICs de la Unidad de Gestión de Tecnologías ESPE, de manera personal al Sr. Sgop. Luis Santana, encargado del departamento TICs, se procede a identificar la situación actual de la red LAN, su infraestructura la misma que se encuentra compuesta por las siguientes características de distribución.

Tabla 1

Situación actual Red LAN UGT-ESPE

Institución	Número plantas (Edificio)	Número de Áreas	Número de Usuarios	Número de PCs		Responsable
				Desktop	Laptop	
Unidad de Gestión de Tecnologías ESPE	3	9	90	30	60	Sgop. Luis Santana

La red LAN de la Unidad de Gestión de Tecnologías ESPE, está conformada por una red donde se encuentran la mayoría de los equipos tanto de software, hardware, instalaciones y personal. De la misma manera se encuentran los equipos de los usuarios como computadoras tanto de escritorio como también laptops, impresoras.

3.2. Diagrama Red LAN de la Unidad de Gestión de Tecnologías ESPE.

A continuación, se procede a mostrar el Diagrama de la red en la cual podemos observarlo de manera general, cada uno de los dispositivos que se encuentran implementados.

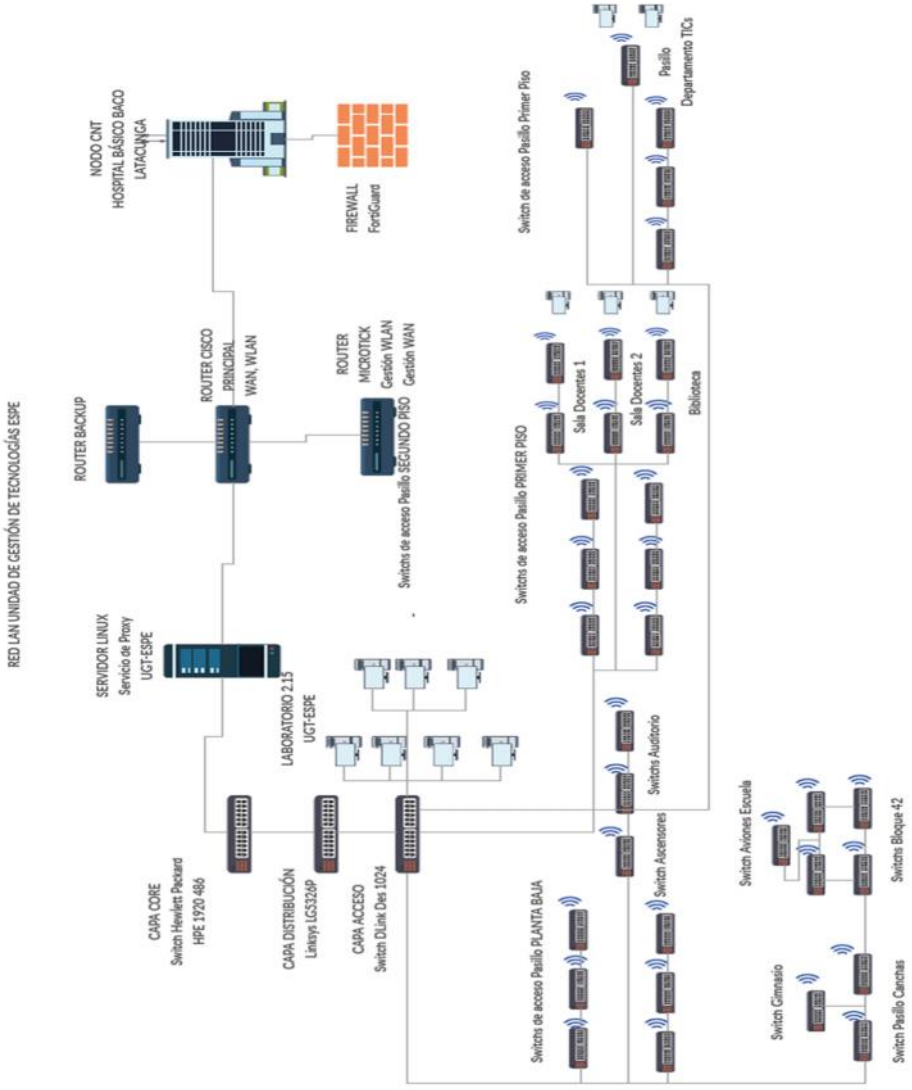


Figura 7 Red LAN de la Unidad de Gestión de Tecnologías ESPE

3.3. Inventario de Activos de la Red LAN de la UGT-ESPE

Tabla 2

Activos Red LAN UGT-ESPE

Cant	Activo	Descripción	Categoría	Ubicación	Responsable TICs
3	Router CISCO	Enlace WAN Backup	Capa 3	Rack Comunicación	Sgop. Luis Santana

1	Router Mikrotik	Gestión WLAN Gestión WAN	Capa 3	Rack Comunicación	Sgop. Luis Santana
2	Switch 24 puertos	Wireless Administrable	Capa 3 Capa 2	Rack Comunicación	Sgop. Luis Santana
3	Switch 24 puertos	No Administrable	Capa 2	Varias Áreas	Sgop. Luis Santana
3	Switch 16 puertos	No Administrable	Capa 2	Varias Áreas	Sgop. Luis Santana
1	Rack	Servidores		Gabinete Cerrado TIC's	Sgop. Luis Santana
1		Firewall FortiGuard		BACO UGT-ESPE TICs	Sgop. Luis Santana
1	UPS 6KVA	Energía Respaldo TIC's		TICs	Sgop. Luis Santana
1	Servidor Linux	Servicio Proxy Permisos Acceso RED		TICs	Sgop. Luis Santana
1	Sistema Operativo Linux	Sistema Operativo Linux		TICs	Sgop. Luis Santana

La tabla anterior, pretende mostrar los dispositivos principales con los cuales está trabajando en la red LAN de la UGT-ESPE.

3.4. Planos Unidad de Gestión de Tecnologías ESEPE

A continuación se muestra planos de las instalaciones y equipos con los cuales se encuentra conformada el edificio de la Unidad de Gestión de Tecnologías ESPE, las mismas que fueron obtenidas en base a las entrevistas técnicas ejecutadas al Sr Sgop. Luis Santana, encargado del Departamento de TICs de la institución:

Los planos constan de:

- Plano Bloque 42, Aviones Escuela, y Canchas deportivas
- Plano Planta Baja
- Plano Primer Piso
- Plano Segundo Piso

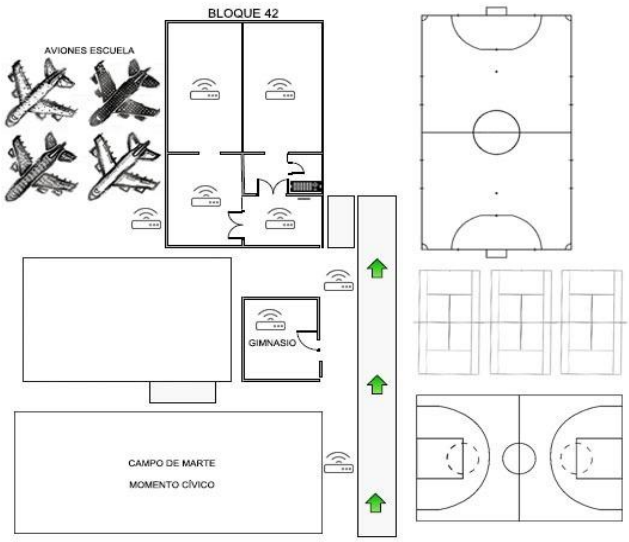


Figura 8 Plano Bloque 42, Canchas, Avión Escuela

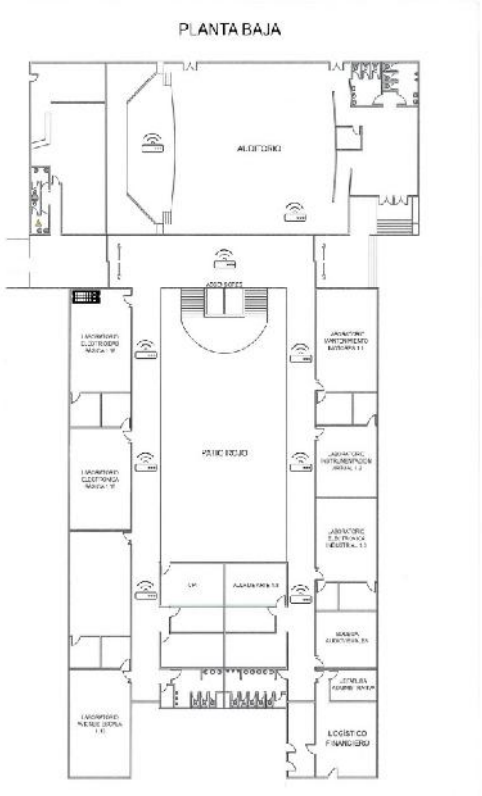


Figura 9 Plano Planta Baja

Figura 10 Plano Primer Piso

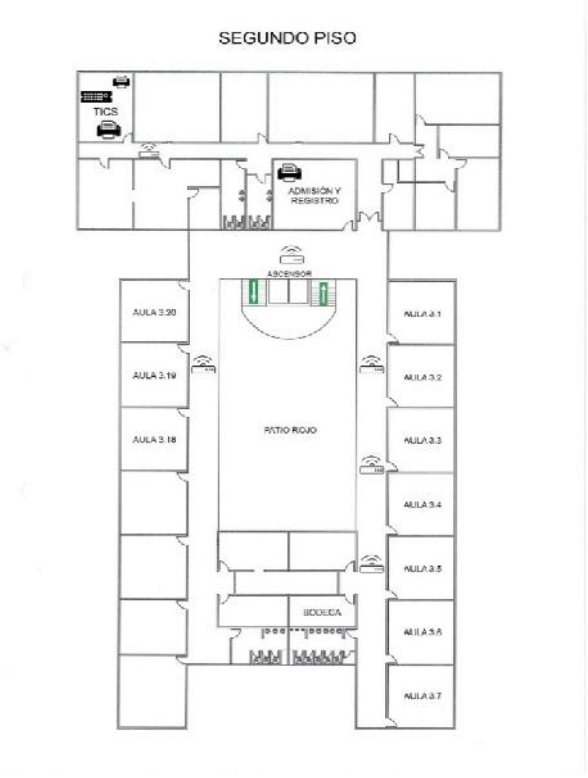


Figura 11 Plano Segundo Piso

3.5. Firewalls

Según (Pérez-Roca Fernández & Pereira Suárez), en su trabajo de Firewalls manifiesta que:

Un firewall es un elemento de hardware o software utilizado en una red de computadoras para controlar las comunicaciones, permitiéndolas o prohibiéndolas según las políticas de red que haya definido la organización responsable de la red.

3.5.1. Firewall FortiGuard: Servicios de seguridad FortiGuard

La protección de seguridad certificada y probada de FortiGuard proporciona Completas actualizaciones de seguridad y protección para el completa gama de soluciones de Fortinet's Security Fabric. FortiGuard Labs consta de cientos de especialistas en investigación, con un promedio de más de 16 años de experiencia en investigación y respuesta a amenazas, proporcionar protección de vanguardia a los clientes y mejorar su defensa de la seguridad cibernética. (Copyright © 2018 Fortinet, 2018)

Las amenazas cibernéticas y el delito cibernético van en aumento. Los criminales son explotando la complejidad de nuestras redes en expansión para infectar, robar datos, y mantener los sistemas de rescate. Amplia investigación y conocimiento del paisaje de amenazas, combinado con la habilidad para responder rápidamente en múltiples niveles, es imprescindible para proporcionar seguridad efectiva**.** (Copyright © 2018 Fortinet, 2018)

Figura 12 Servicios FortiGuard

Fuente: (Solutions, 2018)

3.6. Modelo Jerárquico Red LAN UGT-ESPE

3.6.1. Diseño de red Jerárquica

Según Miranda Candelario Piedad Maribel (2017), en su trabajo de investigación de Diseño y reingeniería de la infraestructura de la red LAN de la facultad de ciencias económicas de la universidad de Guayaquil, manifiesta que:

El diseño de red jerárquica tiene tres capas independientes. Cada una de sus capas cumple funciones específicas que definen su función dentro de la red general. Tiene varias ventajas ya que es más fácil diseñar, implementar, mantener y escalar la red, además de que la hace más confiable, con una mejor relación costo/beneficio.

3.6.2. Beneficios del Modelo de Red Jerárquico

1. **Escalabilidad:** Las redes jerárquicas pueden expandirse con facilidad.
2. **Redundancia:** La redundancia a nivel del núcleo y de la distribución asegura la disponibilidad de la ruta.
3. **Rendimiento:** El agregado de enlaces entre los niveles y los switches del núcleo de alto rendimiento y del nivel de distribución permite casi la “velocidad del cable” en toda la red.
4. **Seguridad:** La seguridad del puerto en el nivel de acceso y las políticas en el nivel de distribución hacen que la red sea más segura y confiable.
5. **Facilidad de administración:** La consistencia entre los switches en cada nivel hace que la administración sea más simple.

El modelo jerárquico principalmente utilizado es el de 3 capas de CISCO, a continuación, se describe cada una de ellas.

- **Capa Core** A esta capa se le conoce también como backbone o el núcleo de la red, donde su función es llevar grandes cantidades de tráfico de manera confiable y veloz. (Rosero Álvarez Edison Oswaldo, 2014)

- **Capa Distribución** En esta capa es el medio de comunicación entre la capa de acceso y el Core, provee ruteo, determinar que paquetes deben llegar al Core o sea se puede implementar listas de acceso, aplicar políticas para la gestión de red. (Rosero Álvarez Edison Oswaldo, 2014)
- **Capa Acceso:** En esta capa es el punto de entrada para los usuarios finales a sus diferentes estaciones de trabajo y también los servidores de la red LAN. (Rosero Álvarez Edison Oswaldo, 2014)

En la Unidad de Gestión de Tecnologías se está utilizando Switches de las tres capas antes mencionadas, los mismos que están conectados en forma de cascada. Siendo los siguientes modelos los cuales están funcionando según cada capa.

1. **Capa Core** (Switch Hewlett Packard HPE 1920 48G)
2. **Capa Distribución** (Switch Linksys LGS326P)
3. **Capa Accesso** (Switch DLINK DES 1024)

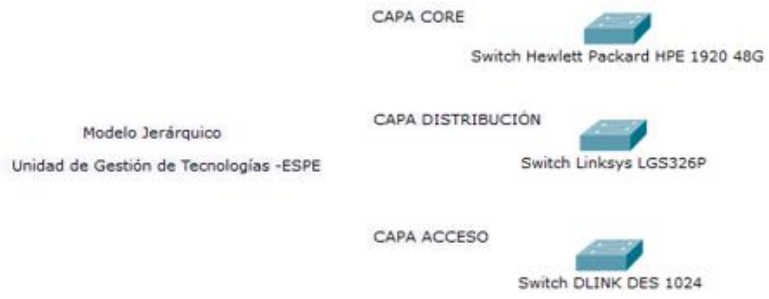


Figura 13 Modelo Jerárquico UGT-ESPE

3.7. EAR / PILAR

Pilar es una herramienta gratuita de análisis y gestión de riesgos en donde permite identificar los activos de una organización y disminuir los riesgos potenciales y residuales en un sistema de información y comunicaciones. (PILAR - Manual de Usuario, 2016)

3.7.1. Instalación

Para realizar la instalación del Software Pilar 7.2.1, se debe ingresar a la página oficial de descarga EAR/PILAR: https: //www.ar-tools.com/es/tools/pilar/v72/download.html, en la cual se puede elegir el software compatible según el sistema operativo del equipo con el que se trabajará, las mismas que existen para Windows, Linux y Mac, en este caso se utilizó la versión de PILAR 7.2.1 de Windows, la cual es la última versión entregada el 31 de Diciembre del 2018.

Figura 14 Descarga Software PILAR 7.2.1

Como segundo se ejecuta el software como administrador, para poder obtener los privilegios para la edición, copia y eliminación que se puedan realizar a los archivos del mismo.

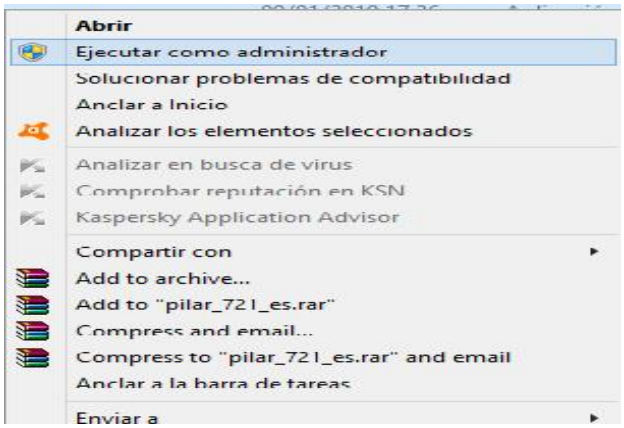


Figura 15 Ejecución Software PILAR 7.2.1

Luego muestra una pantalla de información acerca del software en donde se explica, el paquete que proporciona la herramienta y los requerimientos.

Figura 16 Primera pantalla de instalación Pilar 7.2.1

A continuación, se muestran pantallas en la cual se puede seleccionar la carpeta de destino en la cual se guardarán cada uno de los archivos necesarios para el funcionamiento del software. Las mismas que no requieren modificación.

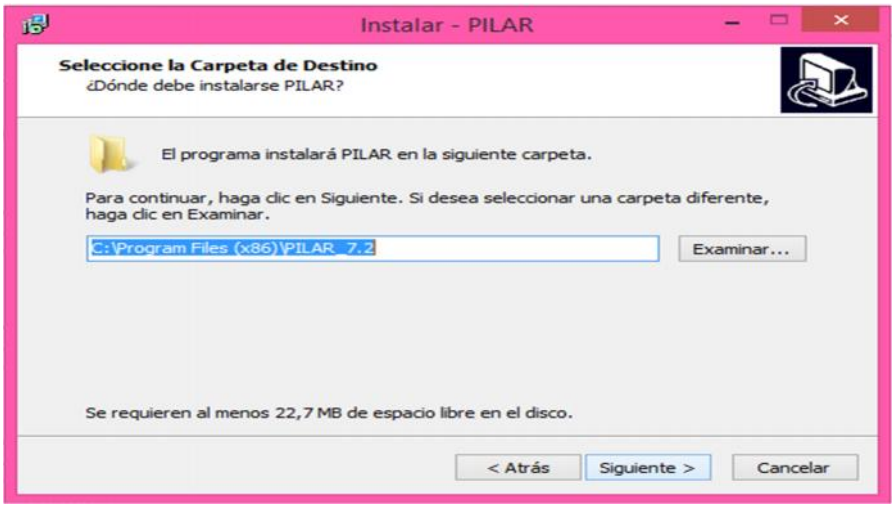


Figura 17 Pantalla seleccionar carpeta de destino

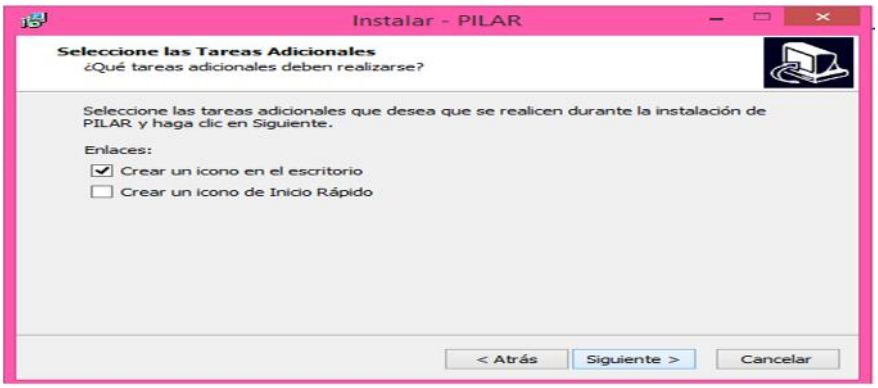


Figura 18 Pantalla Selección para crear ícono en el escritorio

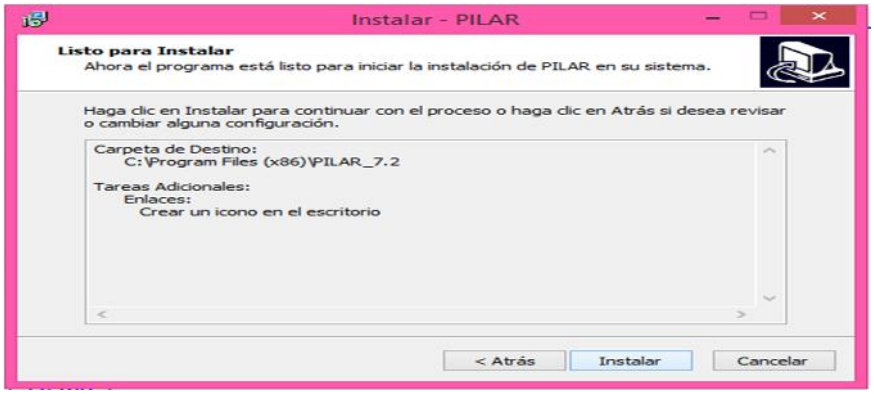


Figura 19 Pantalla opciones seleccionadas anteriormente.

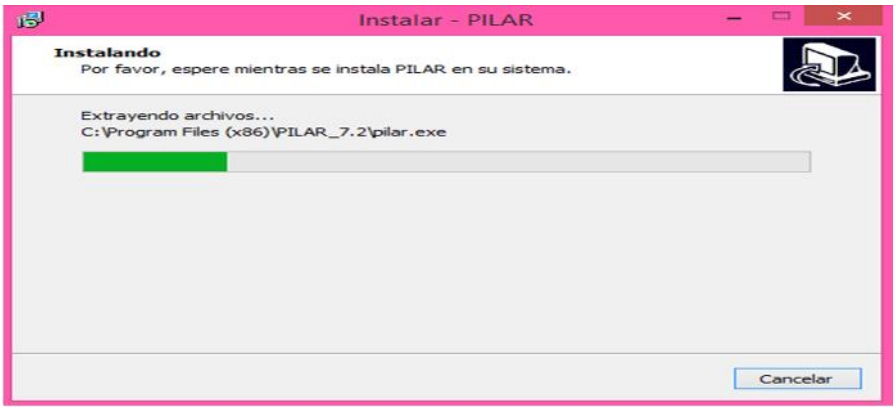


Figura 20 Pantalla muestra avance de instalación.

3.7.2. Resultados

Según (PAE Portal Administración Electrónica, 2004), manifiesta que:

Herramienta para la monitorización continúa del estado de riesgo y seguimiento de proyectos de mejora de la seguridad.

Resultados que pueden obtenerse mediante el software:

- Impacto potencial y residual.
- Riesgo potencial y residual.
- Plan de mejora de la seguridad
- Monitorización continúa del Estado de Riesgo. (PAE Portal Administración Electrónica, 2004)

3.7.3. Ventajas

- Conocer los riesgos a fin de poder tratarlos. (2004)
- Conocer el grado de cumplimiento de diferentes perfiles de seguridad: 27002, protección de datos de carácter personal, esquema nacional de seguridad, etc. (2004)
- Implementar la metodología Magerit e ISO/IEC 27005. (PAE Portal Administración Electrónica, 2004)

3.8. Elaboración del Análisis de Riesgos de la red LAN de la Unidad de Gestión de Tecnologías ESPE.

Figura 21 Elaboración Análisis de la Red LAN de la UGT-ESPE

3.8.1. Entrevista personal TIC's

Para realizar el análisis, se realizó una entrevista con el personal encargado de la gestión de las TIC's de la Unidad de Gestión de Tecnologías ESPE. La misma que ayudó para conocer los principales activos necesarios para el análisis de riesgos.

3.8.2. Descripción General de la Información Adquirida

Se cuenta con toda la descripción de la información recolectada la misma que esta descrita en el mismo capítulo tres, en los puntos 3.1 y 3.3.

3.8.3. Tabulación de la Información Recolectada

Según Amutio Gómez (2012), en su trabajo de investigación de Magerit manifiesta que:

Para proceder a elaborar la tabulación de la información recolectada, la Metodología MAGERIT, sugiere la realización de fichas por cada uno de los activos que hayan sido identificados en la institución.

Formato de las fichas a continuación describiendo cada campo:

1. Titulo general del activo a describir.
2. Código del activo a describir.
3. Nombre del Activo.
4. Breve descripción del Activo.
5. Persona a cargo.
6. Ubicación del activo.
7. Categoría a la que pertenece al activo.
8. Identificación de las dependencias del activo indicando el por qué el activo depende del activo que se indique.
9. Refiere a la estimación del grado de dependencia de 0 hasta 100%.

[HW] HARDWARE

Tabla 3

Modelo Tabulación de Activos

[HW] Equipamiento Informático (Hardware)	
Código: HW_Firewall	**Nombre:** Cortafuegos
Descripción: Un firewall es un elemento de hardware o software utilizado en una red de computadoras para controlar las comunicaciones, permitiéndolas o prohibiéndolas según las políticas de red que haya definido la organización responsable de la red.	
Responsable: Administradores de Red (Encargado TICs).	
Ubicación: BACO UGT-ESPE TIC's	
Número: 1	
Tipo: () [host] grandes equipos () [mid] equipos medios () [pc] informática personal () [mobile] informática móvil () [pda] agendas electrónicas () [vhost] equipo virtual () [backup] equipamiento de respaldo () [peripheral] periféricos () [print] medios de impresión () [scan] escáneres () [crypto] dispositivos criptográficos () [bp] dispositivo de frontera () [network] soporte de la red () [modem] módems () [hub] concentradores () [switch] conmutadores () [router] encaminadores () [bridge] pasarelas **(X)[firewall] cortafuegos**	

() [wap] punto de acceso inalámbrico () [pabx] centralita telefónica () [ipphone] teléfono IP

Dependencias de activos inferiores

Activo: Administrador de Red (Encargado TICs)	**Grado:** 100%
¿Por qué? Es el técnico especializado en tener en buen funcionamiento cada uno de los equipos de la Institución.	
Activo: TICs	**Grado:** 75%

Activo: Administrador de Red	**Grado:** 50%
¿Por qué? Si la persona encargada puede realizar un mal direccionamiento, o establece una mala configuración puede dañar la comunicación.	

Para la recolección del grado de dependencia está basado en la siguiente tabla:

Tabla 4

Estimación de Dependencias

Niveles	Dependencia
25%	Poco
50%	Medio
75%	Alto
100%	Muy Alto

Fuente: (Rosero Álvarez Edison Oswaldo, 2014)

En la ficha de información, se debe realizar para cada activo que se identifique en la organización.

3.8.4. Pasos de Análisis de Riegos

Según Rosero Edison (2014), en su trabajo de investigación de Análisis de riesgos de la seguridad de la red de área local (LAN) de la matriz de la Contraloría General Del Estado, manifiesta que:

El Análisis de riesgos permite analizar cada uno de los elementos de forma metódica para llegar a conclusiones con fundamento.

Para el proceso de Análisis de riesgo se realizará los siguientes pasos:

Tabla 5

Pasos de Análisis de Riesgos

PASOS DE ANÁLISIS DE RIESGOS
Paso 1. Caracterización de los activos
1. Identificación de los activos
2. Dependencias entre activos
3. Valoración de los activos
Paso 2. Caracterización de las Amenazas
1. Identificación de las amenazas
2. Valoración de las amenazas
Paso 3. Caracterización de las salvaguardas
1. Identificación de las salvaguardas pertinentes
2. Valoración de las salvaguardas.
Paso 4. Estimación del estado de riesgo
1. Estimación del impacto
2. Estimación del riesgo

Fuente: (Rosero Álvarez Edison Oswaldo, pág. 38)

Según Rosero Edison (2014), en su trabajo de investigación de Análisis de riesgos de la seguridad de la red de área local (LAN) de la matriz de la Contraloría General Del Estado, manifiesta que:

La Metodología Magerit recomienda realizar paso por paso, el análisis de riesgos, como se observa en la Tabla 4 y la Figura 17 en la cual se indica, como primeros pasos la identificación de los activos, posteriormente la valoración de las amenazas que pueden afectar a los mismo y el establecimiento de las salvaguardas. Y como final la estimación del estado del riesgo.

