UNIVERSIDAD NACIONAL "PEDRO RUIZ GALLO"

FACULTAD DE CIENCIAS FÍSICAS Y MATEMÁTICAS

ESCUELA PROFESIONAL DE INGENIERÍA EN COMPUTACIÓN E INFORMÁTICA

"APLICACIÓN DE LA METODOLOGÍA MAGERIT PARA EL ANÁLISIS Y GESTIÓN DE RIESGOS EN LOS SERVIDORES DE LOS SISTEMAS DE GESTIÓN ACADÉMICA DE LA UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO"

TESIS

PRESENTADO PARA OPTAR EL TÍTULO PROFESIONAL DE INGENIERO EN COMPUTACIÓN E INFORMÁTICA

PRESENTADO POR:
BACH. JAVIER GUSTAVO GUEVARA CHUMÁN

ASESOR:
ING. GILBERTO CARRIÓN BARCO

LAMBAYEQUE - PERÚ
SETIEMBRE - 2015

UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO

FACULTAD DE CIENCIAS FÍSICAS Y MATEMATICAS

ESCUELA PROFESIONAL DE INGENIERÍA EN COMPUTACIÓN E INFORMATICA

TESIS

APLICACIÓN DE LA METODOLOGÍA MAGERIT PARA EL ANÁLISIS Y GESTIÓN DE RIESGOS EN LOS SERVIDORES DE LOS SISTEMAS DE GESTIÓN ACADÉMICA DE LA UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO

PRESENTADO POR:

BACH. JAVIER GUSTAVO GUEVARA CHUMÁN

PARA OPTAR EL TÍTULO PROFESIONAL DE:

INGENIERO EN COMPUTACIÓN E INFORMÁTICA

ASESOR:

ING. GILBERTO CARRIÓN BARCO

Lambayeque, Septiembre del 2015

APLICACIÓN DE LA METODOLOGÍA MAGERIT PARA EL ANÁLISIS Y GESTIÓN DE RIESGOS EN LOS SERVIDORES DE LOS SISTEMAS DE GESTIÓN ACADÉMICA DE LA UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO

Tesis sustentada por:

Bach. Javier Gustavo Guevara Chumán
Tesista

Como requisito para obtener el Título Profesional de:

INGENIERO EN COMPUTACIÓN E INFORMÁTICA

Aceptada por la Escuela Profesional de Ingeniería en Computación e Informática

Ing. Luis Alberto Reyes Lescano
Presidente

Ing. Percy Javier Celis Bravo
Secretario

Ing. Denny John Fuentes Adrianzén
Vocal

Ing. Gilberto Carrión Barco
Asesor

Lambayeque, Septiembre del 2015

DEDICATORIA

A Dios nuestro señor, por guiarme y bendecirme en el recorrido de mi vida.

A mis padres y hermana, a mi familia por la confianza y el apoyo que día a día me brindan.

AGRADECIMIENTO

A Dios, por haber permitido la culminación exitosa de este trabajo y por las bendiciones otorgadas.

A mis padres, por la confianza depositada y el apoyo durante toda mi vida personal y académica. A mi hermana por los consejos, por el apoyo a pesar de la distancia.

A cada uno de mis profesores de la Universidad Nacional Pedro Ruiz Gallo los cuales me brindaron sus conocimientos y enseñanzas. En especial al Ing. Gilberto Carrión por la asesoría brindada en el desarrollo de la presente Tesis.

Y a todas las personas que apoyaron con sus conocimientos profesionales como guías en la realización de la presente tesis.