Paso 1:

3.8.4.1. Identificación y Clasificación de Activos de la red LAN UGT-ESPE

La identificación de los Activos es uno de los pasos más importantes, ya que permite conocer cada uno de los elementos, valorarlos con exactitud, y a

que amenazas pueden estar expuestos. De la misma manera poder conocer cuál sería una posible solución, y actuar de manera acertada. (Rosero Álvarez Edison Oswaldo)

Tabla 6

Activos de Red

Activo	Descripción	Categoría	Ubicación	Responsable TIC's	Identificación Activo
Router CISCO	Enlace WAN	Capa 3	Rack Comunicación	Sgop. Luis Santana	Equipo
Router CISCO	Backup	Capa 3	Rack Comunicación	Sgop. Luis Santana	Equipo
Router CISCO	Enlace WAN	Capa 3	Rack Comunicación	Sgop. Luis Santana	Equipo
Router Mikrotik	Gestión WLAN Gestión WAN	Capa 3	Rack Comunicación	Sgop. Luis Santana	Equipo
Switch 24 puertos	Wireless Administrable	Capa 3	Rack Comunicación	Sgop. Luis Santana	Equipo
Switch 24 puertos	Wireless Administrable	Capa 2	Rack Comunicación	Sgop. Luis Santana	Equipo
Switch 24 puertos	No Administrable	Capa 2	Varias Áreas	Sgop. Luis Santana	Equipo
Switch 24 puertos	No Administrable	Capa 2	Varias Áreas	Sgop. Luis Santana	Equipo
Switch 24 puertos	No Administrable	Capa 2	Varias Áreas	Sgop. Luis Santana	Equipo
Switch 16 puertos	No Administrable	Capa 2	Varias Áreas	Sgop. Luis Santana	Equipo
Switch 16 puertos	No Administrable	Capa 2	Varias Áreas	Sgop. Luis Santana	Equipo
Switch 16 puertos	No Administrable	Capa 2	Varias Áreas	Sgop. Luis Santana	Equipo
Rack	Servidores	TIC's	Gabinete Cerrado TIC's	Sgop. Luis Santana	Equipo
Firewall	Firewall FortiGuard		BACO UGT-ESPE TIC's	Sgop. Luis Santana	Equipo
UPS 6KVA	Energía Respaldo TIC's	TIC's	TIC's	Sgop. Luis Santana	Equipo
Servidor Linux	Servicio Proxy Permisos Acceso RED	TIC's	TIC's	Sgop. Luis Santana	Equipo
Instalación	Departamento TIC's	TIC's	TIC's	Sgop. Luis Santana	Equipo
Personal	Administrador de Red	Personal	TIC's	Sgop. Luis Santana	Personal

	Soporte Técnico	Personal	TIC's	Sgop. Luis Santana	Personal

[SW] SOFTWARE

Según Rosero Edison (2014), en su trabajo de investigación de Análisis de riesgos de la seguridad de la red de área local (LAN) de la matriz de la Contraloría General Del Estado, manifiesta que:

Con múltiples denominaciones (programas, aplicativos, desarrollos, etc.) este epígrafe se refiere a tareas que han sido automatizadas para su desempeño por un equipo informático. Las aplicaciones gestionan, analizan y transforman los datos permitiendo la explotación de la información para la prestación de los servicios.

[SW] SOFTWARE

Tabla 7

Tabulación Activos Software (SWSOLinux)

[SW] Software	
Código: SWSOLinux	**Nombre:** Sistema Operativo Linux
Descripción: GNU/Linux, también conocido como Linux, es un sistema operativo libre tipo Unix; multiplataforma, multiusuario y multitarea.	
Responsable: Administradores de Red (Encargado TICs).	
Ubicación: TICs	
Número: 1	
Tipo: () [prp]desarrollo propio (in house) () [sub]desarrollo a medida (subcontratado) () [std] estándar (off the shelf) () [browser] navegador web () [www] servidor de presentación () [app] servidor de aplicaciones () [email_client] cliente de correo electrónico () [email_server] servidor de correo electrónico () [directory] servidor de directorio () [file] servidor de ficheros () [dbms] sistema de gestión de base de datos () [tm] monitor transaccional () [office] ofimática () [os] sistema operativo () [windows] Windows	

() [solaris] Solaris **(X) [linux] Linux** () [macosx] mac osx () [hypervisor] hypervisor (gestor de la máquina virtual) () [ts] servidor de terminales () [backup] servidor de backup () [sec] herramientas de seguridad () [av] antivirus () [ids] IDS / IPS (detección / prevención de intrusión) () [dlp] prevención de pérdida de datos () [traf] análisis de tráfico () [hp] honey pot

Dependencias de activos inferiores

Activo: Administrador de Red (Encargado TICs)	**Grado:** 100%
¿Por qué? Personal especializado para el manejo del sistema.	
Activo: TICs	**Grado:** 75%

Activo: Administrador de Red	**Grado:** 50%
¿Por qué? Si la persona encargada realiza un mal manejo, el servicio podría dejar de funcionar.	

[HW]EQUIPOS INFORMÁTICOS (Hardware)

Según Rosero Edison (2014), en su trabajo de investigación de Análisis de riesgos de la seguridad de la red de área local (LAN) de la matriz de la Contraloría General Del Estado, manifiesta que:

Los equipos físicos, que soportan directa o indirectamente los servicios que presta la organización, siendo depósitos temporales o permanentes de los datos".

Los Activos de Hardware que posee la Unidad de Gestión de Tecnologías-ESPE son:

- Firewall
- Switch Core HP
- Switch de Distribución Linksys
- Switch de Acceso DLink
- Router Cisco
- Router Mikrotik

- Servidor Linux
- Switch Capa 2

[HW] HARDWARE

Tabla 8

Tabulación Activos Hardware (HWFirewall)

[HW] Equipamiento Informático (Hardware)	
Código: HWFirewall	**Nombre:** Cortafuegos
Descripción: Un firewall es un elemento de hardware o software utilizado en una red de computadoras para controlar las comunicaciones.	
Responsable: Administradores de Red (Encargado TICs).	
Ubicación: BACO UGT-ESPE TIC's	
Número: 1	
Tipo: () [host] grandes equipos (host) () [mid] equipos medios () [pc] informática personal () [mobile] informática móvil () [pda] agendas electrónicas () [vhost] equipos virtuales (máquinas virtuales) () [cluster] cluster () [backup] equipamiento de respaldo () [data] que almacena datos () [peripheral] periféricos () [print] medios de impresión () [scan] escáner () [crypto] dispositivo criptográfico () [robot] robots () [tape] ... de cintas () [disk] ... de discos () [network] soporte de la red () [modem] módem () [hub] concentrador () [switch] conmutador () [router] encaminador () [bridge] puente **(X) [firewall] cortafuegos** () [wap] punto de acceso wireless () [pabx] centralita telefónica () [ipphone] teléfono IP () [ics] Sistemas de control industrial () [rtu]RTU - Unidad terminal remota () [plc] PLC - Controlador lógico programable () [pac] PAC - Controlador de automatización programable () [ied] IED - Dispositivo electrónico inteligente () [meter] Meter – Medidor industrial () [bridge] Puente entre protocolos	

() [hmi] HMI – Interfaz hombre-máquina () [server] servidor () [historian] Registro histórico () [telemetry] Telemetría () [ems] EMS – Sistema de gestión de energía () [dms] DMS – Sistema de gestión de distribución () [home] Red de control de hogar () [hvac] HVAC – Acondicioner de temperatura

Dependencias de activos inferiores

Activo: Administrador de Red (Encargado TICs)	**Grado:** 100%
¿Por qué? Si la persona encargada en tener en buen funcionamiento cada uno de los equipos de la Institución.	
Activo: TICs	**Grado:** 75%

Activo: Administrador de Red	**Grado:** 50%
¿Por qué? Si la persona encargada puede realizar un mal direccionamiento, o establece una mala configuración puede dañar la comunicación.	

[HW] HARDWARE

Tabla 9

Tabulación Activos Hardware (HWSwitch Core HP)

[HW] Equipamiento Informático (Hardware)	
Código: HWSwitch Core HP	**Nombre:** Switch Core HP o Núcleo
Descripción: El Switch Core conocido también como backbone o el núcleo de la red, donde su función es llevar grandes cantidades de tráfico de manera confiable y veloz	
Responsable: Administradores de Red (Encargado TICs).	
Ubicación: Rack Comunicación Gabinete TIC's	
Número: 2	
Tipo: () [host] grandes equipos (host) () [mid] equipos medios () [pc] informática personal () [mobile] informática móvil () [pda] agendas electrónicas () [vhost] equipos virtuales (máquinas virtuales) () [cluster] cluster () [backup] equipamiento de respaldo () [data] que almacena datos () [peripheral] periféricos () [print] medios de impresión () [scan] escáner	

() [crypto] dispositivo criptográfico () [robot] robots () [tape] ... de cintas () [disk] ... de discos () [network] soporte de la red () [modem] módem () [hub] concentrador **(X) [switch] conmutador** () [router] encaminador () [bridge] puente () [firewall] cortafuegos () [wap] punto de acceso wireless () [pabx] centralita telefónica () [ipphone] teléfono IP () [ics] Sistemas de control industrial () [rtu]RTU - Unidad terminal remota () [plc] PLC - Controlador lógico programable () [pac] PAC - Controlador de automatización programable () [ied] IED - Dispositivo electrónico inteligente () [meter] Meter – Medidor industrial () [bridge] Puente entre protocolos () [hmi] HMI – Interfaz hombre-máquina () [server] servidor () [historian] Registro histórico () [telemetry] Telemetría () [ems] EMS – Sistema de gestión de energía () [dms] DMS – Sistema de gestión de distribución () [home] Red de control de hogar () [hvac] HVAC – Acondicioner de temperatura

Dependencias de activos inferiores

Activo: Administrador de Red (Encargado TIC's)	**Grado:** 100%
¿Por qué? Si la persona encargada de las TIC's establece un mal direccionamiento no habría comunicación en el servicio.	
Activo: Rack Comunicación Gabinete TIC's	**Grado:** 75%
¿Por qué? Ya que si sufriera algún accidente el Rack Gabinete el Switch Core sufriría daños y como consecuencia se perdería la comunicación.	

[HW] HARDWARE

Tabla 10

Tabulación Activos Hardware (HWSwitch Distribución Linksys)

[HW] Equipamiento Informático (Hardware)	
Código: HWSwitch Distribución Linksys	**Nombre:** Switch de Distribución Linksys

Descripción: El Switch de Distribución es el medio de comunicación entre la capa de acceso y el Core
Responsable: Administradores de Red (Encargado TICs).
Ubicación: Rack Comunicación Gabinete TIC's
Número: 3
Tipo: () [host] grandes equipos (host) () [mid] equipos medios () [pc] informática personal () [mobile] informática móvil () [pda] agendas electrónicas () [vhost] equipos virtuales (máquinas virtuales) () [cluster] cluster () [backup] equipamiento de respaldo () [data] que almacena datos () [peripheral] periféricos () [print] medios de impresión () [scan] escáner () [crypto] dispositivo criptográfico () [robot] robots () [tape] ... de cintas () [disk] ... de discos () [network] soporte de la red () [modem] módem () [hub] concentrador **(X) [switch] conmutador** () [router] encaminador () [bridge] puente () [firewall] cortafuegos () [wap] punto de acceso wireless () [pabx] centralita telefónica () [ipphone] teléfono IP () [ics] Sistemas de control industrial () [rtu]RTU - Unidad terminal remota () [plc] PLC - Controlador lógico programable () [pac] PAC - Controlador de automatización programable () [ied] IED - Dispositivo electrónico inteligente () [meter] Meter – Medidor industrial () [bridge] Puente entre protocolos () [hmi] HMI – Interfaz hombre-máquina () [server] servidor () [historian] Registro histórico () [telemetry] Telemetría () [ems] EMS – Sistema de gestión de energía () [dms] DMS – Sistema de gestión de distribución () [home] Red de control de hogar () [hvac] HVAC – Acondicioner de temperatura

Dependencias de activos inferiores

Activo: Administrador de Red (Encargado TIC's)	**Grado:** 100%
¿Por qué? Si la persona encargada de las TIC's establece un mal direccionamiento no habría comunicación en el servicio.	

Activo: Rack Comunicación Gabinete TIC's	**Grado:** 75%
¿Por qué? Ya que si sufriera algún accidente el Rack Gabinete el Switch de Distribución sufriría daños y como consecuencia se perdería la comunicación.	

[HW] HARDWARE

Tabla 11

Tabulación Activos Hardware (HWSwitch Acceso DLink)

[HW] Equipamiento Informático (Hardware)	
Código: HWSwitch Acceso DLink	**Nombre:** Switch de Acceso DLink
Descripción: El Switch de Acceso en esta capa es el punto de entrada para los usuarios finales a sus diferentes estaciones de trabajo y también los servidores de la red LAN.	
Responsable: Administradores de Red (Encargado TICs).	
Ubicación: Rack Comunicación Gabinete TIC's	
Número: 4	
Tipo: () [host] grandes equipos (host) () [mid] equipos medios () [pc] informática personal () [mobile] informática móvil () [pda] agendas electrónicas () [vhost] equipos virtuales (máquinas virtuales) () [cluster] cluster () [backup] equipamiento de respaldo () [data] que almacena datos () [peripheral] periféricos () [print] medios de impresión () [scan] escáner () [crypto] dispositivo criptográfico () [robot] robots () [tape] ... de cintas () [disk] ... de discos () [network] soporte de la red () [modem] módem () [hub] concentrador **(X) [switch] conmutador** () [router] encaminador () [bridge] puente () [firewall] cortafuegos () [wap] punto de acceso wireless () [pabx] centralita telefónica () [ipphone] teléfono IP () [ics] Sistemas de control industrial () [rtu]RTU - Unidad terminal remota () [plc] PLC - Controlador lógico programable	

() [pac] PAC - Controlador de automatización programable () [ied] IED - Dispositivo electrónico inteligente () [meter] Meter – Medidor industrial () [bridge] Puente entre protocolos () [hmi] HMI – Interfaz hombre-máquina () [server] servidor () [historian] Registro histórico () [telemetry] Telemetría () [ems] EMS – Sistema de gestión de energía () [dms] DMS – Sistema de gestión de distribución () [home] Red de control de hogar () [hvac] HVAC – Acondicioner de temperatura

Dependencias de activos inferiores

Activo: Administrador de Red (Encargado TIC's)	**Grado:** 100%
¿Por qué? Si la persona encargada de las TIC's establece un mal direccionamiento no habría comunicación en el servicio.	
Activo: Rack Comunicación Gabinete TIC's	**Grado:** 75%
¿Por qué? Ya que si sufriera algún accidente el Rack Gabinete el Switch de Acceso sufriría daños y como consecuencia se perdería la comunicación.	

[HW] HARDWARE

Tabla 12

Tabulación Activos Hardware (HWRouter Cisco)

[HW] Equipamiento Informático (Hardware)	
Código: HWRouter Cisco	**Nombre:** Router Cisco Capa 3
Descripción: Los routers CISCO pueden transformar la red y ofrecen gran seguridad y un servicio confiable en las redes de campus. También está actuando como Backup.	
Responsable: Administradores de Red (Encargado TICs).	
Ubicación: Rack Comunicación Gabinete TIC's	
Número: 5	
Tipo: () [host] grandes equipos (host) () [mid] equipos medios () [pc] informática personal () [mobile] informática móvil () [pda] agendas electrónicas () [vhost] equipos virtuales (máquinas virtuales) () [cluster] cluster **(X) [backup] equipamiento de respaldo** () [data] que almacena datos () [peripheral] periféricos () [print] medios de impresión () [scan] escáner	

() [crypto] dispositivo criptográfico () [robot] robots () [tape] ... de cintas () [disk] ... de discos () [network] soporte de la red () [modem] módem () [hub] concentrador () [switch] conmutador () [router] encaminador () [bridge] puente () [firewall] cortafuegos () [wap] punto de acceso wireless () [pabx] centralita telefónica () [ipphone] teléfono IP () [ics] Sistemas de control industrial () [rtu]RTU - Unidad terminal remota () [plc] PLC - Controlador lógico programable () [pac] PAC - Controlador de automatización programable () [ied] IED - Dispositivo electrónico inteligente () [meter] Meter – Medidor industrial () [bridge] Puente entre protocolos () [hmi] HMI – Interfaz hombre-máquina () [server] servidor () [historian] Registro histórico () [telemetry] Telemetría () [ems] EMS – Sistema de gestión de energía () [dms] DMS – Sistema de gestión de distribución () [home] Red de control de hogar () [hvac] HVAC – Acondicioner de temperatura

Dependencias de activos inferiores

Activo: Administrador de Red (Encargado TIC's)	**Grado:** 100%
¿Por qué? Si la persona encargada de las TIC's establece un mal direccionamiento no habría comunicación en el servicio.	
Activo: Rack Comunicación Gabinete TIC's	**Grado:** 75%
¿Por qué? Ya que si sufriera algún accidente el Rack Gabinete el Router Cisco sufriría daños y como consecuencia se perdería la comunicación.	

[HW] HARDWARE

Tabla 13

Tabulación Activos Hardware (HWRouter Mikrotik)

[HW] Equipamiento Informático (Hardware)	
Código: HWRouter Mikrotik	**Nombre:** Router Capa 3
Descripción: El Router Mikrotik para el control de los accesos de usuarios, encargado de la Gestión WLAN y WAN de la red.	
Responsable: Administradores de Red (Encargado TICs).	

Ubicación: Rack Comunicación Gabinete TIC's
Número: 6
Tipo: () [host] grandes equipos (host) () [mid] equipos medios () [pc] informática personal () [mobile] informática móvil () [pda] agendas electrónicas () [vhost] equipos virtuales (máquinas virtuales) () [cluster] cluster () [backup] equipamiento de respaldo () [data] que almacena datos () [peripheral] periféricos () [print] medios de impresión () [scan] escáner () [crypto] dispositivo criptográfico () [robot] robots () [tape] ... de cintas () [disk] ... de discos () [network] soporte de la red () [modem] módem () [hub] concentrador () [switch] conmutador **(X) [router] encaminador** () [bridge] puente () [firewall] cortafuegos () [wap] punto de acceso wireless () [pabx] centralita telefónica () [ipphone] teléfono IP () [ics] Sistemas de control industrial () [rtu]RTU - Unidad terminal remota () [plc] PLC - Controlador lógico programable () [pac] PAC - Controlador de automatización programable () [ied] IED - Dispositivo electrónico inteligente () [meter] Meter – Medidor industrial () [bridge] Puente entre protocolos () [hmi] HMI – Interfaz hombre-máquina () [server] servidor () [historian] Registro histórico () [telemetry] Telemetría () [ems] EMS – Sistema de gestión de energía () [dms] DMS – Sistema de gestión de distribución () [home] Red de control de hogar () [hvac] HVAC – Acondicioner de temperatura

Dependencias de activos inferiores

Activo: Administrador de Red (Encargado TIC's)	**Grado:** 100%
¿Por qué? Si la persona encargada de las TIC's establece un mal direccionamiento no habría comunicación en el servicio.	
Activo: Rack Comunicación Gabinete TIC's	**Grado:** 75%
¿Por qué? Ya que si sufriera algún accidente el Rack Gabinete el Router Mikrotik sufriría daños y como consecuencia se perdería la comunicación.	

[HW] HARDWARE

Tabla 14

Tabulación Activos Hardware (HWServidor Linux)

[HW] Equipamiento Informático (Hardware)	
Código: HWServidor Linux	**Nombre:** Servidor Linux
Descripción: El servidor Linux es un servidor impulsado por el sistema operativo de código abierto de Linux. Ofrece a las empresas una opción de bajo costo para entregar contenido, aplicaciones y servicios como proxy, permisos y acceso en la institución.	
Responsable: Administradores de Red (Encargado TICs).	
Ubicación: TIC's	
Número: 7	
Tipo: () [host] grandes equipos (host) () [mid] equipos medios () [pc] informática personal () [mobile] informática móvil () [pda] agendas electrónicas () [vhost] equipos virtuales (máquinas virtuales) () [cluster] cluster () [backup] equipamiento de respaldo () [data] que almacena datos () [peripheral] periféricos () [print] medios de impresión () [scan] escáner () [crypto] dispositivo criptográfico () [robot] robots () [tape] ... de cintas () [disk] ... de discos () [network] soporte de la red () [modem] módem () [hub] concentrador () [switch] conmutador () [router] encaminador () [bridge] puente () [firewall] cortafuegos () [wap] punto de acceso wireless () [pabx] centralita telefónica () [ipphone] teléfono IP () [ics] Sistemas de control industrial () [rtu]RTU - Unidad terminal remota () [plc] PLC - Controlador lógico programable () [pac] PAC - Controlador de automatización programable () [ied] IED - Dispositivo electrónico inteligente () [meter] Meter – Medidor industrial () [bridge] Puente entre protocolos () [hmi] HMI – Interfaz hombre-máquina **(X) [server] servidor** () [historian] Registro histórico	

() [telemetry] Telemetría () [ems] EMS – Sistema de gestión de energía () [dms] DMS – Sistema de gestión de distribución () [home] Red de control de hogar () [hvac] HVAC – Acondicioner de temperatura

Dependencias de activos inferiores

Activo: Administrador de Red (Encargado TIC's)	**Grado:** 100%
¿Por qué? Si la persona encargada de las TIC's tener un mal uso podría causar que el servicio se pierda	
Activo: TIC's	**Grado:** 75%
¿Por qué? Si de pronto el servidor Linux podría tener algún daño, o en todo caso mala manipulación el servicio podría parar su funcionamiento.	

[HW] HARDWARE

Tabla 15

Tabulación Activos Hardware (HWSwitch)

[HW] Equipamiento Informático (Hardware)	
Código: HWSwitch	**Nombre:** Switch Capa 2
Descripción: El modelo de interconexión de sistemas abierto es un modelo de referencia utilizado para describir y explicar las comunicaciones de red.	
Responsable: Administradores de Red (Encargado TICs).	
Ubicación: TIC's	
Número: 8	
Tipo: () [host] grandes equipos (host) () [mid] equipos medios () [pc] informática personal () [mobile] informática móvil () [pda] agendas electrónicas () [vhost] equipos virtuales (máquinas virtuales) () [cluster] cluster () [backup] equipamiento de respaldo () [data] que almacena datos () [peripheral] periféricos () [print] medios de impresión () [scan] escáner () [crypto] dispositivo criptográfico () [robot] robots () [tape] ... de cintas () [disk] ... de discos () [network] soporte de la red () [modem] módem	

() [hub] concentrador **(X) [switch] conmutador** () [router] encaminador () [bridge] puente () [firewall] cortafuegos () [wap] punto de acceso wireless () [pabx] centralita telefónica () [ipphone] teléfono IP () [ics] Sistemas de control industrial () [rtu]RTU - Unidad terminal remota () [plc] PLC - Controlador lógico programable () [pac] PAC - Controlador de automatización programable () [ied] IED - Dispositivo electrónico inteligente () [meter] Meter – Medidor industrial () [bridge] Puente entre protocolos () [hmi] HMI – Interfaz hombre-máquina () [server] servidor () [historian] Registro histórico () [telemetry] Telemetría () [ems] EMS – Sistema de gestión de energía () [dms] DMS – Sistema de gestión de distribución () [home] Red de control de hogar () [hvac] HVAC – Acondicioner de temperatura

Dependencias de activos inferiores

Activo: Administrador de Red (Encargado TIC's)	**Grado:** 100%
¿Por qué? El mal uso o una mala configuración podrían causar que el servicio deje de funcionar.	
Activo: TIC's	**Grado:** 75%
¿Por qué? Al tener algún accidente como de mal uso o mala configuración podría causar la detención del servicio el cual ofrece este elemento.	

[AUX] Equipamiento Auxiliar

Equipo auxiliar con la que cuenta la Unidad de Gestión de Tecnologías ESPE:

- Rack Comunicación TICs
- UPS 6KVA

[AUX] Equipamiento Auxiliar

Tabla 16

Tabulación Activos Equipamiento Auxiliar (AUXRackC)

[AUX] Equipamiento Auxiliar	
Código: AUXRackC	**Nombre:** Rack Comunicación TICs

Descripción: Estante metálico cuya finalidad principal es la de alojar equipamiento electrónico, informático y de comunicaciones.
Responsable: Administradores de Red (Encargado TICs).
Ubicación: TIC's
Número: 1
Tipo: () [power] fuentes de alimentación () [ups] sai – sistemas de alimentación ininterrumpida () [gen] generadores eléctricos () [ac] equipos de climatización () [cabling] cableado de datos () [wire]cable eléctrico () [fiber] fibra óptica () [supply] suministros esenciales () [destroy] equipos de destrucción de soportes **(X) [furniture] mobiliario** () [safe] cajas fuertes

Dependencias de activos inferiores

Activo: Administrador de Red (Encargado TIC's)	**Grado:** 100%
¿Por qué? Al tener un accidente, o destruirse podría causar severos daños a cada uno de los elementos que se encuentran en su alojamiento.	
Activo: TIC's	**Grado:** 75%
¿Por qué? Podría causar severos daños si el Rack del servidor podría tener un accidente, detendría el servicio causando graves daños.	

[AUX] Equipamiento Auxiliar

Tabla 17

Tabulación Activos Equipamiento Auxiliar (AUXUPS 6KVA)

[AUX] Equipamiento Auxiliar	
Código: AUXUPS 6KVA	**Nombre:** UPS 6KVA
Descripción: Energía de respaldo, que garantiza energía en caso de cortarse el suministro eléctrico público.	
Responsable: Administradores de Red (Encargado TICs).	
Ubicación: TIC's	
Número: 2	
Tipo: () [power] fuentes de alimentación **(X) [ups] sai – sistemas de alimentación ininterrumpida** **(X) [gen] generadores eléctricos**	

() [ac] equipos de climatización () [cabling] cableado de datos () [wire]cable eléctrico () [fiber] fibra óptica () [supply] suministros esenciales () [destroy] equipos de destrucción de soportes () [furniture] mobiliario () [safe] cajas fuertes

Dependencias de activos inferiores

Activo: Administrador de Red (Encargado TIC's)	**Grado:** 100%
¿Por qué? Si sufre algún incidente, o tenga un mal uso el generador podría dañarse y no rendir en el momento de necesitarlo.	
Activo: TIC's	**Grado:** 75%
¿Por qué? Tuviera un accidente por errores de mantenimiento, uso no previsto, podría tener daños y dejar sin el servicio de electricidad en caso de necesitarlo.	

[L]INSTALACIONES

Según Rosero Edison (2014), en su trabajo de investigación de Análisis de riesgos de la seguridad de la red de área local (LAN) de la matriz de la Contraloría General Del Estado, manifiesta que:

Aquí se puede identificar los lugares en donde se hospedan cada uno de los sistemas de información.

La Unidad de Gestión de Tecnologías ESPE cuenta con la siguiente instalación:

- Cuarto de Comunicaciones TIC's

[L]INSTALACIONES

Tabla 18

Tabulación Activos Instalaciones (LCuartoComunicacion)

[L] Instalaciones	
Código: LCuartoComunicacion	**Nombre:** Cuarto de Comunicación TIC's
Descripción: Cuarto en el cual se tiene cada uno de los elementos de comunicaciones de la Unidad de Gestión de Tecnologías ESPE	
Responsable: Administradores de Red (Encargado TICs).	
Ubicación: TIC's	

Número: 1
Tipo: () [site] recinto () [building] edificio **(X) [local] cuarto** () [mobile] plataformas móviles () [car] vehículo terrestre: coche, camión, etc. () [plane] vehículo aéreo: avión, etc. () [ship] vehículo marítimo: buque, lancha, etc. () [shelter] contenedores () [channel] canalización () [backup]instalaciones de respaldo

Dependencias de activos inferiores

Activo: Administrador de Red (Encargado TIC's)	**Grado:** 100%
¿Por qué? Personal que tiene acceso.	
Activo: Personal de Soporte Técnico	**Grado:** 75%
¿Por qué? Velen por la seguridad del Cuarto de Comunicación de las TIC's y cada uno de los elementos que allí contiene.	