RESUMEN

La presente tesis se desarrolló en los ambientes de la Universidad Nacional Pedro Ruiz Gallo en la provincia de Lambayeque, región Lambayeque específicamente en el área de administración de servidores – Red Telemática, en donde participo el encargado del área que brindo información y apoyo para determinar la situación actual de la seguridad de los servidores de los sistemas de gestión académica y los criterios para identificar los riesgos que se presentan. El propósito fue brindar un Plan de Mitigación de riesgos basado en las medidas de seguridad ya implementadas, aplicando la metodología Magerit, Metodología de Análisis y Gestión de riesgos de las tecnologías de Información, la cual abarca dos procesos que son estructurados de la siguiente manera: Método de análisis de riesgos (Identificación, Dependencias y Valoración de los activos; Identificación y Valoración de las amenazas; Identificación y Valoración de las salvaguardas existentes; estimación del impacto y riesgo). Proceso De Gestión De Riesgos (Toma de decisiones y Plan de Mitigación), y la herramienta Pilar, Procedimiento Informático Lógico de Análisis de Riesgos, aplicación desarrollada en java y desarrollada a medida para la implementación de Magerit.

ABSTRACT

This thesis is developed in the environment of the National University Pedro Ruiz Gallo in the province of Lambayeque, Lambayeque region specifically in the area of server management - Telematic Network, where he participated in charge of the area to provide information and support to assess the situation Current security servers academic management systems and criteria for identifying the risks that arise. The purpose was to provide a Risk Mitigation Plan based on the security measures already in place, applying the methodology Magerit, Methods of Analysis and Risk Management Information technology, which includes two processes that are structured as follows: risk analysis method (ID, Agencies and evaluation assets; identification and assessment of threats, identification and assessment of existing safeguards, impact and risk estimation). Risk Process (Decision Making and Mitigation Plan) Management and Pilar, Logical Computer Procedure for Risk Analysis, application developed in Java and developed as for the implementation of Magerit tool

ÍNDICE GENERAL

ÍNDICE DE CUADROS

INDICE DE TABLAS

ÍNDICE DE GRÁFICOS

INDICE DE FIGURAS

INTRODUCCIÓN

La presente tesis que tiene por objetivo Identificar los riesgos que se presentan en los servidores de los sistemas de Gestión Académica de la Universidad Nacional Pedro Ruiz Gallo aplicando la metodología MAGERIT para el Análisis y Gestión de riesgos y proponiendo las medidas que deben adoptarse para el control de estos riesgos.

La situación problemática que conllevo a realizar el desarrollo de la presente tesis es el problema que se genera cada inicio y fin de ciclo en la Universidad Nacional Pedro Ruiz Gallo donde existen sistemas que gestionan el proceso de matrículas y la publicación de notas de fin de ciclo. Constantemente las quejas por parte del sector universitario ya que a pesar de establecerse un calendario para el proceso de matrícula la gran mayoría tiene problemas a la momento del acceso a la aplicación para la matricula; los sistemas de gestión de matrícula están almacenados en servidores de aplicaciones, y como soporte de data servidores de base de datos, en base a esto se procedió a planificar y desarrollar la presente tesis.

Las fuentes bibliográficas fueron difícil de recolectar ya que en el país no se cuenta con mucha información acerca de la aplicación Magerit ni de la herramienta Pilar, se acudió a información de casos aplicados similares en otros países , ya que la metodología fue desarrollada por el gobierno Español.

CAPITULO I:
DATOS GENERALES DE LA ORGANIZACIÓN

CAPITULO I: DATOS GENERALES DE LA ORGANIZACIÓN

1.1 Descripción de la Organización

La organización elegida es la Universidad Nacional Pedro Ruiz Gallo (UNPRG), ubicada en la av. Juan XXIII # 391 en la Ciudad Universitaria, Lambayeque – Perú, es una comunidad académica orientada a la investigación y a la docencia, que brinda una formación humanista, científica y tecnológica con una clara conciencia de nuestro país como realidad multicultural. Adopta el concepto de educación como derecho fundamental y servicio público esencial. Está integrada por profesores, estudiantes, trabajadores administrativos y graduados.

El desarrollo del proyecto de tesis en mención está centrado en el Área de Administración de Red (AAR), perteneciente a la Dirección Universitaria de Informática y Sistemas (DUIS) anteriormente conocida como Oficina Central de Informática (OCCI).