[P] PERSONAL

En este tipo de activos aparecen las personas relacionadas con los sistemas de comunicaciones. Además, este tipo de activos (Personal) no se identifican dependencias. (Rosero Álvarez Edison Oswaldo, 2014)

En la Unidad de Gestión de Tecnologías ESPE se ha podido identificar lo siguiente:

- Administrador de Red
- Soporte Técnico

[P] PERSONAL

Tabla 19

Tabulación Activos Personal (PAdminRedes)

[P] Personal	
Código: PAdminRedes	**Nombre:** Administradores de Red
Descripción: Persona especializada encargada de las TIC's, de la Unidad de Gestión de Tecnologías ESPE.	
Responsable: Administradores de Red (Encargado TICs).	
Ubicación: TIC's	

Número: 1
Tipo: () [ue] usuarios externos () [ui] usuarios internos () [op] operadores () [adm] administradores de sistemas **(X) [com] administradores de comunicaciones** () [dba] administradores de BBDD () [sec] administradores de seguridad () [dev] desarrolladores / programadores () [sub] subcontratas () [prov] proveedores () [other] otros

[P] PERSONAL

Tabla 20

Tabulación Activos Personal (PTechniSupport)

[P] Personal	
Código: PTechniSupport	**Nombre:** Personal Soporte Técnico
Descripción: Persona especializada encargada de las TIC's, de la Unidad de Gestión de Tecnologías ESPE.	
Responsable: Encargado TICs	
Ubicación: TIC's	
Número: 2	
Tipo: () [ue] usuarios externos () [ui] usuarios internos **(X) [op] operadores** () [adm] administradores de sistemas () [com] administradores de comunicaciones () [dba] administradores de BBDD () [sec] administradores de seguridad () [des] desarrolladores / programadores () [sub] subcontratas () [prov] proveedores	

3.8.4.2. Valoración de los Activos

Según Rosero Edison (2014), en su trabajo de investigación de Análisis de riesgos de la seguridad de la red de área local (LAN) de la matriz de la Contraloría General Del Estado, manifiesta que:

La valoración de los activos se basa en los pasos anteriores, para la valoración se identifica en que dimensión es valioso un activo y se valora el coste de la destrucción del activo, para esta tarea se utiliza los criterios de valoración que a continuación se muestra en la siguiente tabla.

Tabla 21

Criterios de Valoración de Activos

VALOR		CRITERIO
10	Extremo	Daño extremadamente grave
9	Muy alto	Daño muy grave
6-8	Alto	Daño grave
3-5	Medio	Daño importante
1-2	Bajo	Daño menor
0	Despreciable	Irrelevante a efectos prácticos

Fuente: (Rosero Álvarez Edison Oswaldo, 2014, pág. 63)

Paso 2

3.8.4.3. Identificación de Amenazas

Posterior de la identificación de los activos, se debe también identificar las amenazas que pueden afectar a cada activo. (Rosero Álvarez Edison Oswaldo, 2014)

Valoración de las Amenazas

Para la valoración de la amenaza se debe tener en cuenta la frecuencia y la degradación, con las cuales se puede obtener la vulnerabilidad en el activo. (Rosero Álvarez Edison Oswaldo, 2014)

Riesgo= Frecuencia * Degradación

(Quintero Villarroya & SDG TIC. Ministerio de Defensa, 2012)

Según (Rosero Álvarez Edison Oswaldo), en su trabajo de investigación dice que:

La degradación mide el daño causado por un incidente en el supuesto de que ocurriera. Se caracteriza con una fracción del valor del activo.

A continuación, se muestra la escala que se tomara en consideración.

Tabla 22

Escala de Degradación

NIVELES	DEGRADACIÓN
25%	Poco(P)
50%	Medio(M)
75%	Alto(A)
100%	Muy Alto (MA)

Fuente: (Rosero Álvarez Edison Oswaldo, 2014)

Según (Rosero Álvarez Edison Oswaldo), en su investigación dice que:

La frecuencia es cada cuanto se materializa la amenaza, se modela como una tasa anual de ocurrencia, siendo valores típicos.

Tabla 23

Escala de Frecuencia

PRIORIDAD	FRECUENCIA
360	A Diario
12	Mensualmente
4	Cuatro veces al año
2	Dos veces al año
1	Una vez al año
½	Cada varios años

Fuente: (Rosero Álvarez Edison Oswaldo, 2014, pág. 65)

En la siguiente tabla se puede observar cada una de las amenazas a los cuales pueden estar expuestos los diferentes activos identificados de la red

LAN de la Unidad de Gestión de Tecnologías ESPE, tomando en cuenta la frecuencia en la cual ocurren y el posible daño que pueden sufrir, basados en las tablas anteriormente descritas.

(F)= Frecuencia

(D)= Degradación

Tabla 24

Activos y Amenazas a las que están expuestas

CAPA	ACTIVO	AMENAZAS	(F)	(D)
Equipamiento	**Firewall**	▪ Fuego ▪ Daños por agua ▪ Desastres Naturales ▪ Desastres industriales ▪ Contaminación Mecánica ▪ Contaminación Electromagnética ▪ Avería de Origen físico o lógico ▪ Corte de suministro eléctrico ▪ Condiciones inadecuadas de temperatura o humedad ▪ Caída del sistema por agotamiento de recursos ▪ Errores del administrador ▪ Errores de mantenimiento actualización de programas ▪ Perdida de equipos ▪ Alteración de secuencia ▪ Acceso no autorizado ▪ Uso no previsto ▪ Manipulación del hardware ▪ Denegación de servicio ▪ Ataque destructivo	**360**	**75%**
		▪ Fuego ▪ Daños por agua ▪ Desastres Naturales ▪ Desastres industriales		

Equipamiento	**Switch Acceso DLink**	▪ Contaminación medioambiental ▪ Contaminación electromagnética ▪ Avería de origen físico o lógico ▪ Corte del suministro eléctrico ▪ Condiciones inadecuadas de temperatura o humedad ▪ Errores de mantenimiento/ actualización de equipos (hardware) ▪ Caída del sistema por agotamiento de recursos ▪ Pérdida de equipos ▪ Uso no previsto ▪ Acceso no autorizado ▪ Manipulación del hardware ▪ Denegación de servicio ▪ Robo de equipos ▪ Ataque destructivo	**12**	**50%**
Equipamiento	**Switch Distribución Linksys**	▪ Fuego ▪ Daños por agua ▪ Desastres Naturales ▪ Desastres industriales ▪ Contaminación medioambiental ▪ Contaminación electromagnética ▪ Avería de origen físico o lógico ▪ Corte del suministro eléctrico ▪ Condiciones inadecuadas de temperatura o humedad ▪ Errores de mantenimiento/ actualización de equipos (hardware) ▪ Caída del sistema por agotamiento de recursos ▪ Pérdida de equipos ▪ Uso no previsto ▪ Acceso no autorizado ▪ Manipulación del hardware ▪ Denegación de servicio	**12**	**50%**

		▪ Robo de equipos ▪ Ataque destructivo		
Equipamiento	**Switch Core HP**	▪ Fuego ▪ Daños por agua ▪ Desastres Naturales ▪ Desastres industriales ▪ Contaminación medioambiental ▪ Contaminación electromagnética ▪ Avería de origen físico o lógico ▪ Corte del suministro eléctrico ▪ Condiciones inadecuadas de temperatura o humedad ▪ Errores de mantenimiento/ actualización de equipos (hardware) ▪ Caída del sistema por agotamiento de recursos ▪ Pérdida de equipos ▪ Uso no previsto ▪ Acceso no autorizado ▪ Manipulación del hardware ▪ Denegación de servicio ▪ Robo de equipos ▪ Ataque destructivo	**12**	**75%**
Equipamiento	**Router Cisco**	▪ Fuego ▪ Daños por agua ▪ Desastres Naturales ▪ Desastres industriales ▪ Contaminación medioambiental ▪ Contaminación electromagnética ▪ Avería de origen físico o lógico ▪ Corte del suministro eléctrico ▪ Condiciones inadecuadas de temperatura o humedad ▪ Errores de mantenimiento/ actualización de equipos (hardware) ▪ Caída del sistema por agotamiento de recursos ▪ Pérdida de equipos	**12**	**50%**

		▪ Uso no previsto ▪ Acceso no autorizado ▪ Manipulación del hardware ▪ Denegación de servicio ▪ Robo de equipos Ataque destructivo		
Equipamiento	**Router Mikrotik**	▪ Fuego ▪ Daños por agua ▪ Desastres Naturales ▪ Desastres industriales ▪ Contaminación medioambiental ▪ Contaminación electromagnética ▪ Avería de origen físico o lógico ▪ Corte del suministro eléctrico ▪ Condiciones inadecuadas de temperatura o humedad ▪ Errores de mantenimiento/ actualización de equipos (hardware) ▪ Caída del sistema por agotamiento de recursos ▪ Pérdida de equipos ▪ Uso no previsto ▪ Acceso no autorizado ▪ Manipulación del hardware ▪ Denegación de servicio ▪ Robo de equipos Ataque destructivo	**12**	**50%**
Equipamiento	**Servidor Linux**	▪ Fuego ▪ Daños por agua ▪ Desastres Naturales ▪ Desastres industriales ▪ Contaminación medioambiental ▪ Contaminación electromagnética ▪ Avería de origen físico o lógico ▪ Corte del suministro eléctrico ▪ Condiciones inadecuadas de temperatura o humedad ▪ Errores de mantenimiento/	**12**	**75%**

		actualización de equipos (hardware) ▪ Caída del sistema por agotamiento de recursos ▪ Pérdida de equipos ▪ Uso no previsto ▪ Acceso no autorizado ▪ Manipulación del hardware ▪ Denegación de servicio ▪ Robo de equipos ▪ Ataque destructivo		
Equipamiento	**UPS 6KVA**	▪ Fuego ▪ Daños por agua ▪ Desastres naturales ▪ Desastres industriales ▪ Contaminación ambiental ▪ Interrupción de otros servicios o suministros esenciales ▪ Errores de mantenimiento / actualización de equipos (hardware) ▪ Uso no previsto ▪ Manipulación del hardware ▪ Robo de equipos ▪ Ataque destructivo	**12**	**75%**
Equipamiento	**Rack Servidor**	▪ Fuego ▪ Daños por agua ▪ Desastres naturales ▪ Desastres industriales ▪ Contaminación ambiental ▪ Interrupción de otros servicios o suministros esenciales ▪ Errores de mantenimiento / actualización de equipos (hardware) ▪ Uso no previsto ▪ Manipulación del hardware ▪ Robo de equipos ▪ Ataque destructivo	**4**	**50%**
		▪ Fuego ▪ Daños por agua ▪ Desastres naturales ▪ Desastres industriales		

Equipamiento	**Switch Capa 2**	▪ Contaminación medioambiental ▪ Contaminación electromagnética ▪ Avería de origen físico o lógico ▪ Corte del suministro eléctrico ▪ Condiciones inadecuadas de temperatura o humedad ▪ Emanaciones electromagnéticas ▪ Errores de mantenimiento / actualización de equipos (hardware) ▪ Caída del sistema por agotamiento de recursos ▪ Pérdida de equipos ▪ Uso no previsto ▪ Acceso no autorizado ▪ Manipulación del hardware ▪ Denegación de servicio ▪ Robo de equipos ▪ Ataque destructivo	**12**	**75%**
Equipamiento	**Sistema Operativo Linux**	▪ Avería de origen físico o lógico ▪ Difusión de software dañino ▪ Vulnerabilidades de los programas (software) ▪ Errores de mantenimiento/actualización de programas (software) ▪ Difusión de software dañino ▪ Manipulación de programas	**12**	**75%**
Instalaciones		▪ Fuego ▪ Daños por agua ▪ Desastres naturales ▪ Desastres industriales ▪ Contaminación medioambiental ▪ Contaminación electromagnética ▪ Avería de origen físico o lógico ▪ Corte del suministro eléctrico	**12**	**75%**

Personal	**Cuarto de Comunicación TICs**	▪ Condiciones inadecuadas de temperatura o humedad ▪ Emanaciones electromagnéticas ▪ Errores de mantenimiento / actualización de equipos (hardware) ▪ Caída del sistema por agotamiento de recursos ▪ Pérdida de equipos ▪ Uso no previsto ▪ Acceso no autorizado ▪ Manipulación del hardware ▪ Denegación de servicio ▪ Robo de equipos ▪ Ataque destructivo		
	Administradores de Red	▪ Destrucción de la información ▪ Fugas de información ▪ Indisponibilidad del personal ▪ Revelación de información ▪ Extorsión ▪ Ingeniería social (picaresca)	**12**	**75%**
	Soporte Técnico	▪ Destrucción de la información ▪ Fugas de información ▪ Indisponibilidad del personal ▪ Revelación de información ▪ Extorsión ▪ Ingeniería social (picaresca)	**12**	**75%**

En la anterior tabla se muestra cada uno de los activos de equipamiento, instalaciones y personal que cuenta la Unidad de Gestión de Tecnologías ESPE, juntamente con el porcentaje de degradación y frecuencia de que las amenazas puedan cristalizarse. En un mayor porcentaje se tiene el firewall, ya que uno de los elementos de seguridad el mismo el que puede ser atacado. Por otra parte, también se tiene en instalaciones el Cuarto de comunicación TICs, el cual tiene un porcentaje de 75% de degradación y con una frecuencia

de 12 lo mismo que significa que la amenaza puede afectar cada mes en el año lo mismo que podría ser crítico a nivel del servicio.

De la misma forma en el personal no es algo que necesariamente puede estar ocurriendo, pero en cuanto a evaluaciones el daño puede ser alto, en el momento de que una de las amenazas puedan cristalizarse como fugas de información, indisponibilidad de información e ingeniería social causando de esta manera un 75% de degradación o daño en el servicio y teniendo una frecuencia de 12 el mismo en el cual se corren riesgos los 12 meses del año por lo mismo que se debe tener en cuenta, la seguridad de la información que se manejada a terceros.

Al contrario de los porcentajes que se muestra en el caso del firewall personal e instalaciones, los activos con menos riesgos de degradación se encuentran en la capa de equipamiento como el rack del servidor ya que los daños no pueden ser tan recurrente por lo mismo cuenta con un nivel de daño del 50% en caso de que una amenaza pueda aparecer, por lo mismo la frecuencia para la amenaza está en 4 la misma que significa 4 veces al año, se ha establecido ese nivel ya que se debe estar pendiente para el mantenimiento para evitar daños.

Paso 3

3.8.4.4. Determinación del Impacto

Según Rosero Edison (2014), en su trabajo de investigación de Análisis de riesgos de la seguridad de la red de área local (LAN) de la matriz de la Contraloría General Del Estado, manifiesta que:

Permite conocer el alcance del daño producido, sobre todos los activos que se encuentran.

Los criterios de valoración que utiliza la herramienta de EAR/PILAR son seis como se muestra a continuación:

Tabla 25

Criterios de Valoración

Valor		Criterio
10	Extremo	[4]
9	Muy alto	Daño muy grave
6-8	Alto	Daño grave
3-5	Medio	Daño importante
1-2	Bajo	Daño menor
0	Despreciable	Irrelevante a efectos prácticos

Fuente: (Rosero Álvarez Edison Oswaldo, 2014, pág. 76)

Disponibilidad

Según Rosero Edison (2014), en su trabajo de investigación de Análisis de riesgos de la seguridad de la red de área local (LAN) de la matriz de la Contraloría General Del Estado, manifiesta que:

La disponibilidad es el aseguramiento de que los usuarios autorizados tienen acceso cuando lo requiera a la información y a sus activos asociados.

La siguiente dimensión de seguridad indica si habrá daños en la institución si se dejara de prestar el servicio.

Disponibilidad

ALTO

- **Obligaciones legales:** Probablemente cause un incumplimiento grave de una ley o regulación.
- **Seguridad:** Probablemente sea causa de un grave incidente de seguridad o dificulte la investigación de incidentes.
- **Interrupción del servicio:** Probablemente cause la interrupción de actividades propias de la Organización.
- **Orden Público:** Puede causar malestar público.
- **Operaciones:** Probablemente merme la eficacia o seguridad de la misión operativa o logística (alcance local).

- **Administración y Gestión:** Pudiera impedir la operación efectiva de una parte de la Organización.
- **Pérdida de Confianza:** Probablemente sea causa de una cierta publicidad negativa. (PILAR Análisis y Gestión de Riesgos Ayuda Versión 7.2, 2018)

Integridad:

Según Rosero Edison (2014), en su trabajo de investigación de Análisis de riesgos de la seguridad de la red de área local (LAN) de la matriz de la Contraloría General Del Estado, manifiesta que:

Es la garantía de la exactitud y completitud de la información y los métodos de su procesamiento.

ALTO

- **Obligaciones legales:** Probablemente cause un incumplimiento grave de una ley o regulación. (2018)
- **Seguridad:** Probablemente sea causa de un incidente excepcionalmente serio de seguridad o dificulte la investigación de incidentes excepcionalmente serios. (PILAR Análisis y Gestión de Riesgos Ayuda Versión 7.2, 2018)

Confidencialidad

Dicho campo es específicamente valorado por las personas con acceso autorizado ya que depende estrictamente de las personas encargadas el aseguramiento de la información en la institución. (Rosero Álvarez Edison Oswaldo)

Autenticidad

ALTO

- **Obligaciones legales:** Probablemente cause un incumplimiento grave de una ley o regulación.

- **Persecución de Delitos:** Dificulte la investigación o facilite la comisión de delitos. (PILAR Análisis y Gestión de Riesgos Ayuda Versión 7.2, 2018)

Trazabilidad:

Es el aseguramiento de que en todo momento se podrá determinar quién hizo que y en qué momento. (Rosero Álvarez Edison Oswaldo, 2014, pág. 79)

Irreparable

MEDIO

- **Obligaciones legales:** Probablemente cause un incumplimiento grave de una ley o regulación.
- **Pérdida de Confianza:** Probablemente sea causa de una cierta publicidad negativa. (PILAR Análisis y Gestión de Riesgos Ayuda Versión 7.2, 2018)

Valor

MEDIO

- **Obligaciones legales:** Probablemente cause un incumplimiento grave de una ley o regulación.
- **Administración y Gestión:** Pudiera impedir la operación efectiva de una parte de la Organización.
- **Pérdida de Confianza:** Probablemente sea causa de una cierta publicidad negativa. (PILAR Análisis y Gestión de Riesgos Ayuda Versión 7.2, 2018)

Datos Personales

ALTO

- **Obligaciones legales:** Probablemente cause un incumplimiento grave de una ley o regulación.

- **Seguridad:** Probablemente sea causa de un grave incidente de seguridad o dificulte la investigación de incidentes.
- **Orden Público:** Puede causar malestar público.
- **Operaciones:** Probablemente merme la eficacia o seguridad de la misión operativa o logística (alcance local).
- **Administración y Gestión:** Pudiera impedir la operación efectiva de una parte de la Organización. (2018)
- **Pérdida de Confianza:** Probablemente sea causa de una cierta publicidad negativa. (PILAR Análisis y Gestión de Riesgos Ayuda Versión 7.2, 2018)

Impacto Acumulado

El impacto acumulado, consiste en el análisis los valores del impacto potencial y los acumulados, en cada fase del proyecto, con el objetivo de poder obtener un informe del impacto potencial que cada activo podría sufrir, para dicho análisis se utilizó las técnicas gráficas. (Rosero Álvarez Edison Oswaldo, 2014)

Tabla 26

Impacto Acumulado Activos

Impacto Acumulado			
Activo	**Amenaza**	**Dimensión**	**Impacto**
[HWSwitch] Switch Capa 2	[A.24] Denegación de servicio	[D]	[5]
[HWServidor Linux] Servidor Linux	[A.24]Denegación de Servicio [A.26] Ataque Destructivo [E.25] Pérdida de equipos [I.6] Corte suministro eléctrico [I.7]Condiciones inadecuadas de temperatura o humedad	[D]	[4]

	[A.11] Acceso no autorizado [A.23] Manipulación del hardware [A.25] Robo de equipos	[C]	[7]
[HWRouter Mikrotik] Router Mikrotik	[A.24]Denegación de Servicio [A.26] Ataque Destructivo [I.6] Corte suministro eléctrico [I.7]Condiciones inadecuadas de temperatura o humedad	[D]	[5]
	[A.11] Acceso no autorizado	[I]	[2]
[HWRouter Cisco] Router Cisco Capa 3	[A.24]Denegación de Servicio [E.25] Pérdida de equipos [A.26] Ataque Destructivo [I.6] Corte suministro eléctrico [I.7]Condiciones inadecuadas de temperatura o humedad	[D]	[1]
	[A.11] Acceso no autorizado	[I]	[2]
[HWSwitch Accesso Dlink] Switch de Accesso DLink	[A.24]Denegación de Servicio [A.26] Ataque Destructivo [I.7]Condiciones inadecuadas de temperatura o humedad [I.5] Avería de origen físico o lógico	[D]	[5]
	[A.11] Acceso no autorizado	[I]	[1]
[HWSwitch Distribucion Linksys] Switch de Distribución Linksys	[A.24]Denegación de Servicio [A.26] Ataque Destructivo [I.6] Corte suministro eléctrico [I.7]Condiciones inadecuadas de temperatura o humedad [A.23] Manipulación del Hardware	[D]	[4]
[HWSwitch Core HP]	A.24]Denegación de Servicio [A.26] Ataque Destructivo	[D]	[1]

Switch Core HP	[I.6] Corte suministro eléctrico [I.7]Condiciones inadecuadas de temperatura o humedad [A.23] Manipulación de hardware		
[HWFirewall] Firewall (Cortafuegos]	[A.24] Denegación de servicio [A.26] Ataque Destructivo [I.6] Corte suministro eléctrico [I.7]Condiciones inadecuadas de temperatura o humedad [A.7] Uso no previsto	[D]	[8]
	[A.11] Acceso no autorizado	[I]	[5]
	[A.23] Manipulación del hardware [A.7] Uso no previsto	[C]	[7]
[AUXRackC] Rack Comunicación TICs	[I.*] Desastres Industriales [A.23] Manipulación del hardware	[D]	[1]
[AUXUPS 6KVA] UPS 6KVA	[I.9] Interrupción de otros servicios [A.26] Ataque destructivo [E.23] Errores de mantenimiento [A.23] Manipulación del hardware	[D]	[1]
[SWSOLinux] Sistema Operativo Linux	[A.8] Difusión de software dañino [I.5] Avería de origen físico o lógico [A.22] Manipulación de programas	[D]	[4]
	[A.8] Difusión de software dañino [E.20] Vulnerabilidades de los programas	[I]	[4]
[LCuartoComunicacion] Cuarto de Comunicación TICs	[N.2] Daños por agua [N.*] Desastres naturales [I.*] Desastres industriales [A.26] Ataque destructivo [A.27] Ocupación enemiga [A.7] Uso no previsto	[D]	[4]
[PadminRedes] Administradores de Red	[E.28] Indisponibilidad del personal [A.18] Destrucción de la información	[D]	[6]

	[A.15] Modificación de la información [A.19] Revelación de la información [A.29] Extorsión [A.30] Ingeniería social (picaresca) [E.15] Alteración de la información [A.18] Destrucción de la información	[I]	[7]
	[A.29] Extorsión [A.30] Ingeniería social (picaresca) [E.19] Fugas de información	[C]	[7]
[PTechniSupport] Personal Soporte Técnico	[E.28] Indisponibilidad del personal [A.18] Destrucción de la información	[D]	[6]
	[A.15] Modificación de la información [A.19] Revelación de la información [A.29] Extorsión [A.30] Ingeniería social (picaresca) [E.15] Alteración de la información [A.18] Destrucción de la información	[I]	[7]
	[A.29] Extorsión [A.30] Ingeniería social (picaresca) [E.19] Fugas de información	[C]	[7]

3.9. Práctica Pilar y Aplicación Metodología Magerit

Herramienta Pilar

La herramienta Pilar analiza cada uno de los activos de una organización, los mismos, que se encuentran proporcionados en el sistema. Calculando de esta manera las amenazas posibles, los riesgos y permiten incorporar salvaguardas (soluciones), para reducir el impacto y la degradación que podrían causar en caso de materializarse.

La herramienta Pilar soporta todas las fases de la Metodología Magerit:

1. Caracterización Activos: identificación, clases de activos y valoración.
2. Caracterización Amenazas: identificación y valoración.
3. Salvaguardas.

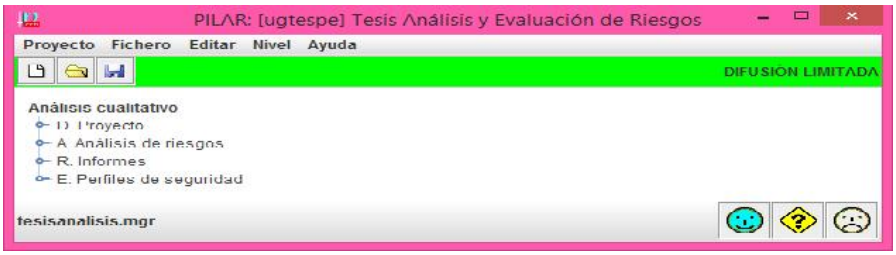


Figura 22 Análisis proyecto Pilar

La herramienta Pilar evalúa el impacto que puede tener una amenaza en uno o varios activos los mismos que pueden estar expuestos. De la misma forma permite visualizar el impacto y riesgo, acumulado y repercutido, potencial y residual, presentándolo en el análisis y posteriormente cada uno de los resultados también puede ser visualizado en gráficas.

A continuación, se muestra la plataforma y cada una de las fases del proyecto:

Las partes principales del proyecto que muestra Pilar son las siguientes:

- **D. Proyecto:** Aquí se muestra los datos del proyecto, Dominios de seguridad y fases del proyecto.
- **A. Análisis de riesgos:** Activos, amenazas y salvaguardas.
- **R. Informes:** Gráficas.
- **E. Perfiles de seguridad:** 27002:2013 Código de prácticas para los controles de seguridad de la información.

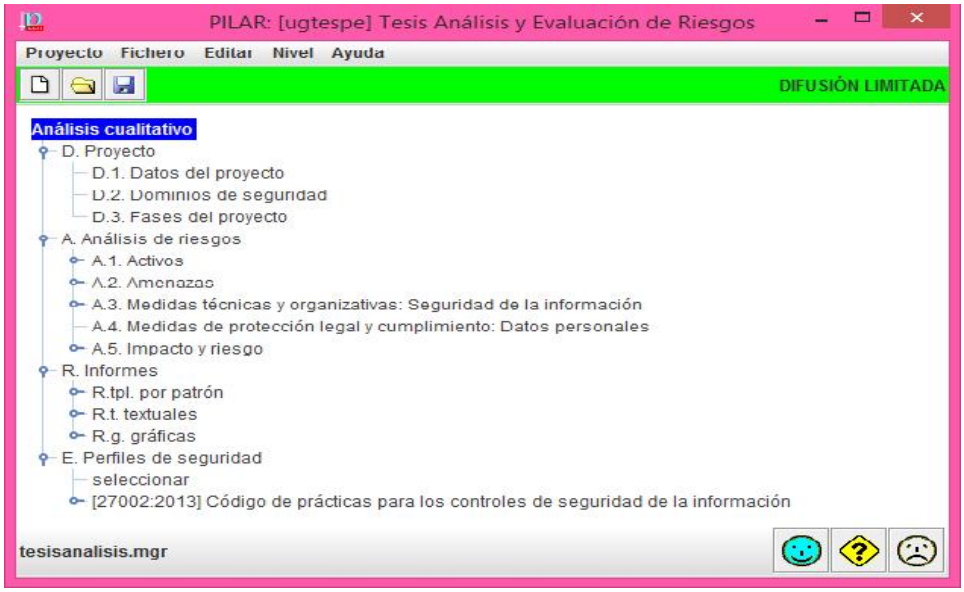


Figura 23 Partes principales del proyecto Herramienta Pilar

3.10. Datos del Proyecto

En la siguiente pantalla se puede apreciar cada uno de los campos que se necesita llenar para la creación de un nuevo proyecto de análisis, en el mismo que consta de las siguientes partes:

1. **Biblioteca:** La misma que es asignada por la herramienta misma.
2. **Código:** Código único para la creación del proyecto.
3. **Nombre:** Asignación del nombre del proyecto.
4. **Proyecto – clasificación:** Donde se puede escoger la clasificación del proyecto como puede ser secreto, reservado, confidencial, difusión limitada y sin clasificar.
5. Luego se muestra una serie de datos más como el nombre de la Organización, la descripción del proyecto, el autor, versión del programa y la fecha del análisis.
6. Pilar consta con las opciones de guardado representadas con una carita feliz y una carita triste según la necesidad. (PILAR Análisis y Gestión de Riesgos Ayuda Versión 7.2, 2018)

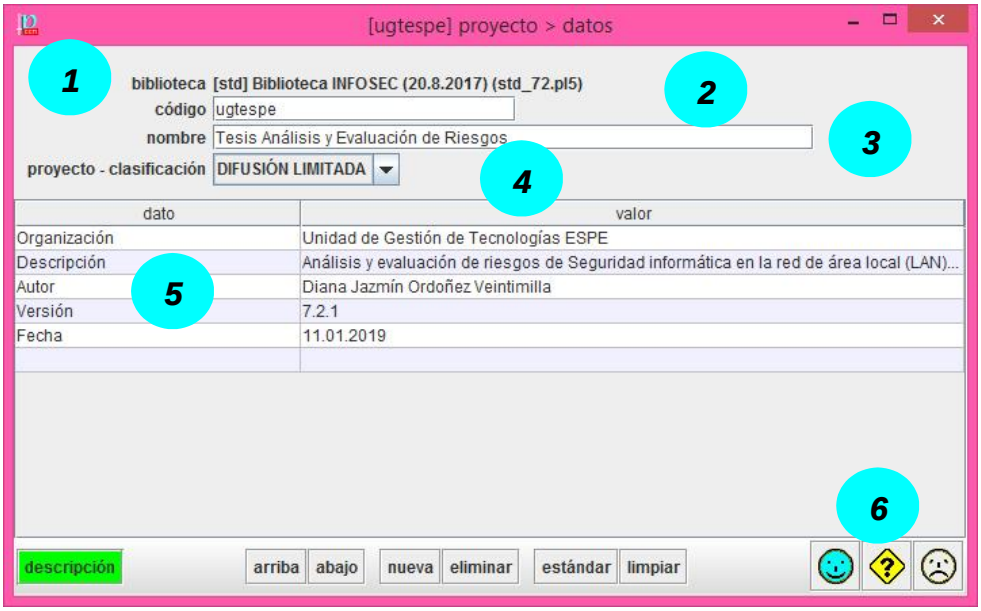


Figura 24 Datos del Proyecto

Además, Pilar cuenta con la opción de ingresar una pequeña descripción del proyecto donde se detalla el análisis a realizar.

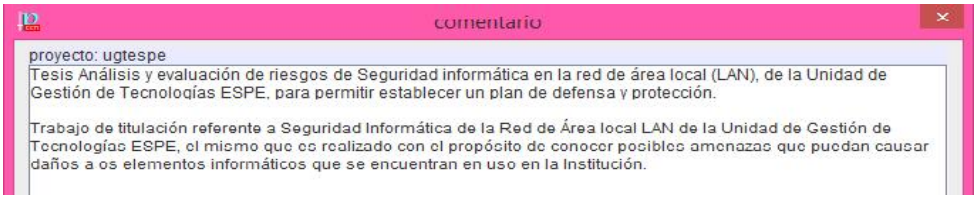


Figura 25 Descripción del Proyecto

Análisis de Riesgos Proyecto Pilar

3.11. Paso 1: Activos Red LAN Unidad de Gestión de Tecnologías ESPE

3.11.1. Identificación de Activos

1. En la Herramienta Pilar, el análisis de riesgos permite ingresar cada uno de los activos identificados en la organización.
    - **Equipamiento:** Hardware, Software, Equipamiento auxiliar, Instalaciones y Personal.

De esta manera clasificando cada uno de los activos por su función y capa que fueron creadas anteriormente.

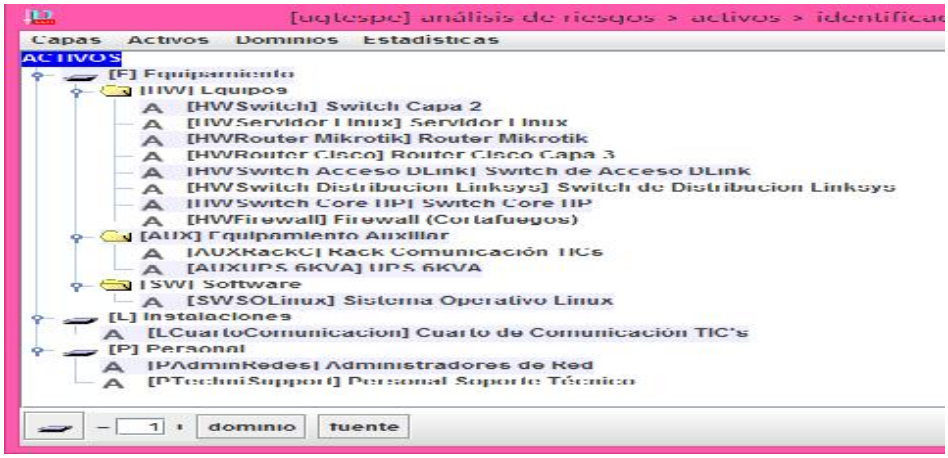


Figura 26 Identificación de Activos de Red

Para el ingreso de los activos se despliega una pantalla dos paneles, en el panel izquierdo, se puede ingresar el código con el cual se reconocerá al activo, el nombre, los datos del activo en conjunto con la fecha de ingreso del mismo, de la misma manera en el panel derecho se encuentran las opciones de clases de los activos según la necesidad en el cuan se puede escoger a que grupo pertenece según sus características de funcionamiento.

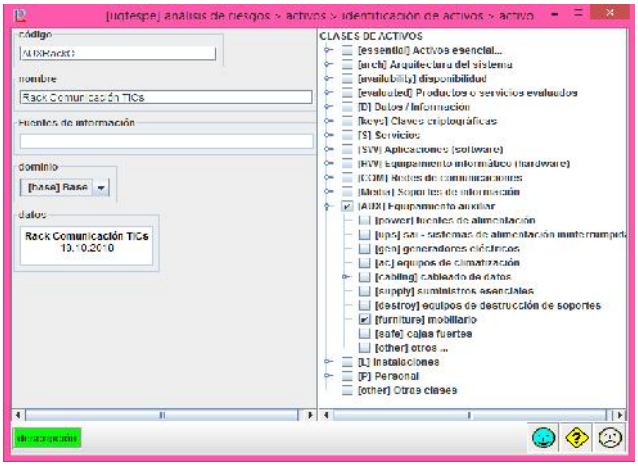


Figura 27 Ingreso de Activos

3.11.2. Clasificación de los Activos

A continuación, se muestra la pantalla de clasificación de los activos, la misma que consta de dos paneles un izquierdo en el cual se puede visualizar la lista de activos que fueron ingresados en el sistema en el paso anterior de identificación de los mismos.

Del mismo modo en la parte derecha se tiene los tipos o clases de activos que provee la misma herramienta, por lo que se puede ir clasificando de manera manual, según la información que se recolectó.

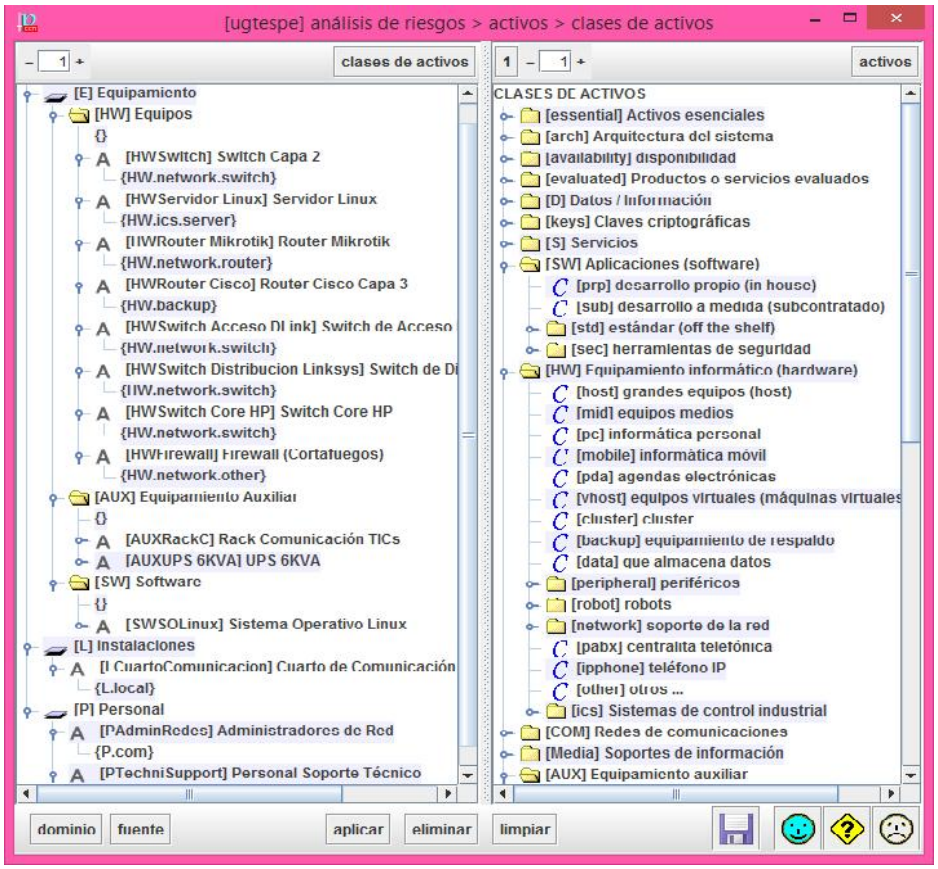


Figura 28 Clasificación de los Activos

3.11.3. Valoración de los Activos

A continuación, se procede a valorar cada uno de los activos, mostrando la puntuación asignada manualmente para cada uno de ellos, en cada una de

las dimensiones de seguridad que proporciona la herramienta (disponibilidad, integridad, confidencialidad, autenticidad, trazabilidad, valor y datos personales), cada uno de los valores son asignados de acuerdo a la Tabla 21 de Criterios de valoración de los activos indicados anteriormente.

Se debe tener en cuenta que la valoración que tiene cada uno de los activos, es asignada en la medida de degradación que pueda causar a la organización si el activo es afectado por una amenaza significativa.

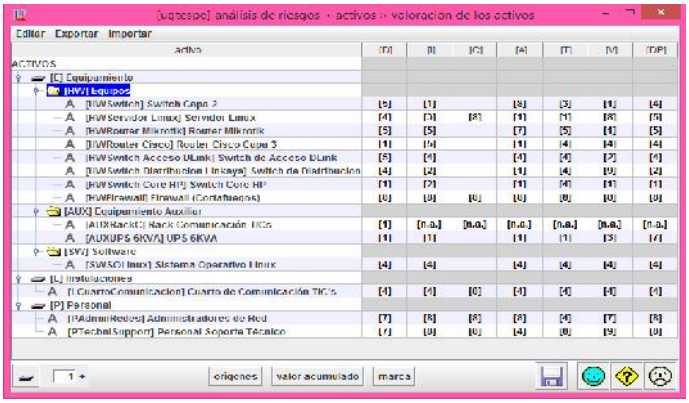


Figura 29 Valoración Activos

Los criterios de valoración que la herramienta Pilar despliega para cada una de las dimensiones son basadas en una serie de preguntas como se muestra en la figura. Las mismas que pueden ser escogidas según el daño que podría causar en caso de tener una amenaza activa.

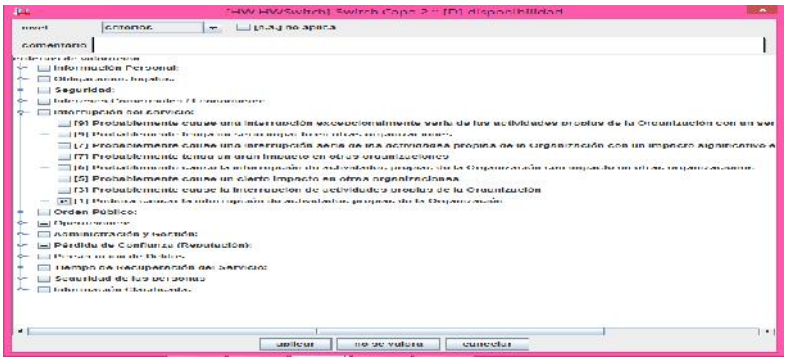


Figura 30 Criterios de Valoración

3.12. Paso 2: Amenazas Red LAN UGT – ESPE

3.12.1. Identificación de Amenazas

La herramienta Pilar de manera automáticamente asigna las amenazas, frecuencia, y el impacto que podrían causar las mismas en caso de producirse. Pilar cuenta con una biblioteca de colección de amenazas las mismas que se van asociando a cada uno de los activos, tomando en cuenta cada una de las clases a las cuales pertenecen.

Para la realización de este análisis se toman en cuenta las amenazas, de mayor probabilidad y que sean consecuentes a cada activo, según el caso de estudio.

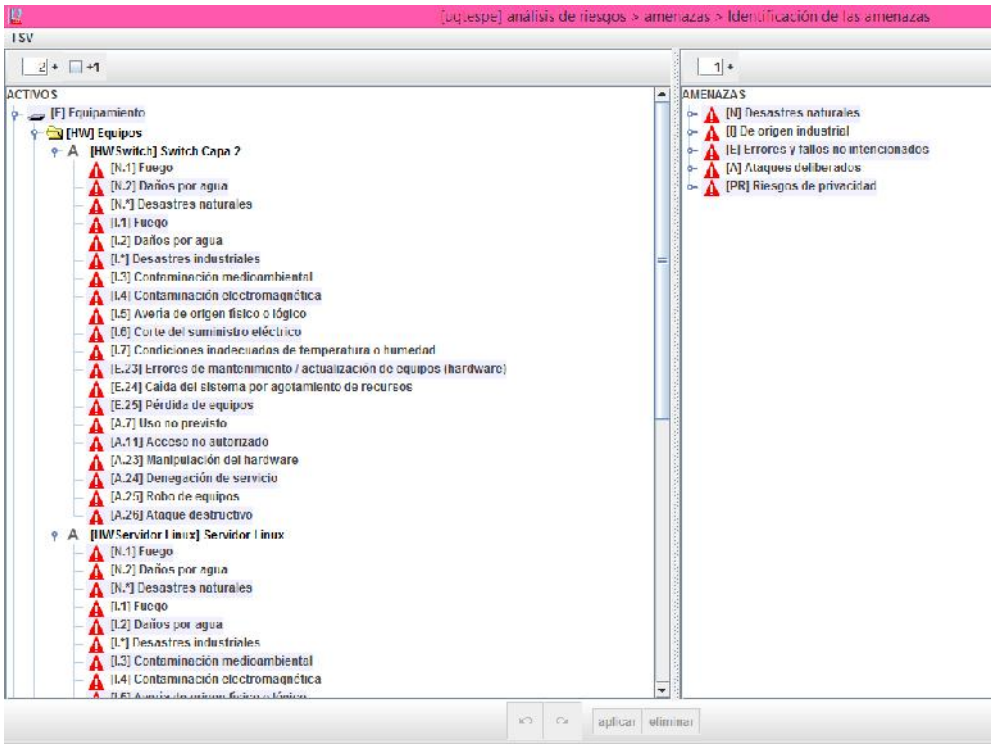


Figura 31 Identificación de Amenazas Pilar

3.12.2. Valoración de las Amenazas

A continuación, se muestra la valoración de cada una de las amenazas que fueron asociados a los activos, las mismas que definen las frecuencias o

probabilidad de la posible aparición de las mismas y el daño o degradación que pueda causar, teniendo de esta forma los porcentajes de las dimensiones de seguridad con mayor afectación.

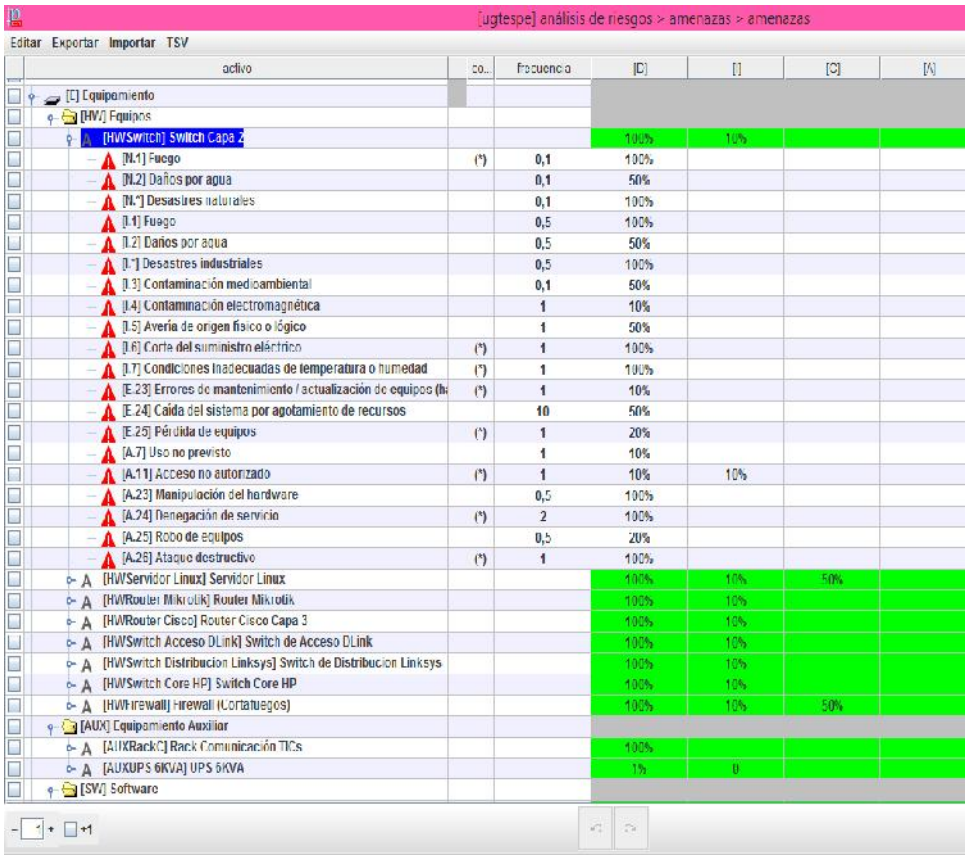


Figura 32 Valoración de amenazas

3.13. Paso 3: Medidas Técnicas y organizativas: Seguridad de la Información (Salvaguardas

3.13.1. Eficacia de las Salvaguardas

A continuación, se muestra cada una de las salvaguardas que la herramienta Pilar proporciona para poder evaluar cada uno de los activos. La evaluación consiste en asignar un nivel de madurez al proceso asociado con las amenazas y los activos.

Las salvaguardas se convierten en un medio para contraatacar las amenazas, las mismas que tienen aspectos ya sean organizativos, técnicos, físicos o relativos a la gestión del personal las mismas que son representadas con letras mayúsculas y mostradas en los primeros cuadros de la pantalla.

Aspectos que trata la salvaguarda:

- **G** para Gestión
- **T** para Técnico
- **F** para seguridad Física
- **P** para gestión del Personal

Además, las salvaguardas emiten un tipo de protección para cada uno de los activos en caso de que una amenaza se materialice siendo las siguientes:

- **PR:** prevención
- **DR:** disuasión
- **EL:** eliminación
- **IM:** minimización del impacto
- **CR:** corrección
- **RC:** recuperación
- **AD:** administrativa
- **AW:** concienciación
- **DC:** detección
- **MN:** monitorización

En las salvaguardas para poder evaluar el peso relativo de cada uno puede ser tratado desde crítico hasta un nivel bajo poco interesante, las mismas que son identificadas por figuras en forma de sombrillas asociados a los colores como se representa a continuación:

3	máximo peso	crítica
2	peso alto	muy importante
1	peso normal	importante
0	peso bajo	interesante
✓	aseguramiento: componentes certificados	

Figura 33 Peso relativo salvaguardas

Fuente: (PILAR Análisis y Gestión de Riesgos Ayuda Versión 7.2, 2018)

Para la valoración de cada una de las salvaguardas están clasificadas según la función y nivel de implantación de la misma. La misma que se puede verificar en la siguiente tabla:

Tabla 27

Valoración de Salvaguardas

NIVEL	EFECTIVIDAD
L0	0%
L1	10%
L2	50%
L3	90%
L4	95%
L5	100%

A continuación, se muestra cada una de las salvaguardas de acuerdo a los valores detallados anteriormente:

Figura 34 Salvaguardas (eficacia)

A continuación para poder observar cada uno de los riesgos, identificados para cada uno de los activos, se procede a selección una salvaguarda y dirigirse a la parte superior de la barra de opciones donde se puede hacer click en la opción Ver donde se desplegará una pantalla en la cual se podrá mostrar una tabla en la cual se puede ver cada una de las amenazas más relevantes según cada activo, en conjunto con la valoración del impacto que puede causar en las dimensiones del activo.

Figura 35 Selección Salvaguardas para verificación de riesgo

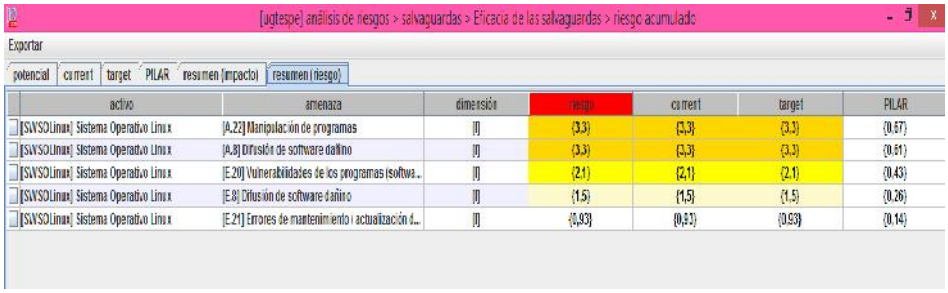


Figura 36 Riesgo Acumulado según el activo y la salvaguarda

Para la evaluación del riesgo acumulado la herramienta Pilar proporciona una tabla de valores en la cuales se puede identificar el grado de criticidad de la amenaza.

Figura 37 Niveles de criticidad para Riesgo Acumulado

Fuente: (PILAR Análisis y Gestión de Riesgos Ayuda Versión 7.2, 2018)

3.14. Impacto Acumulado

A continuación, se detalla los valores del impacto en cada uno de los activos tanto en hardware, software, instalaciones y al personal, el mismo que es evaluado según las amenazas que fueron detectadas anteriormente:

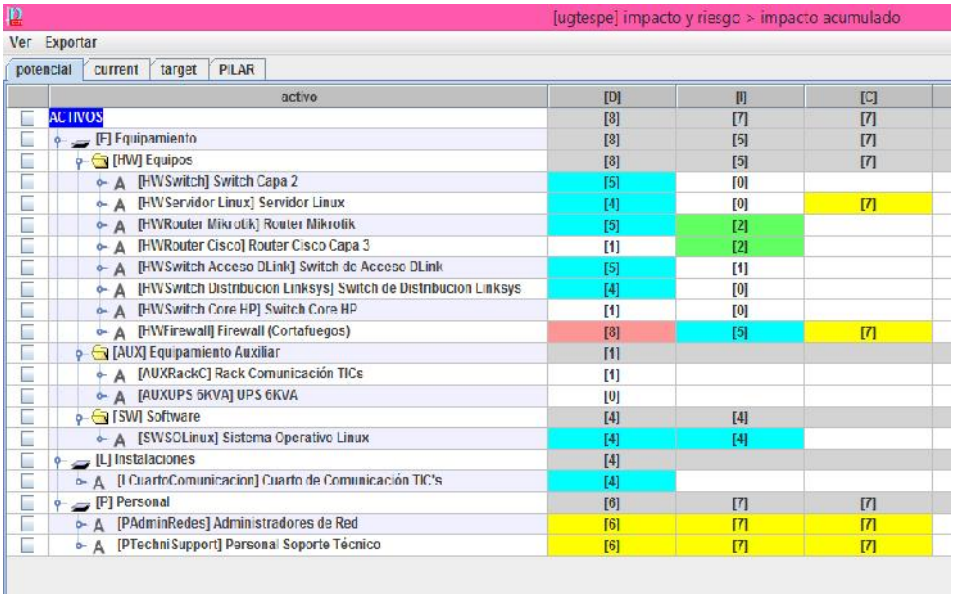


Figura 38 Impacto Acumulado

Para la identificación según el impacto se puede mostrar la siguiente tabla con los valores proporcionados por la misma herramienta pilar:

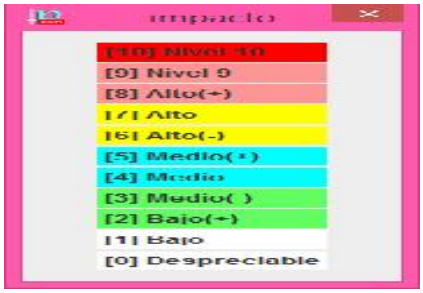


Figura 39 Nivel de impacto según Pilar

Fuente: (PILAR Análisis y Gestión de Riesgos Ayuda Versión 7.2, 2018)

3.15. Riesgo Acumulado

A continuación, se puede visualizar los valores asignados según la evaluación de los riesgos que podrían causar según el activo y la amenaza.

activo	[D]	[I]	[C]
ACTIVOS	{6,0}	{5,1}	{6,0}
[E] Equipamiento	{6,0}	{3,9}	{5,1}
[HW] Equipos	{6,0}	{3,9}	{5,1}
[HWSwitch] Switch Capa 2	{4,2}	{0,75}	
[HWServidor Linux] Servidor Linux	{3,7}	{0,98}	{5,1}
[HWRouter Mikrotik] Router Mikrotik	{4,2}	{2,1}	
[HWRouter Cisco] Router Cisco Capa 3	{1,9}	{2,1}	
[HWSwitch Acceso DLink] Switch de Acceso D	{4,2}	{1,5}	
[HWSwitch Distribucion Linksys] Switch de Di	{3,7}	{0,87}	
[HWSwitch Core HP] Switch Core HP	{1,9}	{0,87}	
[HWFirewall] Firewall (Cortafuegos)	{6,0}	{3,9}	{5,1}
[AUX] Equipamiento Auxiliar	{1,3}		
[SW] Software	{3,3}	{3,3}	
[L] Instalaciones	{3,3}		
[LCuartoComunicacion] Cuarto de Comunicación	{3,3}		
[P] Personal	{4,5}	{5,1}	{6,0}
[PAdminRedes] Administradores de Red	{4,5}	{5,1}	{5,1}
[PTechniSupport] Personal Soporte Técnico	{4,3}	{5,1}	{6,0}

Figura 40 Riesgo Acumulado

Para la valoración del riesgo acumulado se cuenta con una tabla asignada con valores proporcionadas por la misma herramienta:

Figura 41 Nivel de criticidad para riesgo acumulado

3.16. Gráfica Valor Activo

Gráfica emitida por la herramienta Pilar en la misma que se muestra el valor de cada uno de los activos especificados según una escala proporcionada por el mismo software.

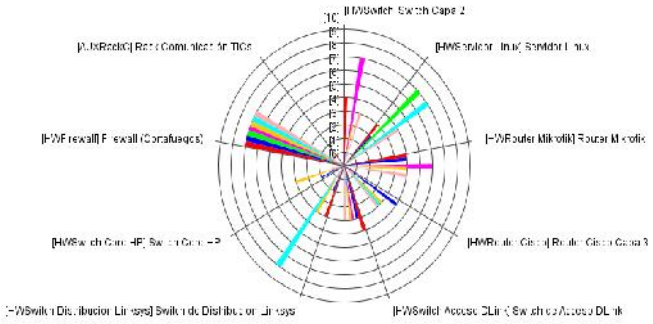


Figura 42 Gráfica valor/activo

3.17. Gráfica Salvaguardas aspecto

Gráfica que representa la aplicación de las Salvaguardas según cada uno de los aspectos como:

- **[G] Gestión:** Las salvaguardas en el aspecto de gestión se encuentra en un porcentaje del 60% de efectividad.
- **[T] Técnica:** En este aspecto el nivel de efectividad se encuentra en 70%, ya que se refiere a todos los aspectos técnicos que comprometen los activos informáticos en la red de la institución.
- **[F] Física:** El porcentaje en base a la protección física de los activos de red cuenta con 70%.
- **[P] Personal:** En cuando al aspecto del personal el nivel de las salvaguardas frente al mismo cuentan con un porcentaje del 50%.