La Dirección Universitaria de Informática y Sistemas es el órgano administrativo de apoyo a la Alta Dirección de la UNPRG, cuyo objetivo es brindar servicios de procesamiento de información a los órganos internos de la Universidad.
Según el Estatuto vigente, aprobado por la Asamblea Estatutaria en sesión del día 09 de octubre de 2014 y promulgado por Resolución N° 1835 - 2014-R, artículo 181°, La Dirección Universitaria de Informática y Sistemas es la encargada de organizar y dirigir los procesos y servicios informáticos de la Universidad, determinando los procedimientos, buenas prácticas y estándares necesarios, a fin de proveer al usuario final el acceso seguro a la información institucional y la red global mediante el correcto uso de las tecnologías de información.

Director de DUIS:
Ing. Luis Alberto Reyes Lescano
Responsable del Área de Administración de Red:
Ing. Vladimir Sabino Gonzáles Mechán

1.2 Misión, Visión y Objetivos de la Organización

1.2.1 Misión

Misión de la Dirección Universitaria de Informática y Sistemas
Planificar, desarrollar, evaluar y dar soporte técnico a los servicios tanto académicos como administrativos que se dan en todas las dependencias de nuestra Universidad, utilizando Tecnologías de la Información y Comunicaciones (TICs) para el logro de los objetivos buscados por la Alta Dirección, dentro del Plan Estratégico Institucional.

1.2.2 Visión

Visión de la Dirección Universitaria de Informática y Sistemas
Ser la Dirección que lidere la generación de herramientas y soluciones tecnológicas que necesita la UNPRG, además que promueva el intercambio y la transferencia de dicho conocimiento con sus pares de otras universidades y empresas públicas y privadas.

1.2.3 Objetivos

Los Principales Objetivos de la Dirección Universitaria de Informática y Sistemas

- Brinda apoyo y asesoramiento técnico – administrativo a las diversas dependencias de la Universidad sobre la base de los requerimientos funcionales de cada una de ellas.
- Vela por la correcta administración de los recursos humanos, financieros y materiales de acuerdo a las normas emitidas, por los correspondientes sistemas administrativos.

1.3 Estructura Orgánica

Organigrama Funcional de la Dirección Universitaria de Informática y Sistemas
Área de Administración de Red (AAR)-UNPRG.

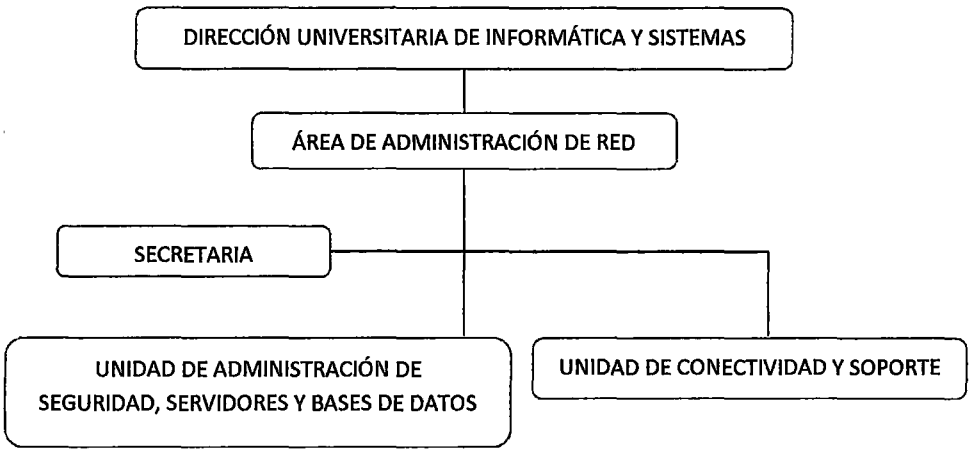

Gráfico 1: Organigrama Funcional del Área de Administración de Red
Fuente: Área de Administración de Red (AAR)-UNPRG

1.4 Situación Actual de los Servidores de los Sistemas de Gestión Académica – Unprg

La situación actual de los servidores, datos que fueron obtenidos a través de entrevistas al encargado del área de administración de la red, recolección de datos de documentos pertenecientes al área, entre otros.

1.4.1 Red Física

Diseño de parte de la red de la UNPRG, centrado en el objetivo principal de estudio y su entorno inmediato.

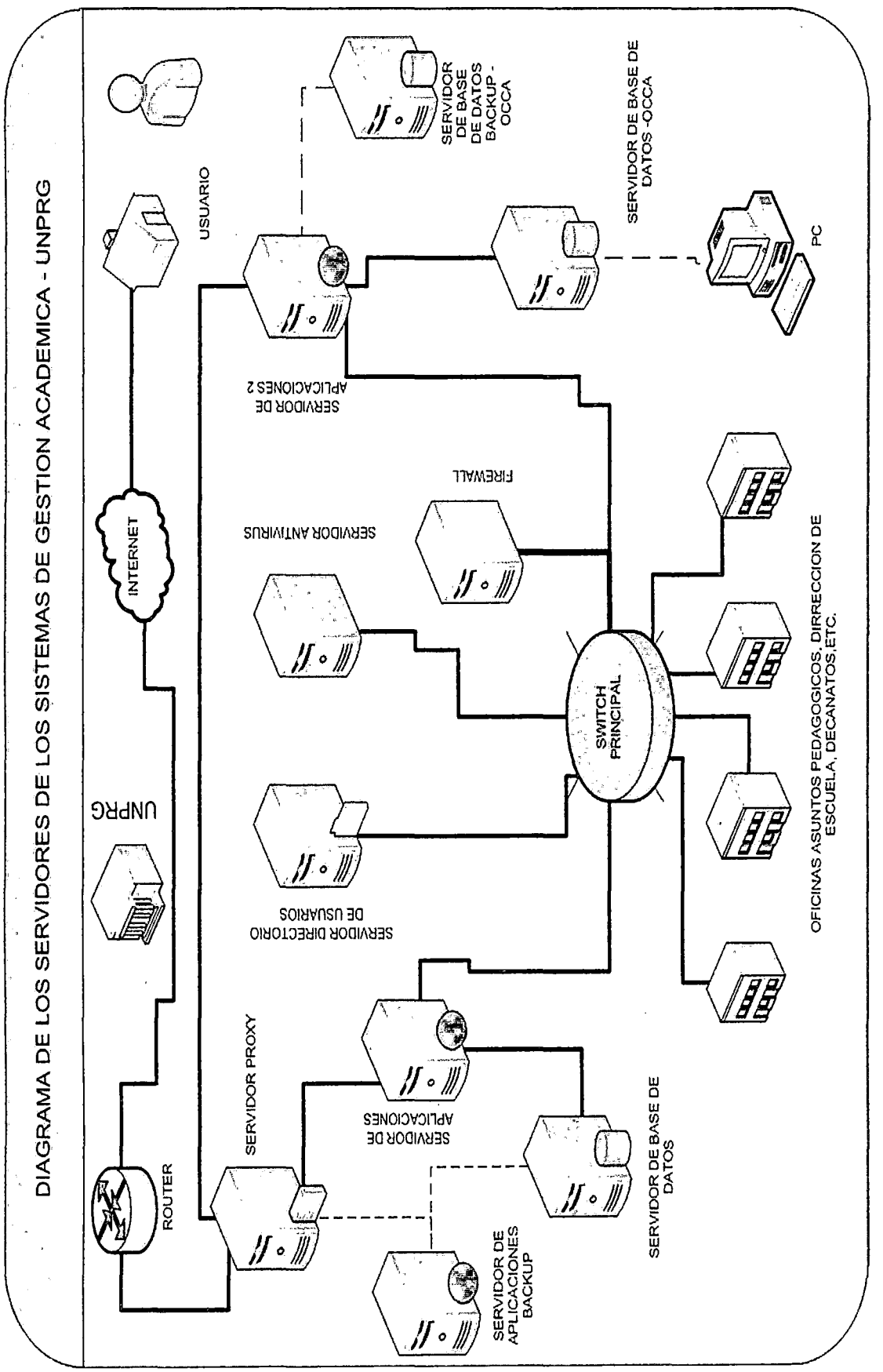

Figura 1: Red física de los servidores de los sistemas de gestión académica – UNPRG

Fuente: Elaborado por el autor

En la figura siguiente, se indica los principales servidores involucrados en el funcionamiento de los sistemas.