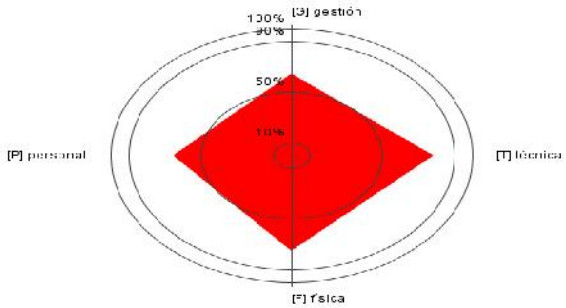


Figura 43 Gráfica Salvaguardas/aspectos

3.18. Gráfica Salvaguardas/Estrategias

Gráfica en la que se indica el porcentaje de efectividad de las salvaguardas como estrategias siendo los siguientes resultados:

1. **[M] Mixta:** Una protección mixta referida a cada una de las acciones referentes a los activos, amenazas y riesgos que han sido identificados e ingresados en el sistema la misma que cuenta con un nivel de efectividad del 65%, frente a los mismos.
2. **[RF] Reducción de la frecuencia (prevención):** Referida a la efectividad de reducción de frecuencia de aparición de las amenazas que puedan afectar a los activos de la red la misma que consta de un 70% de efectividad para contrarrestar.
3. **[R] Reducción del impacto:** Muestra el nivel de efectividad en cuanto a la reducción del impacto de las amenazas frente a los activos, la misma que consta con un 70% según la herramienta.
4. **[D] Detección:** En cuanto a la detección de las amenazas y riesgos según la herramienta consta de un nivel de efectividad de un 80%, ya que en cada uno de los activos ingresados para el análisis se verificó todas las posibles (riesgos) que puedan afectar de manera potencial a los mismos.
5. **[R] Recuperación:** En cuanto a recuperación de los activos en caso de suscitarse una amenaza el nivel de efectividad es de un 70%, para efectuar el recobro de los mismos.

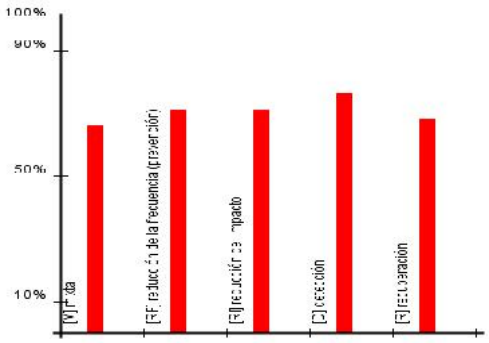


Figura 44 Gráfica Salvaguardas/estrategia

3.19. Gráfica Salvaguardas / Tipos de protección

En la siguiente gráfica se muestra la efectividad de las salvaguardas con respecto a los tipos de protección establecidos por la herramienta Pilar, los mismos que son:

[PR] Prevención: Nivel de efectividad de las salvaguardas en cuanto a protección es de un 85%.

[DR] Disuasión: La salvaguardas en cuanto a que pueda hacer que la amenaza sea modificada a un nivel bajo o que por ende desaparezca en los activos cuenta con un nivel de eficacia de 0% ya que no puede modificar todos los aspectos a los que puede encontrarse expuesto el equipo informático.

[EL] Eliminación: El porcentaje de efectividad frente a la eliminación de las amenazas que puedan afectar los activos de red consta de un 75%.

[IM] Minimizar el Impacto: En cuando a la disminución o minimización del impacto cuenta con un nivel de efectividad del 75%.

[CR] Corrección: En cuanto a corrección consta con un nivel de efectividad del 74%.

[RC] Recuperación: En el caso de recuperación la salvaguarda tiene un nivel de efectividad del 74%.

[DC] Detección: El nivel de detección que ofrece la herramienta se encuentra en un 75%.

[MN] Monitorización: Para el aspecto de monitorización la herramienta ofrece un nivel del 65%. Ya que cabe recalcar que esta tarea se puede realizar según la necesidad del personal encargado del departamento de TICs.

[AW] Concienciación: El nivel de concienciación que pueda causar la herramienta se encuentra de un 55%, ya que eso depende también de la aplicación de las salvaguardas que puedan tomar para la protección de los activos.

[AD] Administrativa: En cuanto al aspecto administrativo la herramienta ofrece un 55% de efectividad.

[std] Normativa: En relación a normativas la herramienta es del 50% de efectividad. Ya que la misma no establece las normas a las que debe regirse una institución ya que la misma se hace según la necesidad.

[proc] Procedimiento: Referente a procedimientos la herramienta proporciona un 50%, para la realización de los mismos.

[cert] Certificaciones / acreditaciones: Referente a ayudar a acreditaciones la herramienta puede ser de gran ayuda así como muestra la siguiente figura con un nivel del 85%.

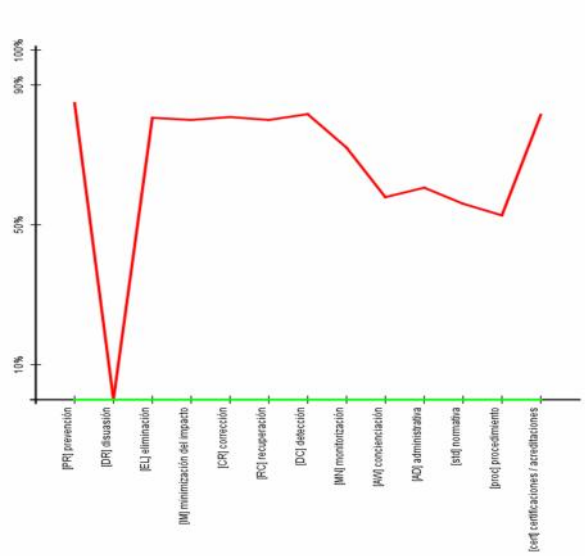


Figura 45 Gráfica Salvaguarda / Tipo de Protección

3.20. Gráfica Impacto Acumulado / Activo

En la siguiente gráfica se muestra el impacto acumulado referente a cada uno de los activos ingresados de Hardware, Software, Equipamiento Auxiliar, Instalaciones y Personal:

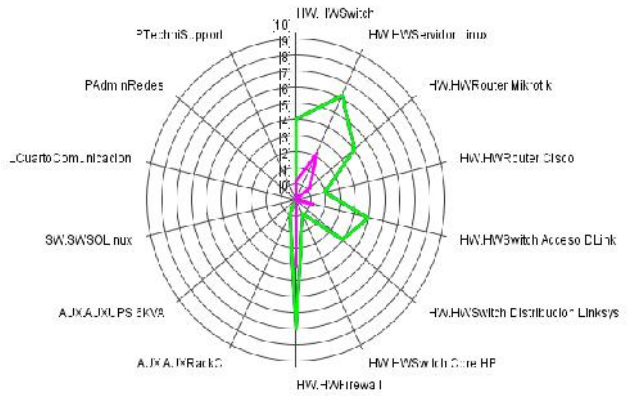


Figura 46 Gráfica Impacto Acumulado / Activo

3.21. Gráfica Impacto Acumulado / Dimensión

En la siguiente gráfica se muestra el impacto acumulado según la dimensión de confidencialidad, integridad y disponibilidad principalmente según la herramienta.

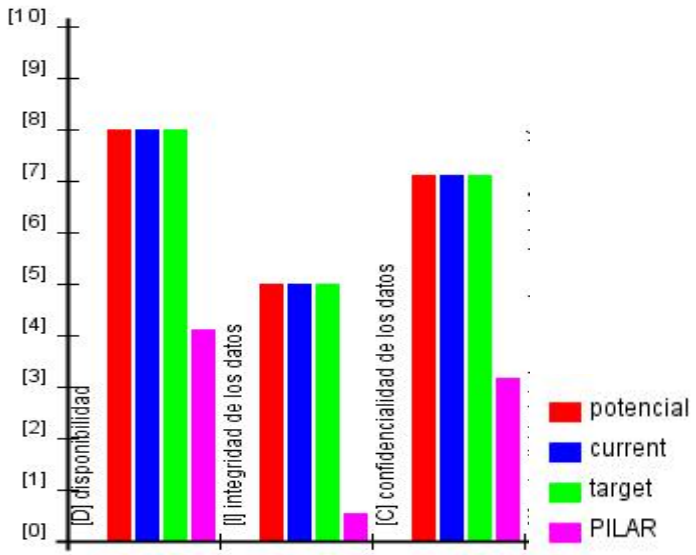


Figura 47 Gráfica Impacto acumulado /Dimensión

3.22. Gráfico Riesgo Acumulado / Activo

En la siguiente gráfica se muestra el riesgo acumulado para los activos.

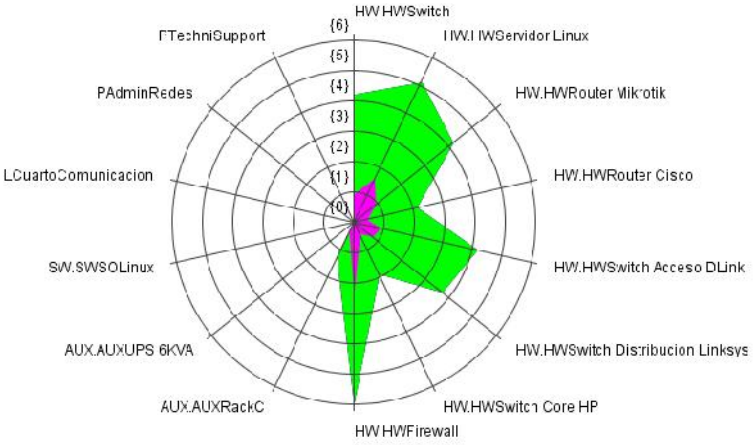


Figura 48 Gráfica Riesgo Acumulado / Activo

3.23. Gráfica Riesgo Acumulado / Dimensión

En la siguiente figura muestra el riesgo acumulado con respecto a las dimensiones de disponibilidad, integridad y confidencialidad respectivamente.

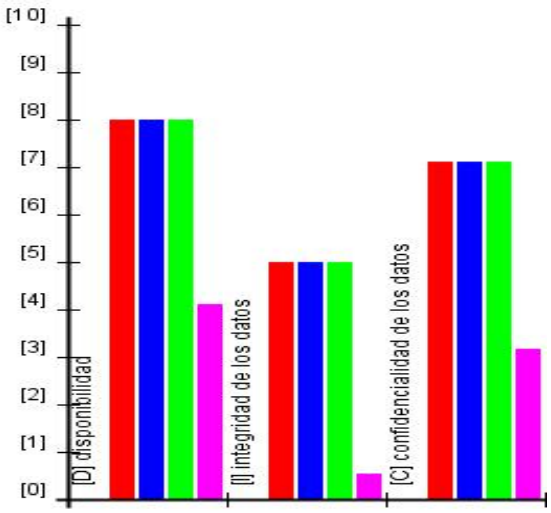


Figura 49 Gráfica Riesgo Acumulado / Dimensión

3.24. Gráfica Riesgo Acumulado / Dimensión / Fase

Se muestra a continuación la gráfica del riesgo acumulado según la dimensión de disponibilidad, integridad y confidencialidad y fase de la herramienta.

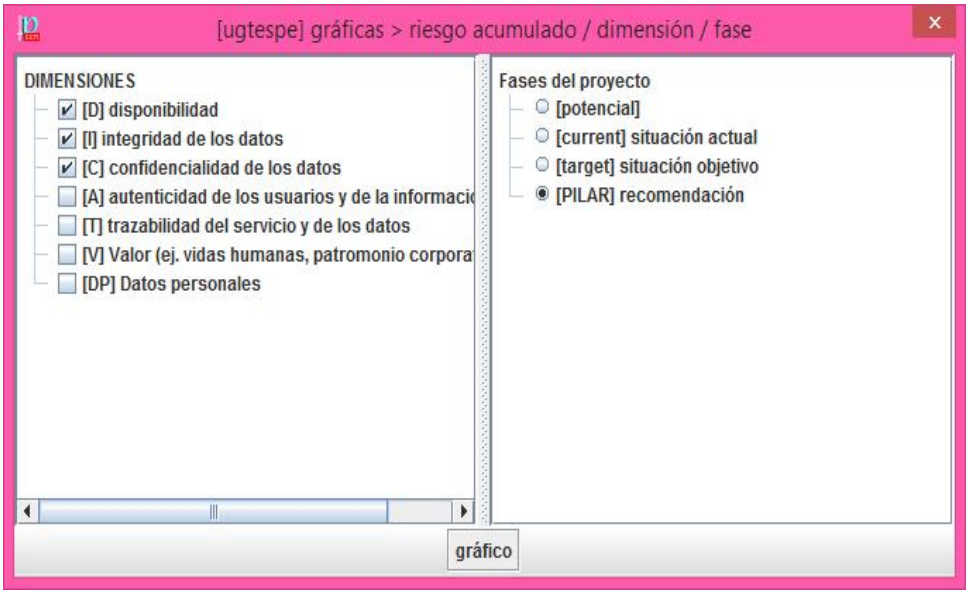


Figura 50 Parámetros Gráfica Riesgo Acumulado/dimensión/fase

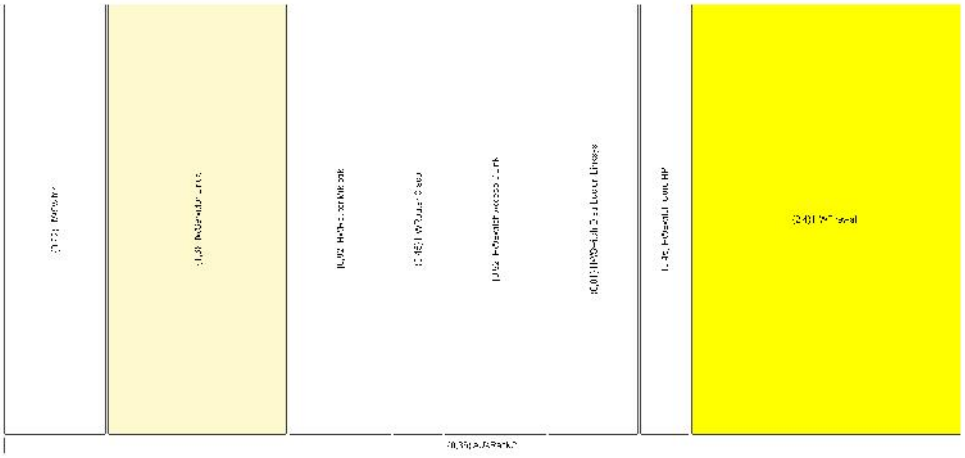


Figura 51 Gráfica Riesgo Acumulado/Dimensión/Fase

PROPUESTA PLAN DE SEGURIDAD INFORMÁTICA PARA LA UNIDAD DE GESTIÓN DE TÉCNOLOGÍAS ESPE

3.25. Alcance del Plan de Seguridad Informática

El presente Plan de Seguridad Informático es aplicable en el área de redes especialmente en la red de área local de la Unidad de Gestión de Tecnologías ESPE (UGT-ESPE), la misma que está ubicada en el Sector la FAE, Cantón Latacunga, Provincia Cotopaxi, Dirección Av. Javier Espinoza N3-47 y Av. Amazonas.

Cada una de las acciones, son presentadas en la siguiente propuesta del plan de seguridad informática, la misma que fue diseñada como una opción de protección frente a posibles riesgos identificados en la red de área local (LAN), de la institución.

La importancia de brindar una propuesta de plan de seguridad informática para la red de área local de la Unidad de Gestión de Tecnologías ESPE (UGT-ESPE), es mantener definido claramente el alcance que tomará el mismo, teniendo en cuenta cada una de las acciones que se pueden tomar para combatir riesgos en caso de materializarse, que puedan afectar la funcionalidad del servicio y la red de esta prestigiosa Institución. De tal manera que dicha propuesta de plan de seguridad consta con una vigencia de dos años valorados en un análisis y evaluación de los mayores riesgos.

3.26. Caracterización del Sistema Informático

3.26.1. RED DE ÁREA LOCAL (LAN) DE LA UNIDAD DE GESTIÓN DE TECNOLOGÍAS – ESPE (UGT-ESPE)

Redes de Área Local (LAN)

Son redes locales privadas, de pocos kilómetros de extensión que principalmente son utilizados en oficinas y centros educativos. Dichas redes se usan para conectar computadoras personales o estaciones de trabajo, con

objeto de compartir recursos e intercambiar información. (Toranzo Reina & Ruiz Rivas , 2012)

La red de área local de la Unidad de Gestión de Tecnologías ESPE está formada por los siguientes activos tanto de hardware y software, contando de la misma manera los principales componentes: tecnologías de información, personas e inmuebles.

A continuación, se puede contar con una organización de cada uno de los componentes para mayor compresión:

3.26.2. Bienes informáticos, Destinación e importancia.

1. **Redes instaladas, Estructura:** La red LAN de la Unidad de Gestión de Tecnologías ESPE se encuentra conformada de la siguiente manera:

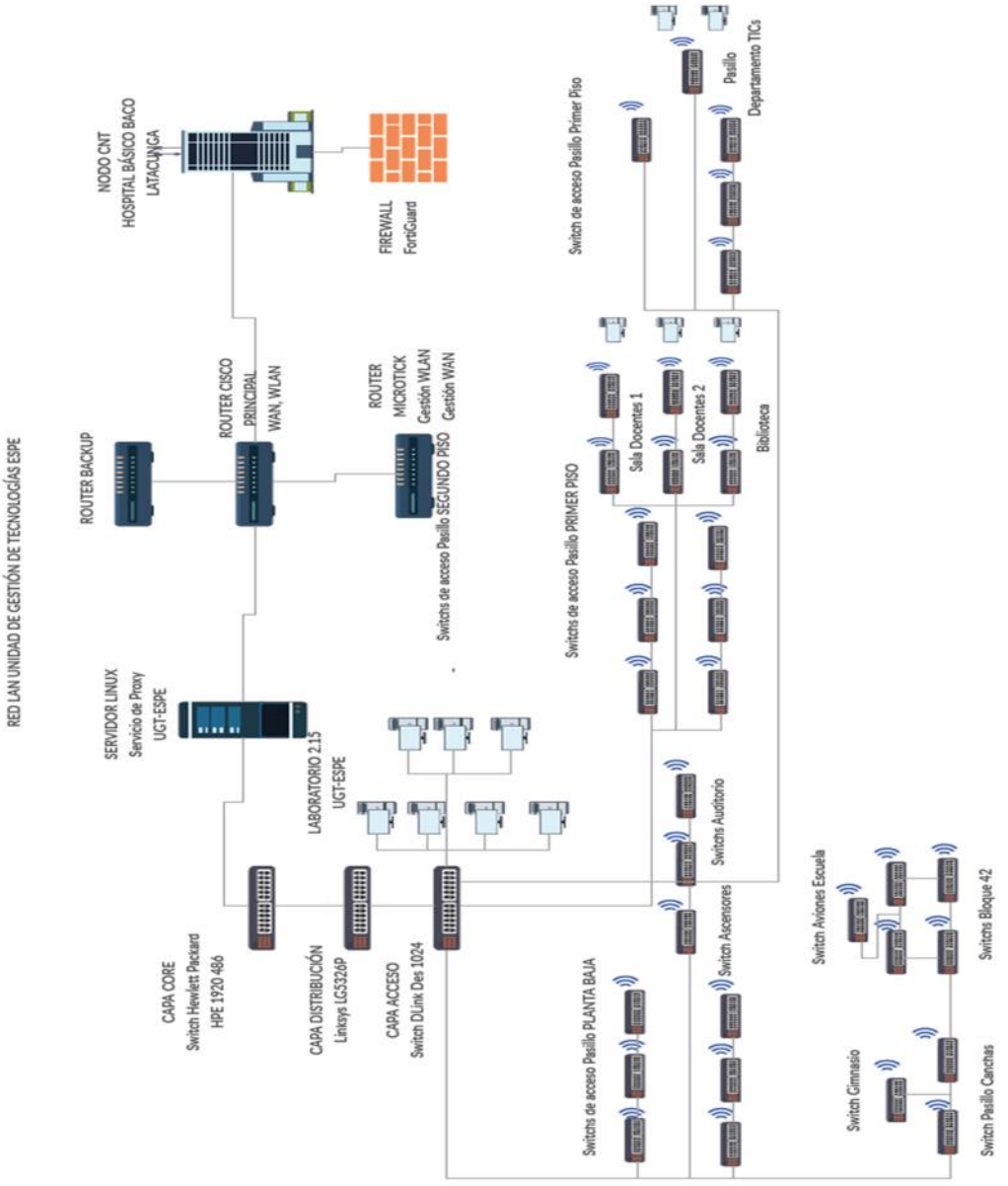
Situación Actual Unidad de Gestión de Tecnologías ESPE

Tabla 28

PLAN Situación Actual Unidad de Gestión de Tecnologías ESPE

Institución	Número plantas (Edificio)	Número de Áreas	Número de Usuarios	Número de PCs		Responsable
				Desktop	Laptop	
Unidad de Gestión de Tecnologías ESPE	3	9	80	30	60	Sgop. Luis Santana

Diagrama de la Red LAN de la Unidad de Gestión de Tecnologías –ESPE



Fuente: Elaboración propia

Activos de la RED LAN UGT-ESPE

Tabla 29

Inventario de Activos de la Red LAN de la UGT-ESPE

Cant	Activo	Descripción	Categoría	Ubicación	Responsable TICs
3	Router CISCO	Enlace WAN Backup	Capa 3	Rack Comunicación	Sgop. Luis Santana
1	Router Mikrotik	Gestión WLAN Gestión WAN	Capa 3	Rack Comunicación	Sgop. Luis Santana

2	Switch 24 puertos	Wireless Administrable	Capa 3 Capa 2	Rack Comunicación	Sgop. Luis Santana
3	Switch 24 puertos	No Administrable	Capa 2	Varias Áreas	Sgop. Luis Santana
3	Switch 16 puertos	No Administrable	Capa 2	Varias Áreas	Sgop. Luis Santana
1	Rack	Servidores		Gabinete Cerrado TIC's	Sgop. Luis Santana
1		Firewall FortiGuard		BACO UGT-ESPE TIC's	Sgop. Luis Santana
1	UPS 6KVA	Energía Respaldo TIC's		TIC's	Sgop. Luis Santana
1	Servidor Linux	Servicio Proxy Permisos Acceso RED		TIC's	Sgop. Luis Santana

2. Modelo Jerárquico de la Red LAN.

Los modelos de Switch utilizados en cada capa de la red LAN de la UGT-ESPE son los siguientes:

- Capa Core (Switch Hewlett Packard HPE 1920 48G), opera en capa 3.
- Capa Distribución (Switch Linksys LGS326P), opera en capa 2 y capa 3.
- Capa Acceso (Switch DLINK DES 1024), opera en capa 2.

SWITCH

Procedente del término inglés switch, un conmutador es un dispositivo digital presente en aquellas organizaciones que necesitan que sus redes estén en permanente interconexión. (Navarro, 2010)

En función de la metodología de segmentación de las subredes empleadas es posible diferenciar entre modelos de 2, 3 y 4 capas. (Navarro, 2010)

En un nivel superior se encuentran los switches de capa 3: además de soportar las funciones de los modelos de capa 2, integran prestaciones de routing como el soporte a los protocolos OSPF y RIP (para la construcción y el mantenimiento de tablas de enrutamiento) y están especialmente indicados para las redes LAN que tienen un tamaño grande y en las que un switch de capa 2 acarrearía, de un lado, pérdida de eficacia y, de otro, rendimiento. (Navarro, 2010)

3.27. Personal vinculado con las tecnologías y servicios

La Unidad de Gestión de Tecnologías ESPE, cuenta un personal especializado, los mismos que se encuentran encargados de todas las actividades correspondientes al manejo de las TICs de la institución, teniendo a cargo cada una de las actividades tanto de mantenimiento al igual que el funcionamiento del mismo contando principalmente con el Sr. Sgop. Luis Santana y el Sr. Ing. Danilo Chorros.

3.28. Condiciones de la edificación, ubicación, estructura.

3.28.1. Edificación de la Unidad de gestión de Tecnologías – ESPE (UGT ESPE):

La edificación ubicada en el Sector la FAE, Cantón Latacunga, Provincia de Cotopaxi, Dirección: Av. Javier Espinoza N3-47 y Av. Amazonas.

Consta de 3 plantas las cuales están identificadas como: planta baja, principalmente utilizada por laboratorios de electrónica e instrumentación y mecánica aeronáutica.

La segunda planta cuenta con aulas de laboratorio de inglés y un laboratorio de computación en el cual se encuentra ubicado un rack para distribución de la red LAN de la UGT – ESPE.

Y por último se encuentra la tercera planta la misma que cuenta con aulas con finalidades educativas. También en dicha planta se encuentra la oficina

principal de Tics de la Unidad de Gestión de tecnologías en la que se plasma el plan de protección.

3.29. Bienes Informáticos más importantes para proteger:

Para realizar el análisis de riesgos de la red de área local (LAN) de la Unidad de Gestión de Tecnologías ESPE, e utilizó como principal herramienta Pilar, la misma que se encuentra apegada a la Metodología Magerit, ayudando a lograr identificar cada uno de los activos con los cuales cuenta la red de la UGT-ESPE, tanto como: hardware, software, instalaciones y personal. De esta manera también logrando identificar cada una de las amenazas a los cuales pueden estar expuestos y los mismos que en caso de materializarse pueden causar degradación en los activos tanto físicamente como también de manera lógica, impidiendo de esta manera el correcto funcionamiento.

A continuación, se muestra los activos informáticos de mayor importancia a proteger:

- **Firewall:** Aunque Dicho activo no está bajo toda la responsabilidad del departamento de TICs, de la Unidad de Gestión de Tecnologías ESPE, se debe tener en cuenta, que el riesgo de que sufra daños podría afectar a la información con la que también cuenta la Institución.
- **Servidor Linux:** Se debe tener en cuenta los daños que podrían ser causados ya sea por un acceso no autorizado o pérdidas de equipo, siendo unos de los daños mayormente exponenciales.
- **Cuarto de Comunicación TICs:** Dicho activo de Instalación también fue considerado como uno de mayor importancia, ya que puede sufrir actos como accesos no autorizados, que puedan causar daños tanto a los equipos que en ella existen, como también daños a la información que se maneja.

Luego de identificar los activos que se pueden encontrar con mayor exposición a daños, cabe recalcar que los demás activos no dejan de ser importantes, ya que también fueron tomados en cuenta y analizados para

poder estructurar de la misma manera acciones para reducir el impacto de una amenaza en caso de efectuarse.

De la misma manera se muestra las amenazas más importantes a considerar de acuerdo con el impacto que pueden tener sobre los activos de la Institución son:

1. El acceso no autorizado tanto a la red como también a las instalaciones del Departamento de TICs de la Unidad de Gestión de Tecnologías ESPE donde se encuentran los dispositivos, dichos riesgos pudiendo ser efectuados producto de un ataque externo o interno.
2. Puede existir errores de mantenimiento, que pueden ser causados no intencionalmente, los mismos que pueden realizar daños graves.
3. En el Cuarto de comunicación TICs (acceso no autorizado o pérdida de equipos)
4. El uso no previsto de los activos en funcionamiento de la red LAN de la UGT- ESPE pueden causar la pérdida del servicio total o parcial, de esta manera provocando retrasos en actividades propias de la Institución.
5. Manipulación no autorizada de dispositivos de Hardware, podría causar graves inconvenientes en el servicio de la red.
6. Denegación de Servicio, puede causar problemas a la hora de querer acceder al servicio.
7. Ataque destructivo, en caso de materializarse podría causar un daño de magnitud total, causando daños como perdida de información o daños en los equipos.
8. La caída del sistema por agotamiento de recursos podría causar inconvenientes en caso de suscitarse.
9. Corte del suministro eléctrico, podría ser causante de pérdida de información en el momento de efectuarse, así como también daño en los equipos.
10. Pérdida de la disponibilidad de los activos causaría ineficiencia para los servicios.

11. Fuga de Información confidencial.

12. El uso inadecuado de las tecnologías y los servicios podrían causar inconvenientes en la red de la Institución.

El área sometida a un mayor peso en cuanto a riesgos y amenazas son:

El Cuarto de Comunicación TICs (acceso no autorizado, pérdida de la disponibilidad, pérdida de equipos, manipulación del hardware, usos no previstos, denegación de servicios ataques destructivos a las áreas encargadas del departamento de TICs de la Unidad de Gestión de Tecnologías ESPE).