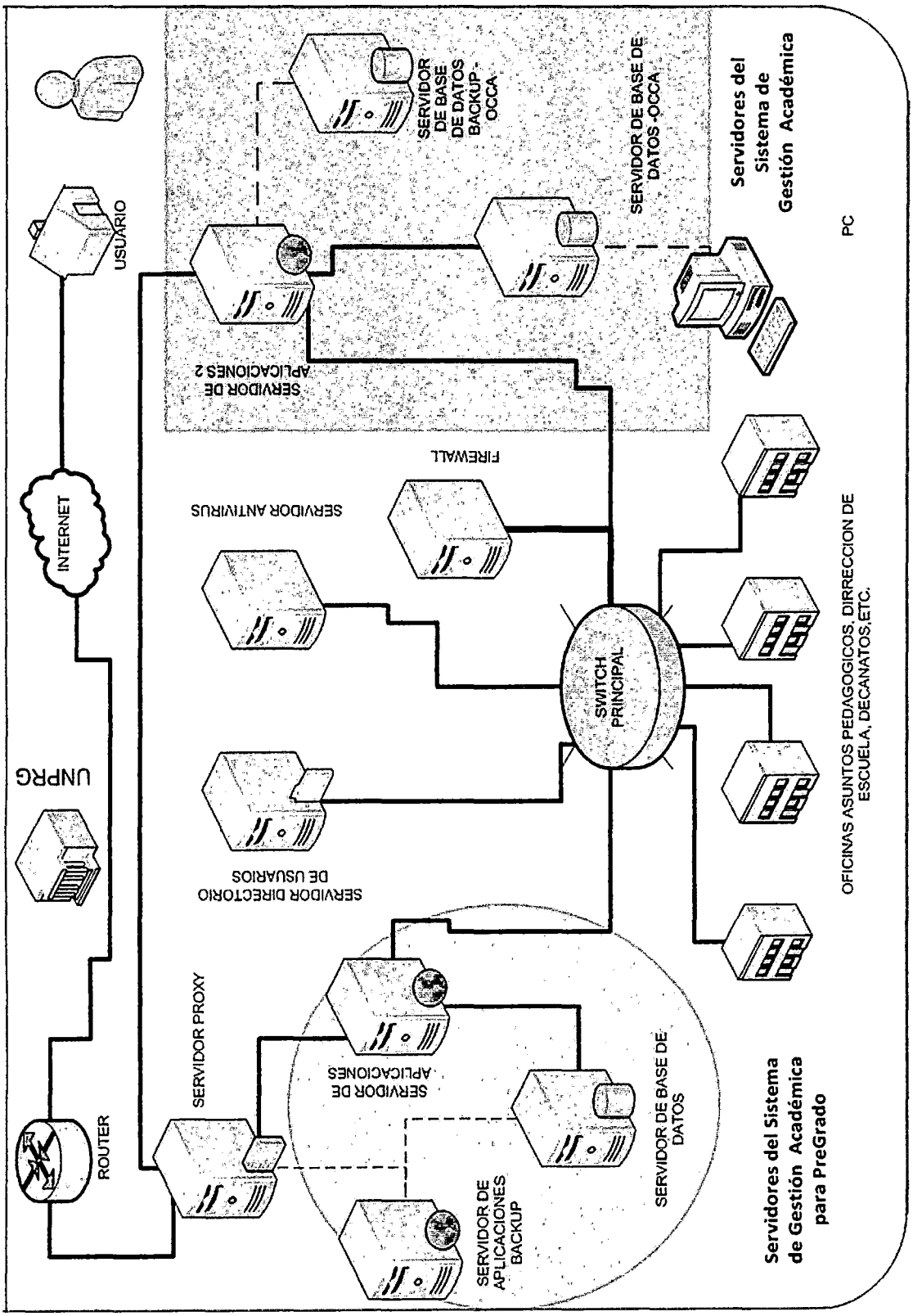

Figura 2: Principales servidores de los sistemas de gestión académica
Fuente: Elaborado por el autor