3.30. Políticas de Seguridad Informática

A continuación, se definen cada uno de los aspectos que forman la estrategia a seguir para combatir los riesgos y amenazas, basándose a las características de los equipos de la red.

De la misma manera se muestra una propuesta de las normas, las mismas que constan como una recomendación de normas generales que podrían cumplirse y de esta manera derivar de cada uno de los resultados obtenidos en el análisis de riesgos realizados mediante la herramienta Pilar y la Metodología Magerit.

1. La propuesta de Plan de defensa y protección de Seguridad Informática para la Unidad de Gestión de Tecnologías ESPE, se encuentra encaminada a mejorar el sistema se seguridad tanto física como lógica, la misma que será entregada conforme a ser una propuesta de plan que pueda ser útil para combatir las amenazas encontradas en el análisis anteriormente realizado.

2. El acceso a cada una de las tecnologías o recursos informáticos de la Institución, estarán estrictamente aprobadas por el personal encargado del Departamento de las TICs de la Unidad de Gestión de Tecnologías ESPE, y siendo previamente listos en cada uno de los aspectos de la seguridad informática.

3. Cada uno de los usuarios de los servicios informáticos que ofrece el Departamento de las TICs de la Unidad de Gestión de Tecnologías ESPE, responden estrictamente por la protección de sus datos, su manejo y se encuentran en la obligación de informar cualquier problema que pueda ocurrir al personal del Departamento de TICs de la Unidad de Gestión de Tecnologías ESPE, para la rápida solución.
4. Todos los bienes informáticos con los que cuenta la Unidad de Gestión de Tecnologías ESPE serán identificados y controlados mediante inventarios y registros los mismos que puedan dar constancia del servicio que prestan y la ubicación en las que se encuentran instalados, evitando de esta manera pérdidas o desconocimiento de la ubicación de los mismos.
5. En caso de un posible ataque o violación de la seguridad informática de la UGT- ESPE, se deberá proceder a comunicar a las personas encargadas del Departamento de TICs de la UGT-ESPE, los mismos que podrán dar aviso a los Directivos y puedan analizar la situación y dar una solución concreta, correcta y a tiempo.

3.31. Responsabilidades

A continuación, se describe la estructura con la que cuenta la Institución para la gestión de la Seguridad Informática, especificando cada una de las funciones y obligaciones con las que cuenta el personal del Departamento de TICs Unidad de Gestión de Tecnologías ESPE.

El personal encargado del Departamento de TICs de la Unidad de Gestión de Tecnologías ESPE, tienen entre sus funciones, responsabilidades y obligaciones:

a) Garantizar la aplicación de las políticas de seguridad definidas para la red de la Institución.
b) Proteger la integridad y funcionamiento de la Red, protegiendo los recursos informáticos con los que cuenta.

c) Garantizar que los equipos, que se encuentran instalados, funcionen de acuerdo con los fines para los que fueron creados.

d) Comunicar a los Directivos de la Unidad de Gestión de Tecnologías ESPE, los nuevos controles técnicos que estén por realizar y cualquier anomalía detectada.

e) Tener la capacidad de activar cada uno de los mecanismos técnicos, en caso de tener inconvenientes o ataques destructivos que puedan causar degradación en los servicios, para poder preservar la integridad de la información y los activos de la red.

f) Tener participación en las elaboraciones de cada uno del procedimiento que impliquen recuperación ante daños que puedan sufrir los recursos informáticos.

g) Informar a los usuarios de cada una de las políticas de seguridad que se encuentran establecidas, brindando capacitaciones frente al correcto uso de los recursos informáticos y lograr de esta manera el cumplimiento de las mismas.

h) Ante posibles materializaciones de amenazas, de programas maliciosos, virus informáticos o ataques, informar a los Directivos de la Unidad de Gestión de Tecnologías ESPE, para lograr encontrar una posible solución.

i) Tener la posibilidad de activar mecanismos técnicos y organizativos, ante la identificación de amenazas, para la red.

j) Controlar de manera regular la integridad, disponibilidad y funcionamiento correcto del software instalados en el servidor.

k) Lograr identificar posibles amenazas, vulnerabilidades en los activos de la red y sistema, tener la capacidad para proponer posibles soluciones para contrarrestar la degradación de los activos.

3.32. Medidas y procedimientos

3.32.1. Clasificación y control de los bienes informáticos.

Cada una de las siguientes medidas y procedimientos que se muestran a continuación, permiten identificar cada uno de los activos o bienes con los que cuenta el Departamento de TICs de la Unidad de Gestión de Tecnologías ESPE, de acuerdo, a su importancia y lograr controlar su utilización según las funciones para los cuales fueron creados y garantizar su correcta protección.

Medidas:

- Cada uno de los activos deben encontrarse debidamente identificados y registrados, evitando confusiones y malos procedimientos.
- Los recursos informáticos con los que cuenta el Departamento de TICs de la Unidad de Gestión de Tecnologías ESPE, debe encontrarse estrictamente bajo documentación legal, para garantizar una protección responsable.
- La realización de auditorías para el control de cada uno de los activos con los que cuenta la Unidad de Gestión de Tecnologías ESPE se debe realizar de manera periódica según lo establecido por la institución.
- Contar con un expediente (documento/registro) técnico, donde se puedan registrar cada uno de los cambios, a realizar y los ya realizados en los activos de la Red de la UGT-ESPE.
- El Departamento de TICs de la Unidad de Gestión de Tecnologías ESPE, debe ser responsable de los controles de cada uno de recursos informáticos.

Procedimientos

Procedimiento No. 1: Alta de Medios Informáticos para su uso.

1. La realización de controles sobre cada uno de los recursos informáticos, que se encuentren en cada uno de los departamentos a cargo de las TICs.
   Responsables: Personal TICs

2. Elaboración de informes, de acuerdo con los resultados, de cada uno de los controles que realicen y colocarlos en conocimiento de la dirección centro, para legalización de las acciones realizadas.
   Responsables: Personal TICs
3. Contar con la documentación legal, de cualquier implementación de un activo o recursos informáticos.
   Responsables: Personal TICs
4. Garantizar que cada uno de los activos informáticos, cuenten con las medidas de protección físicas, tomando en cuenta las condiciones adecuadas necesarias y establecidas para los mismos.
   Responsables: Personal TICs
5. Integrar los nuevos equipos a la red y a los registros necesarios para su legalidad en el Departamento de TICs de la Unidad de Gestión de Tecnologías ESPE y constatar su correcto funcionamiento.
   Responsables: Personal TICs
6. Elaborar un expediente técnico de la infraestructura informática.
   Responsables: Personal TICs
7. Contar con Firmas de Responsabilidad que incluya el expediente técnico de la infraestructura informática.
   Responsables: Personal TICs
8. Capacitación al personal a cargo y usuarios de la Unidad de Gestión de Tecnologías ESPE, para la protección y correcto uso de los recursos informáticos de la institución.
   Responsables: Personal TICs
9. Revisar periódicamente, el cumplimiento de las políticas de seguridad, de igual manera con el personal y usuarios de los recursos informáticos de la Unidad de Gestión de Tecnologías ESPE.
   Responsables: Personal TICs

Procedimiento No. 2: Control de Medios Informáticos

1. Elaboración de un expediente técnico en el cual se pueda registrar todos los recursos informáticos del Departamento de TICs de la Unidad de Gestión de Tecnologías ESPE.
   Responsables: Personal TICs
2. Cuidar que los expedientes técnicos se encuentran actualizados y que consten todos los cambios que se tengan programados a realizar y los ya efectuados.
   Responsables: Personal TICs
3. Tener control del número de registro, manteniendo documentos legales para los cambios que pueden realizarse.
   Responsables: Personal TICs
4. Mantener una revisión constante de que se cumpla con los registros de los cambios en los expedientes referentes a los equipos.
   Responsables: Personal TICs

Procedimiento No. 3: Responsabilidad Materia del Expediente Técnico

Para control de bienes informáticos:

1. Evaluación y autorización del buen uso del recurso informático fuera de las instalaciones del Departamento de TICs de la Unidad de Gestión de Tecnologías ESPE en caso de suscitarse.
   Responsables: Personal TICs
2. Mantener por un tiempo no menor de un año las autorizaciones escritas para la entrada y salida de los equipos de la institución.
   Responsables: Personal TICs
3. Actualizar periódicamente los registros de los usuarios autorizados a utilizar los recursos fuera de la Institución en caso de suceder.
   Responsable: Jefe de Informática.
4. Revisar de manera constante el cumplimiento del procedimiento de las autorizaciones.
   Responsable: Jefe de Informática.

3.33. Del Personal

Las medidas y procedimientos propuestos a continuación, tiene como objetivo, garantizar el correcto cumplimiento de cada una de las responsabilidades de las personas encargadas de las tecnologías y servicios del Departamentos de TICs de la Unidad de Gestión de Tecnologías ESPE, así como también de la documentación.

Medidas:

- Preparación y responsabilidad del personal del Departamento de TICs de la Unidad de Gestión de Tecnologías ESPE respecto a la Seguridad Informática.
- Integridad y confidencialidad de la información y datos manejados diariamente por los usuarios y la Institución.

3.34. Seguridad Física y Ambiental

Las medidas y procedimiento propuestos a continuación tienen como objetivo evitar accesos no autorizados, degradación en las instalaciones y dispositivos que forman la red de la Unidad de Gestión de Tecnologías ESPE y la información que maneja la misma.

Medidas

- En el momento en el que un equipo sea dado de baja, por causa de un inconveniente en el funcionamiento, o sea destinado para otras funciones, deberá ser revisado con anticipación por parte del personal del Departamento de TICs de la Unidad de Gestión de Tecnologías ESPE, para evitar que la información o datos puedan verse comprometidos.
- En caso de que un dispositivo de almacenamiento, que contenga información confidencial sea dado de baja, se deberá destruir físicamente por los encargados del Departamento de TICs de la Unidad de Gestión de Tecnologías ESPE, como medida de protección a la información almacenada.

3.34.1. Medidas generales para todas las áreas con tecnologías informáticas:

- Todos los tomacorrientes deberán tener señalizaciones del tipo de voltaje que suministran para evitar accidentes o incendios por mal uso.
- Los usuarios antes de conectar o desconectar los equipos de la red eléctrica, deberán revisar que estos estén debidamente apagados.
- De manera principal contar con fuentes de respaldo de energía en buen estado y estabilizadores de voltaje para cada computadora que se encuentre en uso del personal de la Unidad de Gestión de Tecnologías ESPE.
- En el caso de que las áreas donde se procesan informaciones confidenciales se deben tener en cuenta la posición del equipamiento, garantizando de esta manera que las computadoras estén situadas de forma tal que se impida ver el monitor por personas que entren al espacio de trabajo o estudio.

3.34.2. Medidas para el ahorro de energía en todas las estaciones de trabajo.

- Activar el Modo de bajo consumo, en la computadora configurando la opción de ahorro de energía para el monitor.
- Habilitar el modo de hibernación para computadoras con este servicio de funcionamiento. Se recomienda seleccionar como rango de tiempo para pasar al modo de hibernación un tiempo no menor de dos horas y no mayor de 6 horas.
- Desconectar los equipos después del horario laboral o actividad académica.

3.34.3. Medidas para el mantenimiento y reparación de las tecnologías informáticas.

- Las reparaciones menores y los mantenimientos que se realizan por el Departamento de TICs de la Unidad de Gestión de Tecnologías ESPE

y las reparaciones mayores por entidades contratadas las mismas que tengan contrato legal con la institución.

- Siempre que se realice el mantenimiento o la reparación de un equipo en la propia Institución, se debe realizar en presencia de una persona del área de la cual es el equipo. Si el equipo contiene información clasificada debe estar presente las respectivas personas involucradas, para evitar inconvenientes.
- En caso de que sea necesario ser traslado un equipo fuera de la Unidad de Gestión de Tecnologías ESPE, deberá registrar el movimiento del equipo, además de actualizar los controles internos que indiquen el lugar, donde se encontrará el equipo, su tiempo de permanencia en el servicio técnico encargado de la reparación.

3.34.4. Medidas para el Control de Acceso a los locales:

Pueden entrar a todos los locales:

1. Personal autorizado del Departamento de TICs de la Unidad de Gestión de Tecnologías ESPE, los mismos que tienen la posibilidad de verificar el cumplimiento de las medidas de seguridad informática establecidas en el plan y la protección de la información.
2. El personal de la TICs que vea necesario la realización del soporte técnico a equipos de uno o varios departamentos, para el mantenimiento al sistema informático.
3. Miembros del Departamento de TICs de la Unidad de Gestión de Tecnologías ESPE que verifique el cumplimiento de esta tarea**.**

Procedimiento No. 4: Bajas de los bienes informáticos.

1. Identificar el equipo informático al que se le dará baja.
2. Recoger el equipo informático del área donde se encuentra y trasladarlo al Departamento de TICs de la Unidad de Gestión de Tecnologías ESPE para poder continuar con el respectivo procedimiento.

3. Dar de baja al equipo informático de los Activos Fijos Tangibles y de los registros del Departamento de TICs de la Unidad de Gestión de Tecnologías ESPE, para generar respaldo de las acciones tomadas.
   Responsable: Personal TICs

Procedimiento No. 5: Bajas de los bienes informáticos que contengan Información Clasificada.

1. Revisar el equipamiento al que se quiere dar de baja.
   Responsable: Departamento TICs
2. Realizar un expediente técnico (registro) del procedimiento de baja que se realiza del equipo. Para respaldo con documentación legal de la acción efectuada.
3. Revisar de manera periódicamente el cumplimiento del procedimiento, en cada caso que se realice.

Procedimiento No. 6: Mantenimiento a Equipos.

1. Realizar el mantenimiento de los equipos y activos de red de la Unidad de Gestión de Tecnologías ESPE según los planes programados por el personal autorizado de la Institución.
2. Realizar un registro en el Expediente Técnico del equipo, en donde debe constar la fecha del mantenimiento, las firmas de responsabilidad y las autorizaciones para la ejecución del mismo.
3. Una vez que se finalice el mantenimiento del o los equipos se debe entregar el informe técnico de las acciones realizadas y archivarlas para protección del mismo.
   Responsable: Personal TICs
4. Revisar la constancia y legalidad en los Expedientes o Informes Técnicos del mantenimiento realizado a los equipos de la Unidad de Gestión de Tecnologías ESPE.
   Responsable: Personal TICs
5. Verificar periódicamente el cumplimiento de este procedimiento en el Departamento de TICs

Responsable: Personal TICs

Procedimiento No. 7: Autorización y control sobre los movimientos de los bienes informáticos

1. Contar con la autorización respectiva, para la realización de algún movimiento de los recursos informáticos del Departamento de TICs de la Unidad de Gestión de Tecnologías ESPE
   Responsable: Personal TICs
2. Actualizar según sea necesario el documento del Departamento donde se produce el movimiento del activo, para documentación de respaldo.
   Responsable: Personal TICs
3. Revisar antes de la salida y entrada al Departamento de TICs de la Unidad de Gestión de Tecnologías ESPE del recurso informático, corroborando que las partes del equipo estén completas y verificación de su funcionamiento.
   Responsable: Personal TICs
4. Registrar cada uno de los movimientos de los equipos, en donde se debe especificar la fecha en la que se realiza el movimiento, de qué lugar se lo realiza y a qué lugar se realiza el movimiento del activo.
   Responsable: Personal TICs
5. Controlar el cumplimiento de las autorizaciones, sobre cada uno de los movimientos que se realicen de los activos informático y su registro adecuado.
   Responsable: Personal TICs
6. Realizar inspecciones de manera sorpresiva para detectar las extracciones no autorizadas.
   Responsable: Personal TICs
7. Verificar periódicamente el cumplimiento de este procedimiento.
   Responsable: Personal TICs

3.35. Seguridad de Operaciones

La gestión de la seguridad de la información involucra el control de cada una de las acciones que pueden ser realizadas dentro del Departamento de TICs y tener la capacidad de garantizar el cumplimiento de las políticas establecidas por la Institución, y el uso de las mismas. Es por esa razón que la seguridad de las operaciones tiene como objetivo lograr la eficiencia de la gestión de la seguridad.

Medidas:

- El cambio de contraseñas corresponde al Departamento de TICs de la Dirección del Campus Central de la Universidad de la Fuerzas Armadas ESPE.
- La introducción de nuevas tecnologías de la información en el Departamento de TICs de la Unidad de Gestión de Tecnologías ESPE será previamente autorizada por el Director de la Institución

Procedimiento No. 8: Corrección de errores y brechas de seguridad

1. Ejecutar las herramientas de seguridad autorizadas por Dirección del Campus Central de la Universidad de la Fuerzas Armadas ESPE.
2. Analizar y evaluar los resultados que arrojaron las herramientas y su correspondencia con el nivel de seguridad previsto por la Dirección del Campus Central de la Universidad de la Fuerzas Armadas ESPE.
3. En caso de detectarse vulnerabilidades o accesos no autorizados, proponer de manera rápida, acciones necesarias para su evaluación y posterior toma de decisiones.
4. Realizar un control periódicamente de este procedimiento e informar de sus resultados a la Dirección del Departamento de TICs de la Universidad de las Fuerzas Armadas ESPE.
   Responsable: Personal TICs
5. Verificar regularmente el cumplimiento de este procedimiento. **Responsable:** Personal TICs

Procedimiento No. 9: Introducción de nuevos sistemas informáticos, actualizaciones y nuevas versiones.

1. Solicitar la aprobación Dirección del Campus Central de la Universidad de la Fuerzas Armadas ESPE para la instalación del nuevo sistema informático, actualización o versión.
   Responsable: Personal TICs
2. Aprobar o denegación solicitud de los mismos.
   Responsable: Departamento TICs
3. Comprobar que el nuevo sistema informático, actualización o versión cumpla con los requerimientos del sistema de seguridad establecido en la Unidad de Gestión de Tecnologías ESPE.
   Responsable: Personal TICs
4. La instalación y configuración del nuevo sistema informático, actualización o versión que sea aprobado para su uso.
   Responsable: Proveedor.
5. Verificar regularmente el cumplimiento del procedimiento.
   Responsable: Personal TICs

3.36. Seguridad ante programas malignos.

El antivirus se debe mantener debidamente actualizado. Para ello, los responsables del Departamento de TICs de la Unidad de Gestión de Tecnologías ESPE deberán tomar en cuenta el correcto funcionamiento del mismo.

Medidas:

- Cada trabajador deberá ser responsable de lo que permite introducir en el ordenador antes de su utilización.
- El personal del Departamento de TICs de la Unidad de Gestión de Tecnologías ESPE serán los encargados de efectuar la descontaminación de virus y programas maliciosos de los ordenadores.

Procedimiento No. 10: Descontaminación de programas malignos

1. Al detectar un programa maligno en algún equipo, se deberá detener la actividad de manera radical, que se esté efectuando e informar al personal de del Departamento de TICs de la Unidad de Gestión de Tecnologías ESPE
   Responsable: Usuario del equipo infectado.
2. Se debe desconectar el cable de red de la PC e identificar qué tipo de virus es el que está afectando al equipo
3. Investigar las posibles causas de aparición del virus o programa malicioso, e identificar responsables y disponer acciones correctivas.
4. Dejar constancia del suceso en el Registro de Incidencias del ordenador, para documentación legal del Departamento de TICs de la Unidad de Gestión de Tecnologías ESPE.
5. Verificar regularmente el cumplimiento de dicho procedimiento
   Responsable: Personal TICs

3.37. Respaldo de la información

Las medidas y procedimientos de respaldo que se implementen garantizaran mantener la integridad y disponibilidad de la información y de las instalaciones del Departamento de TICs de la Unidad de Gestión de Tecnologías ESPE.

Medidas:

- Se realizarán copias de seguridad de la información y del software requerido, en opción de respaldo.
- Cada usuario será responsable de la información que maneje y guarde en su equipo y por consiguiente en el servidor de la Institución.

3.38. Seguridad en Redes

Medidas:

- El personal encargado del Departamento de TICs de la Unidad de Gestión de Tecnologías ESPE, regularmente deberá verificar el tráfico que se encuentra experimentando la red, para de esta manera detectar variaciones que pueden ser síntoma de mal uso de la misma o amenazas.
- El personal del Departamento de TICs de la Unidad de Gestión de Tecnologías ESPE, serán los encargados de monitorear las conexiones activas y los puertos en la red para saber qué puertos están habilitados y verificar la seguridad de los mismos.

Procedimiento No. 11: Auditoria de eventos.

1. Revisar diariamente los registros de los eventos generados en la Unidad de Gestión de Tecnologías ESPE que sean referentes a los recursos informáticos.
2. Ante cualquier anomalía que sea detectada, se deberá investigar las causas y determinar si se está ante algún incidente o riesgo de seguridad informática.
3. Mantener de manera efectiva la disponibilidad y la actualización de las herramientas que garantizan la auditoria de los eventos autorizadas por la Universidad de las Fuerzas Armadas ESPE.
   Responsable: Personal TICs
4. Controlar regularmente el cumplimiento de dicho procedimiento.
   Responsable: Personal TICs
5. Verificar el cumplimiento de dicho procedimiento.
   Responsable: Personal TICs

Procedimiento No. 12: Revisión de las trazas de navegación.

1. Se debe controlar de manera adecuada y confidencial la actividad de los usuarios (Sitios visitados, fechas y horarios de las consultas, información descargada, etc.), para evitar filtraciones y programas maliciosos que puedan afectar a los activos de la red y de esta manera proporcionar capacitaciones a los usuarios de la navegación segura.

2. Si se detecta alguna violación se deberá realizar un informe detallado mostrando evidencia de la violación y la concurrencia con la que se efectuó.
3. Se deberá notificar por escrito o documentos legales la violación al Director del Departamento de TICs de la Universidad de las Fuerzas Armadas ESPE.
4. Verificar periódicamente el cumplimiento de dicho procedimiento.
   Responsable: Personal TICs

3.39. Gestión de Incidentes de Seguridad.

Procedimiento No. 13: Acceso y/o divulgación de información no autorizada

1. Informar al Personal del Departamento de TICs de la Unidad de Gestión de Tecnologías ESPE.
   Responsable: Persona que lo detecte
2. Cancelar las operaciones que se estén realizando y por consiguiente la eliminación del lugar en que se encuentre una vez que sea posible eliminar la evidencia.
3. Trata de eliminar la posibilidad de que se pueda repetir la violación.
   Responsable: Personal TICs
4. Proceder a aplicar las medidas disciplinarias que correspondan, si se llega a identificar la procedencia del hecho.
   Responsable: Personal TICs
5. Verificar periódicamente el cumplimiento de este procedimiento.
6. **Responsable:** Personal TICs

Procedimiento No. 14: Acceso pirata a la red

1. Informa al personal del Departamento de TICs de la Unidad de Gestión de Tecnologías ESPE.
   Responsable: Persona que lo detecte.
2. Verificar periódicamente la red en busca de vulnerabilidades o posibilidad de amenazas que puedan afectar el servicio de la red.

3. Si el ataque procede de la propia entidad: El personal del Departamento de TICs de la Unidad de Gestión de Tecnologías ESPE debe revisar los permisos otorgados y realizar un diagnóstico interno para precisar fallas que pudieran ser aprovechadas por el atacante.
4. Si el ataque procede del exterior: El personal del Departamento de TICs de la Unidad de Gestión de Tecnologías ESPE debe coordinar un diagnóstico para poder dar una solución efectiva.
   Responsable: Personal TICs
5. Se debe tener un Registro de Incidencias de la Seguridad Informática para este tipo de casos en donde pueda permanecer de manera legal los incidentes ocurridos.
   Responsable: Personal TICs
6. Se investigan y analizan las vulnerabilidades de la red que propiciaron los hechos.
   Responsable: Personal TICs
7. Verificar periódicamente el cumplimiento de este procedimiento.
   Responsable: Personal TICs

Procedimiento No. 15: Fallo de Hardware

1. Informa al personal del Departamento de TICs de la Unidad de Gestión de Tecnologías ESPE.
   Responsable: Persona que lo detecte.
2. Contactar a técnicos o personal encargado de reparación y mantenimiento del equipamiento o a la entidad proveedora del equipamiento defectuoso para corroborar y mantener de manera legal el inconveniente suscitado.
   Responsable: Personal TICs o persona que detecte.
3. Si es necesario extraer el equipo para lograr arreglarlo.
   Responsable: Personal TICs
4. Analizan el fallo ocurrido y ejecuta las acciones necesarias para la reparación del equipo.
   Responsable: Personal TICs

5. Verificar periódicamente el cumplimiento de este procedimiento.
   Responsable: Personal TICs

Procedimiento No. 16: Robo de tecnologías informáticas

1. Informar al personal del Departamento de TICs de la Unidad de Gestión de Tecnologías ESPE.
   Responsable: Persona que lo detecte.
2. Analizar la posibilidad de continuar el procesamiento. Capacitar a los usuarios de manera regular sobre los pasos a seguir de suscitarse un robo de las tecnologías en la Unidad de Gestión de Tecnologías ESPE.
   Responsable: Personal TICs
3. Analizar el hecho y la posibilidad de aplicar medidas disciplinarias y la evaluación de las medidas de seguridad para poder mejorarlas.
   Responsable: Personal TICs
4. Verificar periódicamente el cumplimiento de este procedimiento.
   Responsable: Personal TICs

Procedimiento No. 17: Fallo de comunicaciones

1. Informar al personal del Departamento de TICs de la Unidad de Gestión de Tecnologías ESPE.
   Responsable: Persona que lo detecte.
2. Determinar de manera principal las causas del fallo de comunicaciones. De ser necesario se deberá contactar al proveedor del servicio e informar de la situación presentada.
   Responsable: Personal TICs.
3. Analizar el fallo ocurrido y ejecutar las acciones para restablecer de manera rápida el servicio.
   Responsable: Personal TICs
4. Verificar periódicamente el cumplimiento de este procedimiento.
   Responsable: Personal TICs

Procedimiento No. 18: Fallo de Software.

1. Informar al personal del Departamento de TICs de la Unidad de Gestión de Tecnologías ESPE
   Responsable: Persona que lo detecte.
2. Restaurar el software, realizar acciones de restauración para que el software vuelva a entrar en servicio.
3. Realizan registro de las actividades.
   Responsable: Personal TICs
4. Verificar periódicamente el cumplimiento de este procedimiento.
   Responsable: Personal TICs

Procedimiento No. 19: Destrucción o modificación de la información.

1. Informa al personal del Departamento de TICs de la Unidad de Gestión de Tecnologías ESPE
   Responsable: Persona que lo detecte.
2. Tratar de determinar las causas en la Seguridad de los sistemas que iniciaron los hechos para corregirlos.
   Responsable: Personal TICs
3. Capacitar al personal encargado de la información afectada.
4. Hacer el registro de Incidencias.
   Responsable: Personal TICs
5. Verificar periódicamente el cumplimiento de este procedimiento.
   Responsable: Personal TICs

3.40. Políticas de Seguridad Informática de los usuarios que hacen uso de las tecnologías informáticas.

- Los usuarios que hagan uso de las tecnologías informáticas son responsables de la protección de la información que utilicen o creen en el transcurso del desarrollo de sus labores, lo cual incluye: protección de acceso y a sus microcomputadoras, así como cumplir con lo establecido respecto al tratamiento de la información oficial que se procese, intercambie, reproduzca o conserve a través de las

tecnologías de información, según su categoría y demás regulaciones. (Raúl Castro Ruz, 2019)

- Los usuarios tendrán acceso sólo a los recursos que necesitan en el cumplimiento de su labor diaria, implementándose mediante la definición del equipamiento, aplicaciones a utilizar mediante los privilegios y derechos de acceso a los activos de información que se le otorgue. (Raúl Castro Ruz, 2019)
- Se emplearán las tecnologías informáticas y los servicios asociados con fines estrictamente de trabajo. (Raúl Castro Ruz, 2019)
- Se realizarán salvas que permitan identificar y autenticar a los usuarios en correspondencia con el empleo a que está destinadas la información que en ellas se procese, intercambie y reproduzca. (Raúl Castro Ruz, 2019)
- Todo software traído a la entidad se le aplicará un período de cuarentena que permitan asegurar su funcionamiento seguro.
- Es obligatorio la desinfección de los dispositivos externos antes de su uso en las tecnologías informáticas. (Raúl Castro Ruz, 2019)

3.41. Sobre los Activos

- El establecimiento de salvaguardas preventivas puede ayudar a reducir las probabilidades, de que las amenazas se materialicen y causen degradación. (Raúl Castro Ruz, 2019)
- Aumentar la seguridad, para la protección del acceso controlado, donde se puedan limitar intentos de ataques y robo de equipos. (Raúl Castro Ruz, 2019)

CAPÍTULO IV

CONCLUSIONES Y RECOMENDACIONES

4.1. Conclusiones

- Los requerimientos de las herramientas, fueron identificadas y especificadas según sus características operacionales, dando lugar al desarrollo exitoso de las actividades planteadas para el análisis de los riesgos de activos de red de la institución.