1.4.2 Redes de Datos

El acceso a los sistemas de gestión académica es a través de internet desde cualquier punto, teniendo un usuario y contraseña registrada, también se puede acceder al sistema utilizando la red de datos de la universidad está comprendida en diferentes áreas, las direcciones ip no se muestran completas por motivos de seguridad o mal uso de los mismos, las cuales se detallan en el siguiente cuadro:

Descripción de la Ubicación	***Direccionamiento ip***
Edificio del Rectorado	*10.1.x.y*
Facultad de Ingeniería Mecánica Eléctrica (FIME)	*10.1.x.y*
Facultad de Ingeniería Civil, de Sistemas y Arquitectura (FICSA)	*10.1.x.y*
Facultad de Ingeniería Química e Industrias Alimentarías (FIQIA)	*10.1.x.y*
Facultad de Ciencias Físicas y Matemáticas	*10.1.x.y*
Facultad de Biología	*10.1.x.y*
Facultad de Ingeniería Agrícola	*10.1.x.y*
Facultad de Agronomía	*10.1.x.y*
Facultad de Zootecnia	*10.1.x.y*
Facultad de Derecho	*10.1.x.y*
Facultad de Enfermería	*10.1.x.y*
Facultad de Ciencias Económicas, Contables y Administrativas	*10.1.x.y*
Dirección Universitaria de Informática y Sistemas (DUIS)	*10.1.x.y*
Facultad de Ciencias Históricas, Sociales y Educación (FACHSE)	*10.1.x.y*
Facultad de Medicina Humana	*10.1.x.y*
Facultad de Medicina Veterinaria	*10.1.x.y*

Cuadro 1: Ubicación De La Red Del Campus Universitario – UNPRG

Fuente: Elaborada por el autor

1.4.3 Configuración de la Red del Campus UNPRG.

El enrutamiento de los equipos de las áreas involucradas, se realiza dinámicamente utilizando el protocolo DHCP

1.4.4 Servicios

La universidad ofrece varios servicios, mencionare el servicio que abarca el estudio del proyecto que es el servicio de gestión académica, el cual cuenta con dos sistemas implementados que se describen a continuación:

- Sistema de Gestión Académica para Pregrado
- Sistema de Gestión Académica

1.4.4.1 Sistema de Gestión Académica para Pregrado

Objetivos: Gestionar el proceso de matrículas y notas de los alumnos de pre grado de las diferentes sedes de la UNPRG

Alcances

- Oficina Central de Asuntos Académicos
- Oficina de Asuntos Pedagógicos
- Departamentos Académicos
- Direcciones de Escuelas
- Oficina de Grados y Títulos

Funciones Principales

- Planificar ciclo académico
- Programar de cursos
- Asignar cargas lectivas
- Generar horarios
- Registrar y verificar matriculas
- Emitir constancias

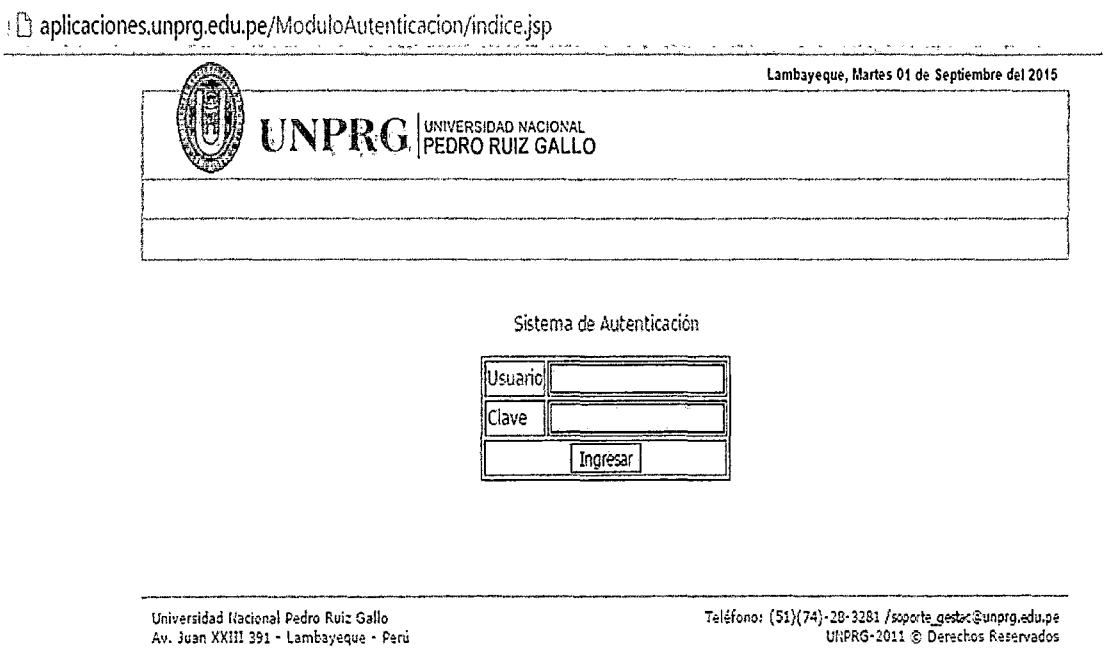

Figura 3: Aplicación de actas virtuales- UNPRG
Fuente: imagen tomada de la página web aplicaciones

1.4.4.2 Sistema de Gestión Académica

Objetivos: Gestionar el proceso de matrículas y notas de los alumnos de la UNPRG

Alcances

- Oficina Central de Asuntos Académicos
- Oficina de Asuntos Pedagógicos
- Departamentos Académicos
- Direcciones de Escuelas
- Oficina de Grados y Títulos

Figura 4: OCAA- UNPRG

Fuente: imagen tomada de la página web.

1.4.5 Descripción del Hardware y Software de los Servidores

La descripción de los servidores de los sistemas de gestión académica de la U.N.P.R.G. En las siguientes tablas, los servidores del sistema de gestión académica y del sistema de gestión académica para pre-grado, y los algunos servidores que aportan al funcionamiento de los sistemas.

HARDWARE	***SOFTWARE***		***DESCRIPCIÓN***
HP PROLIANT DL380G6 INTEL XEON QUAD CORE X5560 2.8 GHZ	*GNU/LINUX CENTOS 5.6*	*VIRTUALIZACIÓN KVM (APLICACIONES WEB , ELEARNING EPG, POSTGRES SQL , APACHE ,MYSQL, TOMCAT 6)*	*SERVIDOR APLICACIONES*
HP PROLIANT DL380G6 INTEL XEON X5560 2.8 GHZ (2)	*WINDOWS SERVER 2008 EE*	*VIRTUALIZACIÓN HYPER-V (APLICACIONES WEB, SERVIDOR VPN), BACKUP DE ADMISIÓN, WEB. EPG UNPRG*	*SERVIDOR APLICACIONES BACKUP*
HP PROLIANT DL380G5 INTEL XEON QUAD CORE 2.0 GHZ	*ORACLE ENTERPRISE LINUX 5.6*	*SERVIDOR DE BASE DE DATOS ORACLE (SISTEMAS INFORMÁTICOS PRODUCCION)*	*SERVIDOR BASE DE DATOS*
HP PROLIANT DL380G5 INTEL XEON QUAD CORE 2.0 GHZ	*ORACLE ENTERPRISE LINUX 5.6*	*VIRTUALIZACIÓN KVM (SERVER APLICACIONES WEB 2, ACCESO REMOTO, SERVER FTP)*	*SERVIDOR APLICACIONES 2*
HP PROLIANT DL380 INTEL XEON 2.80 GHZ	*WINDOWS 2000 ADVANCED SERVER*	*BASE DE DATOS SISTEMA ACADÉMICO GESTAC*	*SERVIDOR BASE DE DATOS GESTAC*
HP STORAGEWORKS MSA20	*ADMINISTRABLE POR SOFTWARE*	*SISTEMA DE ALMACENAMIENTO DE BASES DE DATOS Y ARCHIVOS*	*SERVIDOR BASE DE DATOS BACKUP*