- La Metodología Magerit, aplicada en el proyecto de investigación ayudó de manera principal a la protección de los equipos informáticos, la misma que fue establecida según las dimensiones de seguridad, disponibilidad, integridad, confidencialidad, apoyando a la disposición de los servicios y mantenimiento.

- Pilar, como herramienta complementaria de la metodología Magerit posibilitó la identificación de amenazas a las que se encuentran expuestos los activos que conforman el Departamento de TICs de la Unidad de Gestión de Tecnologías ESPE, mediante el análisis de riesgos, de carácter cualitativo, permitiendo contrarrestar los niveles de impacto, y proporcionando opciones de salvaguardas.

- El desarrollo del plan de defensa y protección, efectuado, a partir del análisis de los activos de la red LAN de la Unidad de Gestión de Tecnologías ESPE, es pieza fundamental en la prevención de incidentes, el cual ayuda a mejorar la seguridad del uso adecuado de los recursos informáticos. Obteniendo la reducción significativa entre el 75% al 80% de ocurrencia de amenazas; y asegurando de mejor manera la gestión de la seguridad en la Institución, en función del tratamiento de los riesgos de mayor importancia.

- Fortalecer las herramientas de seguridad con las que cuenta la red LAN de la Unidad de Gestión de Tecnologías ESPE, para precautelar la seguridad de la información y equipos.

4.2. Recomendaciones

- Definir de manera primordial los requerimientos de procesos y pasos a seguir tanto de la Metodología Magerit como de la Herramienta Pilar, para obtener un resultado óptimo de las actividades de análisis y procesos consiguientes.

- Se recomienda la utilización de metodologías, referentes a seguridad informática, en las que se pueda identificar riesgos recurrentes para de esta manera ayudar a reducirlos.

- Es recomendable contar con herramientas de análisis y gestión de riesgos como Pilar porque en el caso de suscitarse una amenaza da una respuesta eficaz, para minimizar los riesgos de degradación en los activos de una red

- Mantener actualizadas las políticas de seguridad de la información en el Departamento de TICs de la Unidad de Gestión de Tecnologías ESPE, para precautelar la integridad de cada uno de los recursos informáticos, basándose en procedimientos que ayuden a incrementar la protección de los equipos.

- Verificar de manera constante la evolución de herramientas de seguridad informática y por consiguiente el surgimiento de nuevas amenazas en general, para tratar de evitarlas o aplicar la solución más efectiva.

BIBLIOGRAFÍA

Pérez-Roca Fernández, J. Á., & Pereira Suárez, J. A. (s.f.). *FIREWALLS.* Recuperado el 24 de Septiembre de 2018, de http://sabia.tic.udc.es/docencia/ssi/old/2006-2007/docs/trabajos/06%20-%20Firewalls%20%5Bupdated%5D.pdf

Aguirre Mollehuanca, D. A. (Octubre de 2014). Recuperado el Mayo de 2018, de http://tesis.pucp.edu.pe/repositorio/bitstream/handle/123456789/5677/AGUIRRE_DAVID_SISTEMA_GESTION_SEGURIDAD_INFORMACION_SERVICIOS_POSTALES.pdf;sequence=1

Aldas Falcón, C. A. (2017). Recuperado el Mayo de 2018, de http://repositorio.uta.edu.ec/bitstream/123456789/27124/1/Tesis_%20t1359si.pdf

Alvarez Basaldúa, L. D. (13 de Octubre de 2005). Recuperado el Mayo de 2018, de http://www.bib.uia.mx/tesis/pdf/014663/014663.pdf

Álvarez Edison Oswaldo Rosero. (2014). Recuperado el 8 de Mayo de 2018, de http://www.dspace.uce.edu.ec/bitstream/25000/2464/1/T-UCE-0011-81.pdf

Amutio Gómez, M. A., Candau, J., & Mañas, J. A. (2012). MAGERIT. En M. d. Miguel Angel Amutio Gómez, J. Gonzáles Barroso, & D. y. Subdirección General de Información (Edits.), *MAGERIT - versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Libro I - Método* (Responsable edición digital: Subdirección General de Información, Documentación y Publicaciones ed., pág. 127). Madrid, España: © Ministerio de Hacienda y Administraciones Públicas, Secretaría General Técnica, Subdirección General de Información, Documentación y Publicaciones Centro de Publicaciones. Recuperado el 31 de Agosto de 2018, de https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html

Andrés Rodrigo Reinoso. (2017). *Análisis y Evaluación de Riesgos de Seguridad Informática a través del Análisis de tráfico de Datos en Redes de Área local (LAN).* QUITO.

Antonio Jose Segovia. (2019). *Advisera Expert Solutions*. Recuperado el Enero de 2019, de Advisera Expert Solutions 27001 Academy ISO 27001 and ISO 22301 Online Consultation Center: https://advisera.com/27001academy/es/que-es-iso-27001/

Areitio Bertolín Javier. (2008). *Seguridad de la Información Redes, informática y sistemas de información.* (C. L. Carmona, Ed.) Madrid, ESPAÑA: Ediciones Paraninfo S.A. Recuperado el Julio de 2018, de https://books.google.com.ec/books?id=_z2GcBD3deYC&printsec=frontcover&hl=es#v=onepage&q&f=false

BERMÚDEZ MOLINA , K. G., & BAILÓN SÁNCHEZ , E. R. (MARZO de 2015). Recuperado el Mayo de 2018, de https://dspace.ups.edu.ec/bitstream/123456789/10372/1/UPS-GT001514.pdf

COMERCIO, D. E. (6 de Julio de 2017). *El Comercio.com*. Obtenido de El Comercio.com: https://www.elcomercio.com/guaifai/ecuador-seguridad-internet-hackeo-ciberataque.html

Copyright © 2018 Fortinet, I. (2018). FortiGuard Security Services. (Fortinet®, Ed.) *Fortinet Inc.* Recuperado el 24 de Septiembre de 2018, de https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiGuard_Security_Services.pdf

EL HERALDO. (2 de Febrero de 2015). (REDACCIÓN ELHERALDO.CO) Recuperado el 06 de Febrero de 2019, de EL HERALDO: https://www.elheraldo.co/tecnologia/como-va-el-mundo-en-seguridad-informatica-182638

(2005). *ESTÁNDAR INTERNACIONAL ISO/IEC 17799 SEGUNDA EDICIÓN.*

Gaona Vásquez, K. d. (Octubre de 2013). Recuperado el Mayo de 2018, de https://dspace.ups.edu.ec/bitstream/123456789/5272/1/UPS-CT002759.pdf

González Agudelo, D. F. (2014). Recuperado el 06 de 02 de 2019, de https://repository.unimilitar.edu.co/bitstream/handle/10654/12251/ENSAYO%20FINAL.pdf;jsessionid=FB5FACE81825B9FC9C886A8B32A34E25?sequence=1

Grajales Bartolo, M. (Diciembre de 2011). Recuperado el Mayo de 2018, de http://repositorio.utp.edu.co/dspace/bitstream/handle/11059/4700/6213821G743.pdf;sequence=1

HERNÁNDEZ BUGARINI, F. (Octubre de 2007). Recuperado el Mayo de 2018, de https://tesis.ipn.mx/bitstream/handle/123456789/498/TESIS%20PROPUESTA%20SEGURIDAD.pdf?sequence=1&isAllowed=y

Jhon Erik Guanoluisa Huertas. (2015). Recuperado el 06 de Febrero de 2019, de http://bibdigital.epn.edu.ec/bitstream/15000/10499/1/CD-6217.pdf

MIRANDA CANDELARIO PIEDAD MARIBEL. (2017). Obtenido de http://repositorio.ug.edu.ec/bitstream/redug/23181/1/DISE%C3%91O%20Y%20REINGENIERIA%20DE%20LA%20INFRAESTRUCTURA%20DE%20LA%20RED%20LAN%20DE.pdf

Navarro, M. (2010). Comparativa Switches. (Comparativa, Ed.) *Byte TI*. Recuperado el 05 de Septiembre de 2018, de https://www.revistabyte.es/comparativa-byte-ti/switches/

PAE Portal Administración Electrónica. (20 de Junio de 2004). Obtenido de PAE Portal Administración Electrónica: http://administracionelectronica.gob.es/ctt/pilar/infoadicional#.XDanFlVKjIU

Paz Pellat, M. A. (19 de Diciembre de 2017). *Ruiz Realy Times*. Obtenido de Ruiz Realy Times: https://www.ruizhealytimes.com/ciencia-y-tecnologia/amenazas-a-la-seguridad-informatica-2018

(2016).*PILAR - Manual de Usuario.* Recuperado el 10 de Enero de 2019, de https://www.pilar-tools.com/doc/v62/manual_std_risk_es_2016-08-21.pdf

PILAR Análisis y Gestión de Riesgos Ayuda Versión 7.2. (26 de Noviembre de 2018). Obtenido de PILAR Análisis y Gestión de Riesgos Ayuda Versión 7.2: file:///C:/Program%20Files%20(x86)/PILAR_7.2/help_es/cia/WebHelp/index.html#!1089

Quintero Villarroya, J. L., & SDG TIC. Ministerio de Defensa. (2012). *Análisis y Gestión de Risgos. Pilar.* Madrid, España: Asociación Española de Calidad CSTIC 2012. Recuperado el 10 de Enero de 2019, de https://www.aec.es/c/document_library/get_file?uuid=b3945e58-17f2-4dc0-88ac-863ae9f998cb&groupId=10128

Raúl Castro Ruz. (10 de Enero de 2019). *Instituciones SLD Plan de Seguridad Informática.* Obtenido de Instituciones SLD Seguridad Informática: http://instituciones.sld.cu/faenflidiadoce/files/2014/04/Plan-de-Seguridad-Inform%C3%A1tica-1.pdf

Reinoso Córdova, A. R. (2017). Recuperado el Mayo de 2018, de http://bibdigital.epn.edu.ec/handle/15000/17542

ROBAYO LÓPEZ, J. M., & RODRÍGUEZ RODRÍGUEZ, R. M. (2015). Recuperado el MAYO de 2018, de https://repository.unad.edu.co/bitstream/10596/3818/5/79626344.pdf

Rodríguez, J. M., Peralta, I., & Consejo Superior de Administración Electrónica. (2013). Gestión de Riesgos Magerit. En J. M. Rodríguez, I. Peralta, Consejo Superior de ADministración Electrónica, & t. P. Peralta (Ed.), *Gestión de Riesgos Magerit* (pág. 38). ©tiThink 2013.

Recuperado el 31 de Agosto de 2018, de https://www.tithink.com/publicacion/MAGERIT.pdf

Rosero Álvarez Edison Oswaldo. (2014). Recuperado el 24 de Septiembre de 2018, de www.dspace.uce.edu.ec/bitstream/25000/2464/1/T-UCE-0011-81.pdf

Solutions, G. (2018). FORTINET. (C. ©.-F. S.R.L, Ed.) *Grid Solutions*. Recuperado el 24 de Septiembre de 2018, de https://www.gridsolutionsperu.com/soluciones-fortinet-peru/

Tixilima Cisneros, V. d. (2015). Recuperado el 07 de Julio de 2018, de http://repositorio.puce.edu.ec/bitstream/handle/22000/11437/ELABORACI%C3%93N%20DE%20POLITICAS%20Y%20NORMAS%20DE%20SEGURIDAD%20DE%20LA%20INFORMACI%C3%93N.pdf?sequence=1&isAllowed=y

Toranzo Reina, F., & Ruiz Rivas , J. A. (2012). REDES DE ÁREA LOCAL. En F. Toranzo Reina, & J. A. Ruiz Rivas, *REDES DE ÁREA LOCAL* (pág. 30). Recuperado el 5 de Septiembre de 2018, de http://ing.unne.edu.ar/pub/local.pdf

GLOSARIO

MAGERIT: de análisis y gestión de riesgos elaborada por el Consejo Superior de Administración Electrónica, que permite: estudiar los riesgos que soporta un sistema de información y el entorno asociado a él.

EAR/PILAR: Entorno de análisis y riesgos, herramienta complementaria de la metodología Pilar que permite incorporar salvaguardas para reducir el riesgo a valores residuales aceptables.

RIESGOS: Posibles eventos que puedan causar daño a un activo o información.

ACTIVOS: Componente o funcionalidad de un sistema de información susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización.

FRECUENCIA: cada cuánto se materializa una amenaza.

DEGRADACIÓN: impacto que tiene la materialización de la amenaza en el activo.

INFORMACIÓN: Es todo grupo organizado de datos que puede manejar una organización, y que tenga valor para la misma, independientemente de la manera en la cual se la puede almacenar, procesar o transmitir como también su origen o fecha de elaboración.

AMENAZA: Cosa o persona que constituye una posible causa de riesgo o perjuicio para alguien o algo.

ANEXOS

ÍNDICE DE ANEXOS

Anexo A

Libro I Método - Magerit

TÍTULO: MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.
Libro I - Método

Elaboración y coordinación de contenidos:
Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica

Equipo responsable del proyecto:
Director, Miguel Angel Amutio Gómez, Ministerio de Hacienda y Administraciones Públicas
Javier Candau, Centro Criptológico Nacional, Ministerio de la Presidencia
Consultor externo: José Antonio Mañas, Catedrático de la Universidad Politécnica de Madrid

Características: Adobe Acrobat 5.0
Responsable edición digital: Subdirección General de Información, Documentación y Publicaciones
(Jesús González Barroso)

Madrid, octubre de 2012
Disponible esta publicación en el Portal de Administración Electrónica (PAe):
http://administracionelectronica.gob.es/

Edita:
© Ministerio de Hacienda y Administraciones Públicas
Secretaría General Técnica
Subdirección General de Información,
Documentación y Publicaciones
Centro de Publicaciones

Colección: administración electrónica
NIPO: 630-12-171-8

Anexo B

Libro II Catálogo de Elementos - Magerit

TÍTULO: MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro II - Catálogo de Elementos

Elaboración y coordinación de contenidos:
Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica

Equipo responsable del proyecto:
Director, Miguel Angel Amutio Gómez, Ministerio de Hacienda y Administraciones Públicas
Javier Candau, Centro Criptológico Nacional, Ministerio de la Presidencia
Consultor externo: José Antonio Mañas, Catedrático de la Universidad Politécnica de Madrid

Características: Adobe Acrobat 5.0
Responsable edición digital: Subdirección General de Información, Documentación y Publicaciones
(Jesús González Barroso)

Madrid, octubre de 2012
Disponible esta publicación en el Portal de Administración Electrónica (PAe):
http://administracionelectronica.gob.es/

Edita:

Secretaría General Técnica
Subdirección General de Información,
Documentación y Publicaciones
Centro de Publicaciones

Colección: administración electrónica
NIPO: 630-12-171-8

Anexo C

Libro III Guía de Técnicas - Magerit

TÍTULO: MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.
Libro III - Guía de Técnicas

Elaboración y coordinación de contenidos:
Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica

Equipo responsable del proyecto:
Director, Miguel Angel Amutio Gómez, Ministerio de Hacienda y Administraciones Públicas
Javier Candau, Centro Criptológico Nacional, Ministerio de la Presidencia
Consultor externo: José Antonio Mañas, Catedrático de la Universidad Politécnica de Madrid

Características: Adobe Acrobat 5.0
Responsable edición digital: Subdirección General de Información, Documentación y Publicaciones
(Jesús González Barroso)

Madrid, octubre de 2012
Disponible esta publicación en el Portal de Administración Electrónica (PAe):
http://administracionelectronica.gob.es/

Edita:
© Ministerio de Hacienda y Administraciones Públicas
Secretaría General Técnica
Subdirección General de Información,
Documentación y Publicaciones
Centro de Publicaciones

Colección: administración electrónica
NIPO: 630-12-171-8

Anexo D

Tipos de Activos utilizados según la Metodología Magerit y Pilar

En el siguiente anexo se colocan los tipos de activos que se utilizan según la Metodología Magerit y la Herramienta Pilar:

[SW] SOFTWARE

() [prp]desarrollo propio (in house)
() [sub]desarrollo a medida (subcontratado)
() [std] estándar (off the shelf)
() [browser] navegador web
() [www] servidor de presentación
() [app] servidor de aplicaciones
() [email_client] cliente de correo electrónico
() [email_server] servidor de correo electrónico
() [directory] servidor de directorio
() [file] servidor de ficheros
() [dbms] sistema de gestión de base de datos
() [tm] monitor transaccional
() [office] ofimática
() [os] sistema operativo
() [windows] Windows
() [solaris] Solaris
() [linux] Linux
() [macosx] mac osx
() [hypervisor] hypervisor (gestor de la máquina virtual)
() [ts] servidor de terminales
() [backup] servidor de backup
() [sec] herramientas de seguridad
() [av] antivirus
() [ids] IDS / IPS (detección / prevención de intrusión)
() [dlp] prevención de pérdida de datos
() [traf] análisis de tráfico
() [hp] honey pot

[HW] HARDWARE

() [host] grandes equipos (host)
() [mid] equipos medios
() [pc] informática personal
() [mobile] informática móvil
() [pda] agendas electrónicas
() [vhost] equipos virtuales (máquinas virtuales)
() [cluster] cluster
() [backup] equipamiento de respaldo
() [data] que almacena datos
() [peripheral] periféricos
() [print] medios de impresión
() [scan] escáner
() [crypto] dispositivo criptográfico
() [robot] robots
() [tape] ... de cintas
() [disk] ... de discos
() [network] soporte de la red
() [modem] módem
() [hub] concentrador

() [switch] conmutador
() [router] encaminador
() [bridge] puente
() [firewall] cortafuegos
() [wap] punto de acceso wireless
() [pabx] centralita telefónica
() [ipphone] teléfono IP
() [ics] Sistemas de control industrial
() [rtu]RTU - Unidad terminal remota
() [plc] PLC - Controlador lógico programable
() [pac] PAC - Controlador de automatización programable
() [ied] IED - Dispositivo electrónico inteligente
() [meter] Meter – Medidor industrial
() [bridge] Puente entre protocolos
() [hmi] HMI – Interfaz hombre-máquina
() [server] servidor
() [historian] Registro histórico
() [telemetry] Telemetría
() [ems] EMS – Sistema de gestión de energía
() [dms] DMS – Sistema de gestión de distribución
() [home] Red de control de hogar
() [hvac] HVAC – Acondicioner de temperatura

[AUX] EQUIPAMIENTO AUXILIAR

() [power] fuentes de alimentación
() [ups] sai – sistemas de alimentación ininterrumpida
() [gen] generadores eléctricos
() [ac] equipos de climatización
() [cabling] cableado de datos
() [wire]cable eléctrico
() [fiber] fibra óptica
() [supply] suministros esenciales
() [destroy] equipos de destrucción de soportes
() [furniture] mobiliario
() [safe] cajas fuertes

[L] INSTALACIONES

() [site] recinto
() [building] edificio
() [local] cuarto
() [mobile] plataformas móviles
() [car] vehículo terrestre: coche, camión, etc.
() [plane] vehículo aéreo: avión, etc.
() [ship] vehículo marítimo: buque, lancha, etc.
() [shelter] contenedores
() [channel] canalización
() [backup]instalaciones de respaldo

[P] PERSONAL

() [ue] usuarios externos
() [ui] usuarios internos
() [op] operadores
() [adm] administradores de sistemas
() [com] administradores de comunicaciones

() [dba] administradores de BBDD
() [sec] administradores de seguridad
() [dev] desarrolladores / programadores
() [sub] subcontratas
() [prov] proveedores
() [other] otros

Anexo E

Inventario de Amenazas Metodología Magerit

[N] Desastres naturales

- [N.1] Fuego
- [N.2] Daños por agua
- [N.*] Desastres naturales

[I] De origen industrial

- [I.1] Fuego
- [I.2] Daños por agua
- [I.*] Desastres industriales
- [I.3] Contaminación medioambiental
  - [I.3.1] Vibraciones
  - [I.3.2] Ruido
  - [I.3.3] Polvo
  - [I.3.4] Humo
  - [I.3.5] Vapor
- [I.4] Contaminación electromagnética
  - [I.4.11] Ruido electromagnético accidental
  - [I.4.12] Ruido electromagnético deliberado
  - [I.4.15] Pulsos electromagnéticos accidentales
  - [I.4.16] Pulsos electromagnéticos deliberados
  - [I.4.21] Ruido término accidental
  - [I.4.22] Ruido término deliberado
  - [I.4.31] Jamming
- [I.5] Avería de origen físico o lógico
  - [I.5.1] Software
  - [I.5.2] Hardware
  - [I.5.3] Equipos de Comunicaciones
  - [I.5.4] Equipamiento Auxiliar
- [I.6] Corte del suministro eléctrico
  - [I.6.11] Interrupción accidental
  - [I.6.12] Interrupción deliberada por un agente externo
  - [I.6.13] Interrupción deliberada por un agente interno
- [I.7] Condiciones Inadecuadas de temperatura o humedad
- [I.8[Fallo de servicios de comunicaciones
  - [I.8.11] Interrupción accidental
  - [I.8.12] Interrupción deliberada por agente externo
  - [I.8.13] Interrupción deliberada por un agente interno
- [I.9] Interrupción de otros servicios o suministros esenciales
  - [I.9.1] Papel
  - [I.9.2] Refrigerante
  - [I.9.3] Diesel
- [I.10] Degradación de los soportes de almacenamiento de la información
- [I.11] Emanaciones electromagnéticas
  - [I.11.1] Radio
  - [I.11.2] Térmica

[E] Errores y fallos no intencionados

- [E.1] Errores de los usuarios
- [E.2] Errores del administrador del sistema / de la seguridad
- [E.3] Errores de monitorización (log)
- [E.4] Errores de configuración
- [E.7] Deficiencias en la organización
- [E.8] Difusión de software dañino
  - [E.8.0] Gusanos
  - [E.8.1] Virus
  - [E.8.2] Caballos de Troya
  - [E.8.3] Spyware

- [E.9] Errores de [re-] encaminamiento
  - [E.9.1] Queda en casa
  - [E.9.2] A terceros con acuerdo establecido
  - [E.9.3] Al mundo entero
- [E.10] Errores de secuencia
- [E.14] Fugas de información (>E.19)
- [E.15] Alteración de la información
- [E.18] Destrucción de la Información
- [E.19] Fugas de información
  - [E.19.1] A personal interno que no necesita conocerlo
  - [E.19.2] A contratistas que no necesitan conocerlo
  - [E.19.3] A personas externas que no necesitan conocerlo
  - [E.19.4] Al público en general
  - [E.19.5] A los medios de comunicación
  - [E.19.11] Identificación de la localización
- [E.20] Vulnerabilidades de los programas (software)
  - [E.20.dos] denegación de servicio
  - [E.20.read] acceso de LECTURA
  - [E.20.write] acceso de ESCRITURA
  - [E.20.escalation] escala de privilegios
- [E.21] Errores de mantenimiento / actualización de programas (software)
- [E.23] Errores de mantenimiento / actualización de equipos (hardware)
- [E.24] Caída del sistema por agotamiento de recursos
- [E.25] Pérdida de equipos
- [E.28] Indisponibilidad del personal
  - [E.28.1] Enfermedad
  - [E.28.2] Huelga
  - [E.28.3] No hay personal
  - [E.28.4] Personal insuficiente]

[A] Ataques deliberados

- [A.3] Manipulación de los registros de actividad (log)
- [A.4] Manipulación de los ficheros de configuración
- [A.5] Suplantación de la identidad
  - [A.5.1] Por personal interno
  - [A.5.2] Por subcontratistas
  - [A.5.3] Por personas externas
- [A.6] Abuso de privilegios de acceso
  - [A.6.1] Por personal interno
  - [A.6.2] Por subcontratistas
  - [A.6.3] Por personas externas
- [A.7] Uso no previsto
  - [A.7.1] Por personal interno
  - [A.7.2] Por subcontratistas
  - [A.7.3] Por personas externas
- [A.8] Difusión de software dañino
- [A.9] [Re-]encaminamiento de mensajes
- [A.10] Alteración de secuencia
- [A.11] Acceso no autorizado
- [A.12] Análisis de tráfico
- [A.13] Repudio (negación de actuaciones)
- [A.14] Interceptación de información (escucha)
- [A.15] Modificación de la información
- [A.18] Destrucción de la información
- [A.19] Revelación de la información
- [A.22] Manipulación de programas
- [A.23] Manipulación de hardware
- [A.24] Denegación de servicio
- [A.25] Robo de equipos
- [A.26] Ataque destructivo
- [A.27] Ocupación enemiga

[A.28] Indisponibilidad del personal
[A.29] Extorsión
[A.29.1] Ataque desde el exterior
[A.29.2] Ataque desde el interior
[A.30] Ingeniería social (picaresca)
[A.31] Distracción
[A.40] Incumplimiento (leyes, reglamentos, normas, ...)

[PR] Riesgos de privacidad

[PR.2a] Problemas relativos a la licitud de la recogida de datos y del tratamiento
[PR.2b] Problemas relativos a la lealtad en la relación entre el sujeto y la organización
[PR.2c] Problemas relativos a la transparencia del tratamiento
[PR.2d] Problemas relativos a la finalidad del tratamiento
[PR.2e] Problemas relativos a la recolección excesiva de datos
[PR.2f] Problemas relativos a la exactitud de los datos recogidos
[PR.2g] Problemas relativos a la duración del plazo de conservación de los datos recogidos
[PR.2h] Problemas relativos al consentimiento del sujeto
[PR.2i] Problemas relativos a los derechos del sujeto: acceso, rectificación, cancelación y oposición
[PR.2j] Problemas relativos a la transferencia de datos a terceros
[PR.2k] Problemas relativos a roles y funciones del personal de la organización
[PR.2l] Problemas relativos a la seguridad de la información (integridad y confidencialidad)

Anexo F

Inventario de Salvaguardas Magerit

SALVAGUARDAS
[IA] Identificación y Autenticación
[IA.1] Se dispone de normativa de identificación y autenticación [IA.2] Se dispone de procedimientos para las tareas de identificación y autenticación [IA.3] Identificación de los usuarios [IA.3.1] Cada usuario recibe un identificador exclusivo (no compartido) [IA.3.2] La identificación del usuario no indica ni su función ni su nivel de privilegios. [IA.3.3] Las cuentas de invitados están sometidos a un control estricto. [IA.4] Gestión de la identificación y autenticación de usuario [IA.5] Cuentas especiales (administración) [IA.6] Canal seguro de autenticación [IA.7] {xor} Factores de autenticación que se requieren
[AC] Control de acceso lógico
[AC.1] modo evaluación [AC.2] modo evaluación [H.ST] modo evaluación
[D] Protección de la Información
[D.1] modo evaluación [D.2] modo evaluación [D.3] modo evaluación [D.I] modo evaluación [D.5] modo evaluación [D. backup] modo evaluación [D.7] modo evaluación [D.DS] modo evaluación (Uso de firmas electrónicas) [D.TS] modo evaluación
[K] Protección de claves criptográficas
[K.IC] modo evaluación (Gestión de claves de cifra de información) [K.DS] modo evaluación (Gestión de claves de firma de información) [K.disk] modo evaluación [K.comms] modo evaluación [K.509] modo evaluación
[S] Protección de los Servicios
[S.start] modo evaluación (Aceptación y puesta en operación) [S.2] modo evaluación [S.3] modo evaluación [S.4] modo evaluación
[SW] Protección de las Aplicaciones Informáticas
[SW.1] modo evaluación [SW.backup] modo evaluación [SW.start] modo evaluación (Puesta en producción) [SW.SC] modo evaluación (Se aplican perfiles de seguridad) [SW.op] modo evaluación (Explotación / Producción) [SW.CM] modo evaluación [SW.end] modo evaluación
[HW] Protección de los Equipos Informáticos
[HW.1] modo evaluación [HW.start] modo evaluación (Puesta en producción) [HW.SC] modo evaluación (Se aplican perfiles de seguridad) [HW.op] modo evaluación (Operación) [HW.CM] modo evaluación (Cambios (actualizaciones y mantenimiento) [HW.end] modo evaluación (Terminación)

[HW.PCD] modo evaluación (Informática móvil [HW.print] modo evaluación (Reproducción de documentos)
[COM] Protección de las Comunicaciones
[COM.start] modo evaluación (Entrada en servicio) [COM.SC] modo evaluación (Se aplican perfiles de seguridad) [COM.cont] modo evaluación [COM.op] modo evaluación (Operación) [COM.CM] modo evaluación (Cambios (actualizaciones y mantenimiento)) [COM.end] modo evaluación (Terminación) [COM.wifi] modo evaluación (Seguridad Wireless (Wifi)) [COM.mobile] modo evaluación (Telefonía móvil) [COM.DS] modo evaluación [COM.i] modo evaluación (Protección de la integridad de los datos intercambiados)
[AUX] Elementos Auxiliares
[AUX.start] modo evaluación (Instalación) [AUX.power] modo evaluación (Suministro eléctrico) [AUX.AC] modo evaluación (Climatización) [AUX.wires] modo evaluación (Protección del Cableado)
[PPE] Protección física de los equipos **[PPS] Protección del perímetro físico** **[PS] Gestión del Personal** **[PDS] Servicios Potencialmente peligrosos** **[IR] Gestión de incidentes** **[V] Gestión de vulnerabilidades**

Anexo G

Entrevista Personal Departamento TICs UGT-ESPE

UNIVERSIDAD DE LAS FUERZAS ARMADAS ESPE
UNIDAD DE GESTION DE TECNOLOGIAS ESPE

CARRERA DE TECNOLOGÍA EN COMPUTACIÓN

ENTREVISTA FUNCIONARIOS DEPARTAMENTO TICS UNIDAD DE GESTIÓN DE TECNOLOGÍAS ESPE

TEMA TESIS:

Análisis y evaluación de riesgos de Seguridad informática en la red de área local (LAN), de la Unidad de Gestión de Tecnologías ESPE, para permitir establecer un plan de defensa y protección.

REQUERIMIENTOS:

1. **Situación actual de red LAN Unidad de Gestión de Tecnologías ESPE:**

   Distribución de usuarios:

Unidad	Número de Pisos	Número de Áreas	Número de Usuarios	Número de Pc	
				Desktop	Laptop
Unidad de Gestión de Tecnologías (UGT-ESPE)	3	9	80	30	60

2. **Inventario de Activos de la RED LAN Unidad de Gestión de Tecnologías**

Cant	Activo	Descripción	Categoría	Ubicación	Responsable TIC's
3	Router CISCO	Enlace WAN Backup	Capa 3	Rack Comunicación	Sgop. Luis Santana
1	Router Mikrotik	Gestión WLAN Gestión WAN	Capa 3	Rack Comunicación	Sgop. Luis Santana
	Switch	Wireless	Capa 3		

2	24 puertos	Administrable	Capa 2	Rack Comunicación	Sgop. Luis Santana
3	Switch 24 puertos	No Administrable	Capa 2	Varias Áreas	Sgop. Luis Santana
3	Switch 16 puertos	No Administrable	Capa 2	Varias Áreas	Sgop. Luis Santana
1	Rack	Servidores		Gabinete Cerrado TIC's	Sgop. Luis Santana
1		Firewall FortiGuard		BACO UGT-ESPE TIC's	Sgop. Luis Santana
1	UPS 6KVA	Energía Respaldo TIC's		TIC's	Sgop. Luis Santana
1	Servidor Linux	Servicio Proxy Permisos Acceso RED		TIC's	Sgop. Luis Santana
1	Sistema Operativo Linux	Sistema Operativo Linux		TICs	Sgop. Luis Santana

3. Diagrama red LAN Unidad de Gestión de Tecnologías ESPE

4. Modelo Jerárquico de la Red LAN: Switch Unidad de Gestión de Tecnologías:

1 **Capa Core** (Switch Hewlett Packard HPE 1920 48G)

2 **Capa Distribución** (Switch Linksys LGS326P)

3 **Capa Accesso** (Switch DLINK DES 1024)

5. ACTIVOS:

- **[HW]EQUIPOS INFORMÁTICOS (Hardware)**

1	Firewall
2	Switch Core HP
3	Switch de Distribución Linksys
4	Switch de Acceso DLink
5	Router Cisco
6	Router Mikrotik
7	Servidor Linux
8	Switch Capa 2

- **[SW] SOFTWARE**

1	Sistema Operativo Linux

AUX] EQUIPAMIENTO AUXILIAR

1	Rack Comunicación TICs
2	UPS 6KVA

[L] INSTALACIONES

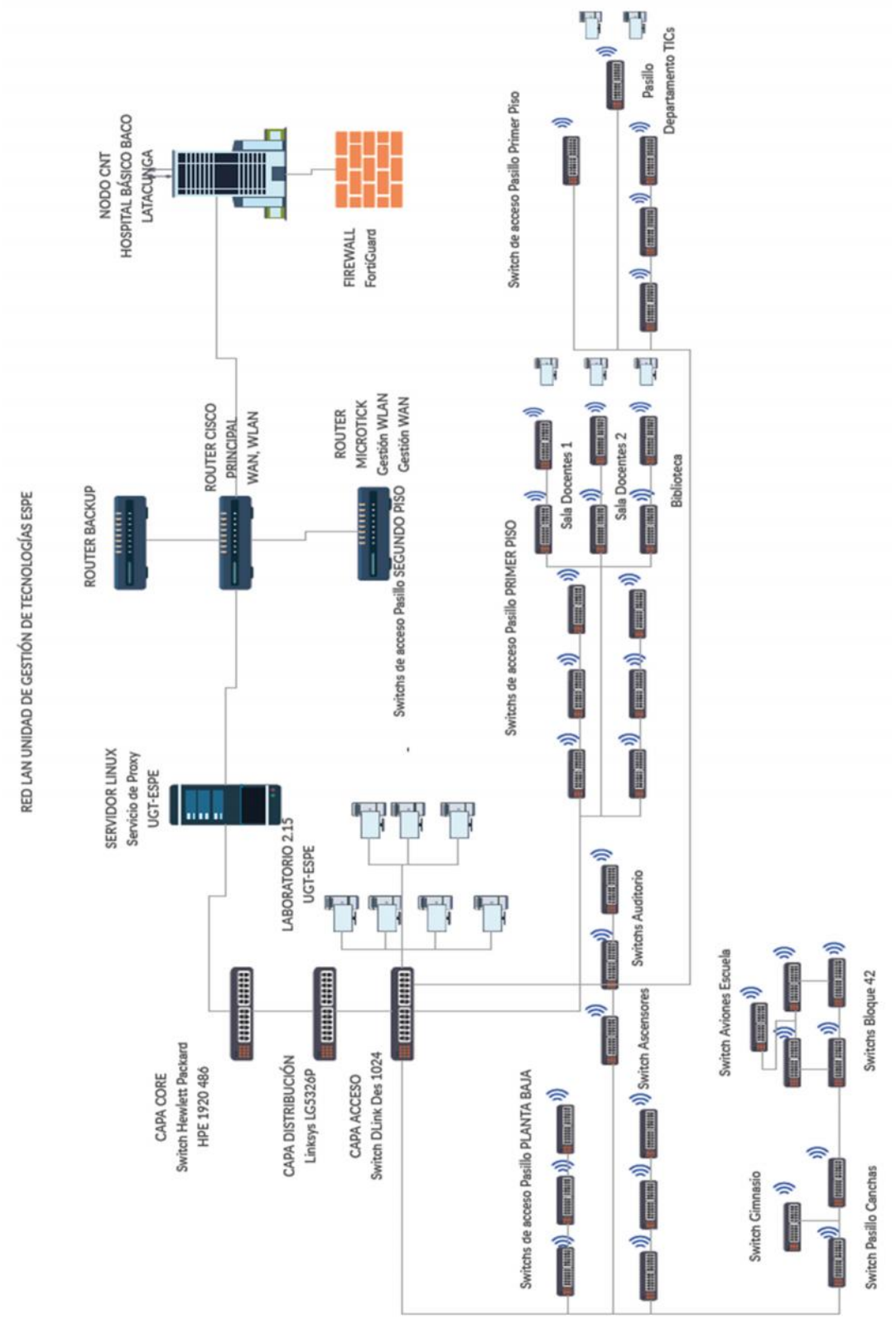
1	Cuarto Comunicaciones TICs

[P] PERSONAL

1	Administradores de Red
2	Soporte Técnico

Anexo H

Diagrama Red LAN Unidad de Gestión de Tecnologías ESPE



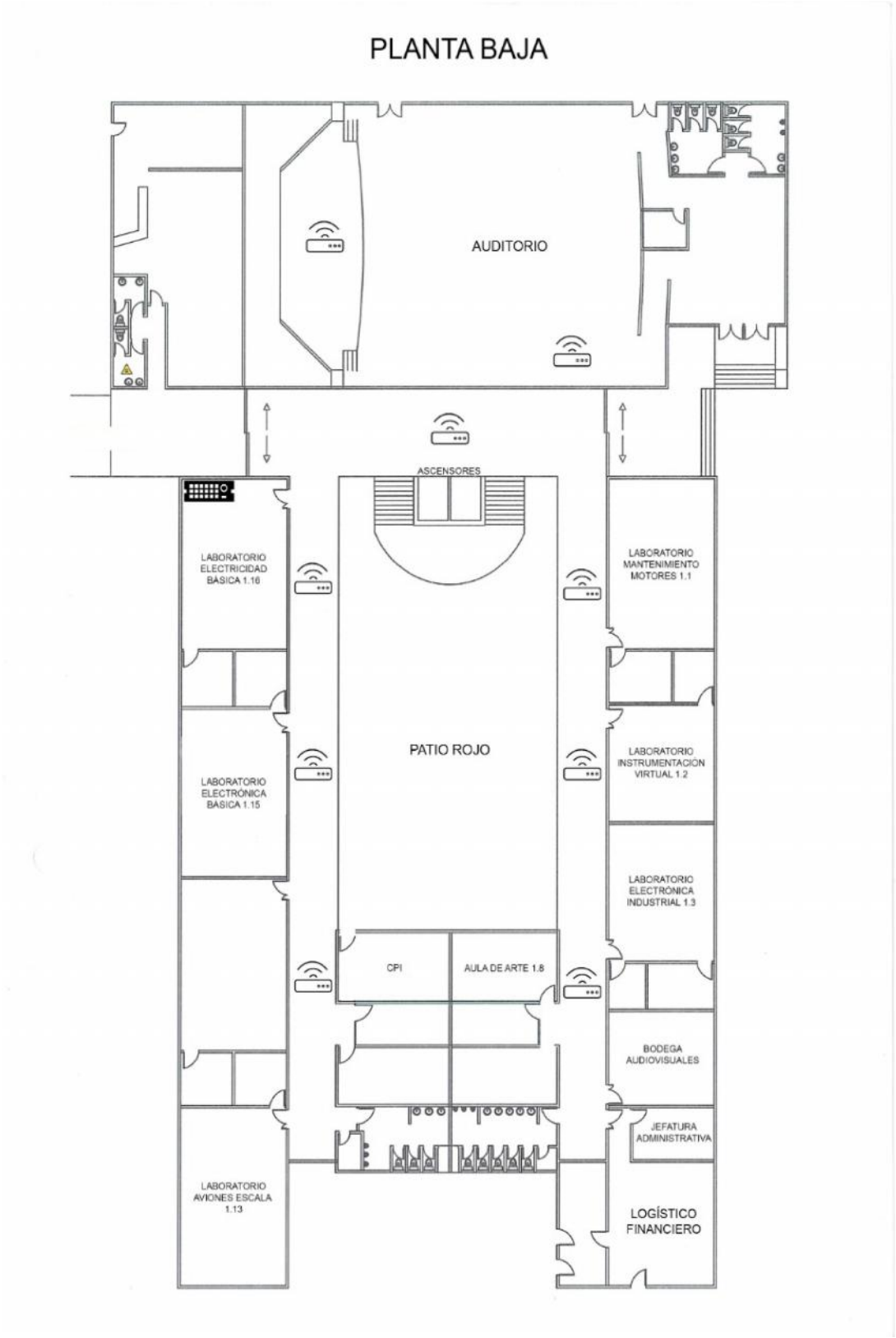
Anexo I

Planos de los equipos e instalaciones Red Unidad de Gestión de Tecnologías ESPE

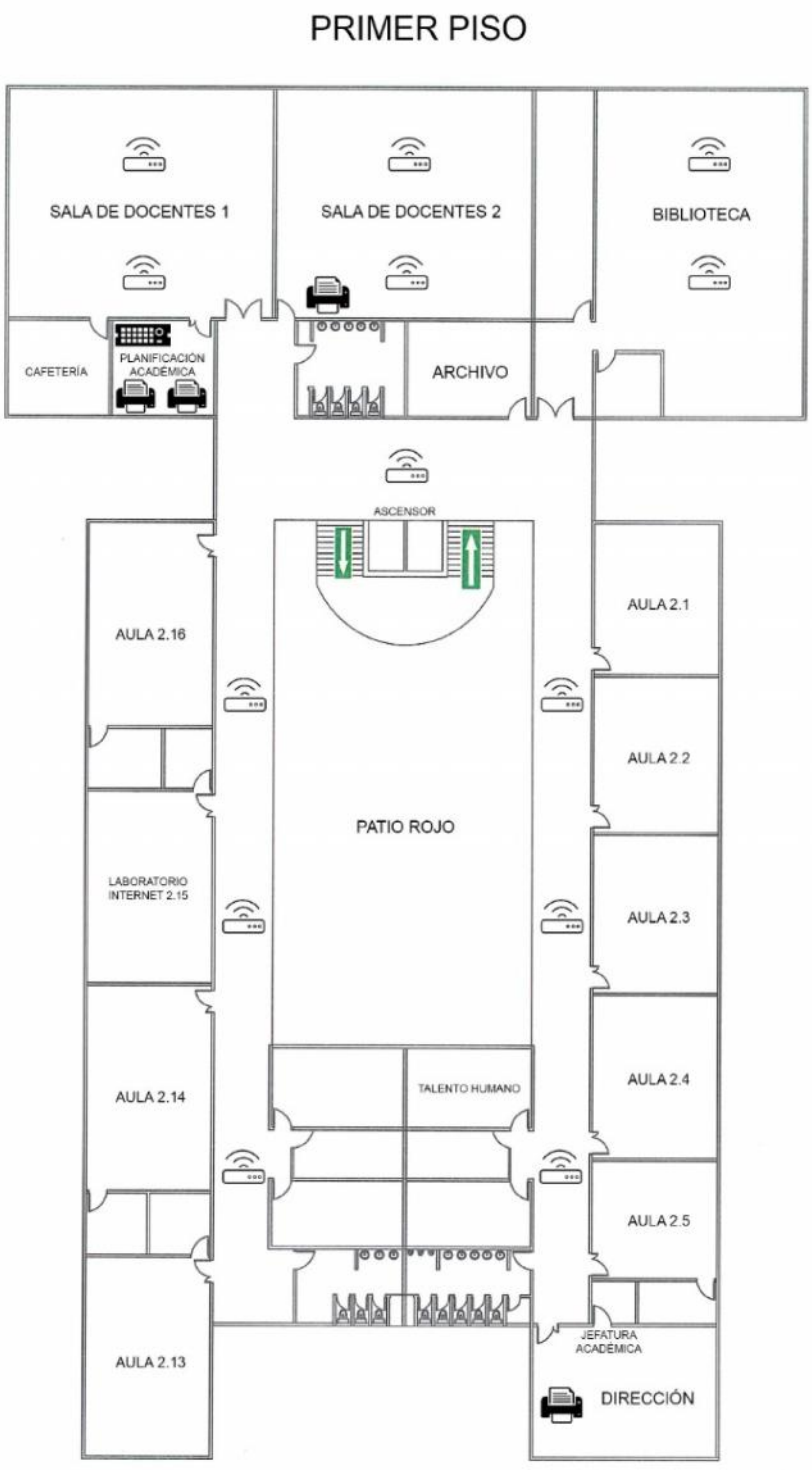
En el presente anexo se adjuntan planos en los cuales se puede identificar los equipos e instalaciones de red y distribución de las secciones en las cuales constan los departamentos que está dividida la Unidad de Gestión de Tecnologías ESPE.

1. Plano canchas, Bloque 42 y Aviones Escuela

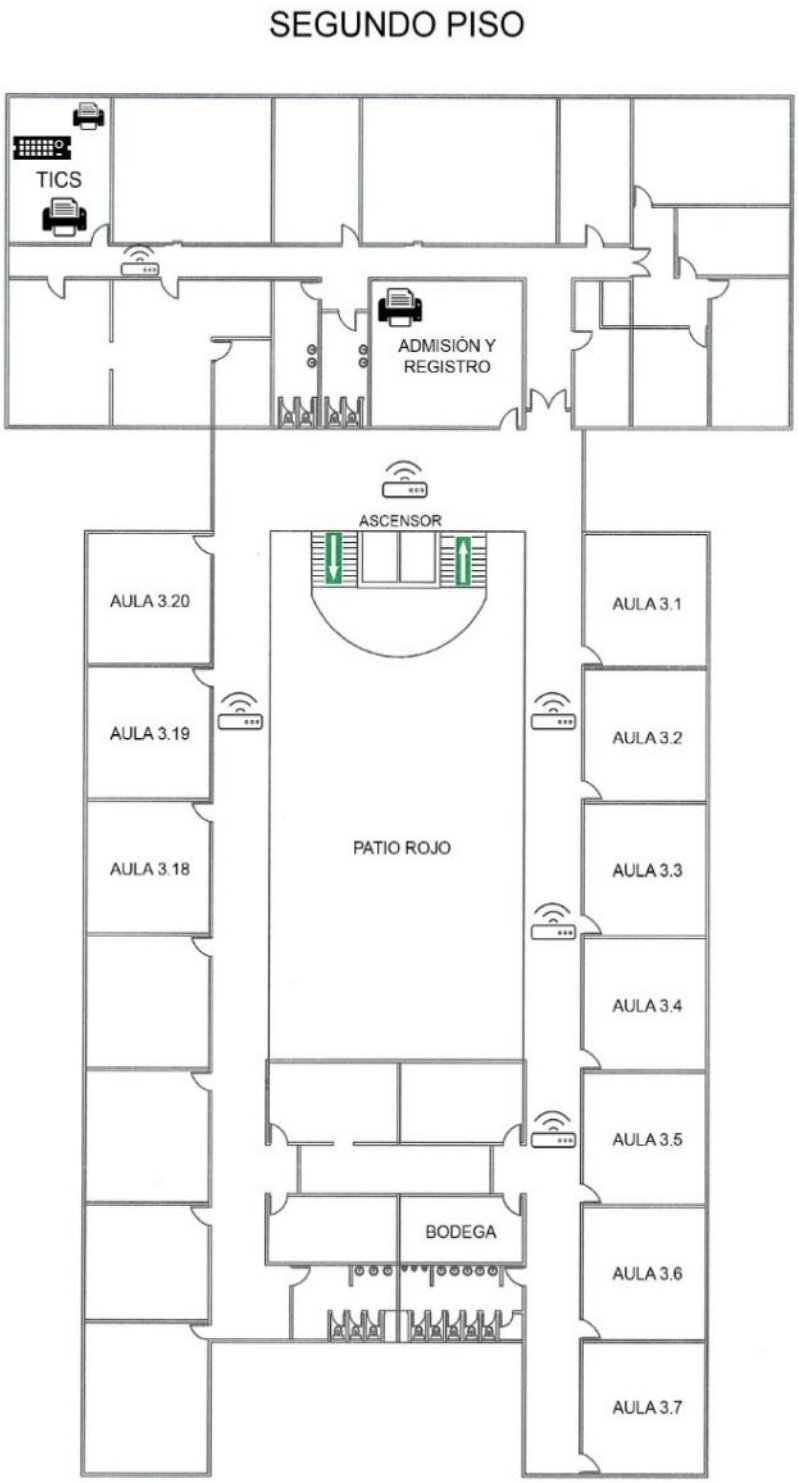
2. Plano Planta Baja



3. Plano Primer Piso



4. Plano Segundo Piso



Anexo J.

Propuesta Documentos Entregables Plan de Seguridad Informática de la Unidad de Gestión de Tecnologías ESPE (Tablas de Registros)

Procedimiento para Control de Documentos

<table>
<tr><td colspan="2">PROCEDIMIENTO PARA CONTROL DE DOCUMENTOS Y REGISTROS</td><td colspan="2">UNIDAD DE GESTIÓN DE TECNOLOGÍAS</td></tr>
<tr><td>Código:</td><td colspan="2">Versión:</td><td>Número de páginas:</td></tr>
<tr><td colspan="2">Elaborado por:</td><td colspan="2">Fecha de Elaboración:</td></tr>
<tr><td>N° Versión del Documento:</td><td>Revisado por:</td><td>Fecha de Revisión:</td><td>Cambio Realizado:</td></tr>
<tr><td colspan="4">Aprobado por:</td></tr>
<tr><td colspan="4">Objetivo:
Definir el manejo de documentos internos y externos de la Unidad de Gestión de Tecnologías ESPE.</td></tr>
<tr><td colspan="4">Alcance:
El presente documento muestra la forma en la cual deben ser elaborados los documentos.</td></tr>
<tr><td colspan="4">Usuarios de la Política:
Documento dirigido para todos los usuarios de la Institución</td></tr>
<tr><td colspan="4">Documento de Apoyo:</td></tr>
<tr><td colspan="4">POLÍTICAS:

El procedimiento de contar con adecuados registros de documentos, permite una organización eficaz de las acciones que pueden realizar, siendo la misma proporcionada de forma ágil y eficiente. Contribuyendo a la correcta preservación de la documentación.</td></tr>
<tr><td colspan="4">RESPONSABILIDAD:
Todos los documentos y registros que se realicen deben tener un responsable. Para lo cual al final de cada documento se debe contar con una firma de responsabilidad, en el mismo que debe tener el nombre, cargo y la fecha en la cual se realizó la firma del documento.

_____
Firma de Responsabilidad
(Sello de la Institución)

NOMBRE: _____
CARGO: _____
FECHA: _____</td></tr>
<tr><td colspan="2">Fecha de Caducidad:</td><td colspan="2">Periodicidad de Revisión:</td></tr>
</table>

Políticas de Seguridad de la Información

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN		UNIDAD DE GESTIÓN DE TECNOLOGÍAS	
Código:	**Versión:**	**Número de páginas:**	
Elaborado por:		**Fecha de Elaboración:**	
N° Versión del Documento:	**Revisado por:**	**Fecha de Revisión:**	**Cambio Realizado:**
Aprobado por:			

Objetivo:

Definir criterios y reglas necesarias para una correcta gestión de la seguridad de la información.

Alcance:

El presente documento muestra políticas que puedan ser aplicadas por la Unidad de Gestión de Tecnologías ESPE

Usuarios de la Política:

Documento dirigido para todos los usuarios involucrados en los procesos de la Institución

Documento de Apoyo:

Norma ISO/IEC 27001

POLÍTICAS:

1. La propuesta de Plan de Seguridad Informática para la Unidad de Gestión de Tecnologías ESPE, se encuentra encaminada a mejorar el sistema se seguridad informática, la misma que será entregada conforme a ser una propuesta de plan que pueda ser útil para combatir amenazas posibles.
2. El acceso a cada una de las tecnologías de la Institución, estarán expresamente aprobadas por el personal encargado del departamento de las TICs, y siendo previamente preparados en cada uno de los aspectos de la seguridad informática.
3. Cada uno de los usuarios de la tecnologías informáticas que ofrece la institución, responden estrictamente por su protección y se encuentran en la obligación de informar cualquier incidente que pueda ocurrir a la persona responsable del Departamento de TICs de la Unidad de Gestión de Tecnologías ESPE, para la rápida solución.

Responsabilidad Personal:

El personal encargado del Departamento de TICs de la Unidad de Gestión de Tecnologías ESPE, tienen entre sus funciones, responsabilidades y obligaciones:

a) Garantizar la aplicación de las políticas de seguridad definidas para la red por la Institución.

b) Proteger la integridad del funcionamiento de la Red, protegiendo el correcto funcionamiento de los dispositivos y servicios de la misma.

c) Garantizar que los servicios, que se encuentran instalados, funcionen de acuerdo a los fines para los que fueron creados.

d) Ante posibles afectaciones por amenazas, de programas maliciosos, virus informáticos o ataques, informar a la persona encargada del Departamento de TICs para poder encontrar una posible solución.

RESPONSABILIDAD:

Todos los documentos y registros que se realicen deben tener un responsable. Para lo cual al final de cada documento se debe contar con una firma de responsabilidad, en el mismo que debe tener el nombre, cargo y la fecha en la cual se realizó la firma del documento.

_____

Firma de Responsabilidad
(Sello de la Institución)

NOMBRE: _____
CARGO: _____
FECHA: _____

Fecha de Caducidad:	**Periodicidad de Revisión:**

Anexo K

Expediente (Registro) Técnico

REGISTRO TÉCNICO DE ACTIVIDADES		**UNIDAD DE GESTIÓN DE TECNOLOGÍAS**	
N° Registro	**Registro Técnico Descripción**	**Registro Técnico Preventivo (P) Detección (D)**	Fecha de Elaboración:
1			
2			
3			
4			
5			

RESPONSABILIDAD:

Todos los documentos y registros que se realicen deben tener un responsable. Para lo cual al final de cada documento se debe contar con una firma de responsabilidad, en el mismo que debe tener el nombre, cargo y la fecha en la cual se realizó la firma del documento.

_____
Firma de Responsabilidad
(Sello de la Institución)

NOMBRE: _____
CARGO: _____
FECHA: _____

Fecha de Caducidad:	**Periodicidad de Revisión:**

HOJA DE LEGALIZACIÓN DE FIRMAS

DEL CONTENIDO DE LA PRESENTE INVESTIGACIÓN

SE RESPONSABILIZA EL AUTOR

ORDOÑEZ VEINTIMILLA DIANA JAZMÍN

DIRECTOR DE LA CARRERA DE TECNOLOGÍA EN COMPUTACIÓN

ING. JORGE PARDO

Latacunga, de Febrero de 2019

SESIÓN DE DERECHOS DE PROPIEDAD INTELECTUAL

Yo, **DIANA JAZMÍN ORDÓÑEZ VEINTIMILLA,** Egresada de la carrera de Tecnología en Computación en el año 2018, con cedula de Ciudadanía No. **0202031076,** Autor del trabajo de Graduación "**ANÁLISIS Y EVALUACIÓN DE RIESGOS DE SEGURIDAD INFORMÁTICA EN LA RED DE ÁREA LOCAL (LAN), DE LA UNIDAD DE GESTIÓN DE TECNOLOGÍAS ESPE, PARA PERMITIR ESTABLECER UN PLAN DE DEFENSA Y PROTECCIÓN**", cedo mis derechos de propiedad intelectual a favor de la Unidad de Gestión de Tecnologías de la Universidad de las Fuerzas Armadas.

Para constancia firmo la presente sesión de propiedad intelectual.

_____

ORDOÑEZ VEINTIMILLA DIANA JAZMÍN

Latacunga, Febrero de 2019

HOJA DE VIDA

DATOS PERSONALES

Nombre: Diana Jazmín

Apellidos: Ordóñez Veintimilla

Cédula de Identidad: 0202031076

Fecha de Nacimiento: 14 de Agosto de 1994

Lugar de Nacimiento: Chillanes – Bolívar - Ecuador

Estado Civil: Soltera

Teléfono: 0981251109

Email: diana.ordonez778577@gmail.com

FORMACIÓN ACADÉMICA

ESTUDIOS PRIMARIOS: Escuela “Belisario Quevedo”

ESTUDIOS SECUNDARIOS: Colegio “Nacional Chillanes”

ESTUDIOS DE TERCER NIVEL: Universidad de las Fuerzas Armadas -ESPE