Cuadro 2: Descripción de los servidores de los sistemas de gestión académica – UNPRG
Fuente: Área de Administración de Red (AAR)-UNPRG

HARDWARE	*SOFTWARE*		*DESCRIPCIÓN*
HP PROLIANT DL360 G3 INTEL XEON 2.80 GHZ	*WINDOWS 2000 SERVER*	*ISA SERVER 2000 - ACCESO INTERNET*	*ACCESO A INTERNET*
HP BLADESYSTEM C3000 INTEL XEON QUAD CORE 2 GHZ	*WINDOWS SERVER 2008*	*SERVICIOS ACTIVE DIRECTORY DOMAIN SERVICES WINDOWS 2008 R2, APLICACIONES DE ESCRITORIO SIGA, RADIUS*	*SERVIDOR DIRECTORIO DE USUARIOS*
HP DC5750 INTEL 2 DUO CORE 3.0 GHZ	*WINDOWS SERVER 2003*	*SERVER ANTIVIRUS CONSOLA DE ACTUALIZACIÓN*	*SERVIDOR ANTIVIRUS*
HP DC7600 Intel Pentium 4 3.0 GHz	*ENDIAN*	*FIREWALL PROXY ENDIAN LINEA SPEEDY*	*SERVIDOR PROXY*

Cuadro 3: Descripción de los servidores – UNPRG
Fuente: Área de Administración de Red (AAR)-UNPRG

CAPITULO II: PROBLEMÁTICA DE LA INVESTIGACIÓN

CAPITULO II: PROBLEMÁTICA DE LA INVESTIGACIÓN

2.1 Realidad Problemática

2.1.1 Planteamiento del Problema

La Universidad Nacional Pedro Ruiz Gallo, cuenta con una diversidad de sistemas de información, entre los cuales se encuentra el Sistema De Gestión Académica Para Pregrado y el Sistema de Gestión Académica (GESTAC), que tiene como objetivo Gestionar el proceso de matrículas y notas de los alumnos, utilizando servidores para el flujo e intercambio de la información a través de una red que conecta a la Dirección Universitaria de Admisión, Dirección Universitaria de Asuntos Académicos, los Departamentos Académicos, las Oficinas de Procesos Académicos, las Direcciones de Escuelas y las Oficina de Grados y Títulos. Así mismo permiten el acceso a través de internet a catedráticos, personal administrativo y alumnos.

El problema que se presenta es la falta de la elaboración e implementación de un plan de contingencia y mitigación actualizado, que nos detalle los riegos que están expuestos los servidores de los sistemas y las medidas que se puedan adoptar, en el centro de administración de los servidores. Por lo cual cada vez que se presenta dificultades en la conexión entre los servidores y los sistemas ya sea por conflictos en las redes o en el servicio eléctrico, se tarda un tiempo considerable en la solución a dichos problemas.

Ante la ausencia de la identificación de los riesgos que presentan los servidores y por lo consiguiente desconocer las medidas que podría adaptarse, hace que todo dependa del esfuerzo particular de los administradores encargados.

Por lo cual se plantean las siguientes interrogantes ¿Están bien implementados los servidores y la red de los sistemas de gestión académica?, ¿Qué grado de confiabilidad y seguridad se le brindan a los datos que fluyen a través de la red de los servidores de los sistemas de gestión académica?

2.2 Formulación del Problema

¿La aplicación de la metodología MAGERIT para el Análisis y Gestión de Riesgos en los Servidores de los Sistemas de Gestión Académica de la Universidad Nacional Pedro Ruiz Gallo, ayudara a identificar los riesgos que presentan los servidores, y definir las medidas que deben adoptarse para el control de estos riesgos?

2.3 Justificación e Importancia de la investigación

2.3.1 Justificación

2.3.1.1 Justificación Académica

Los sistemas de gestión académica cuentan con barreras de protección implementadas, las cuales no están situadas en un plan conjunto sino a base de conocimiento de seguridad de equipos tecnológicos.

Existen diversas metodologías que permiten realizar un estudio del nivel de confiabilidad y seguridad dentro de un sistema de información, entre ellas

encontramos a la metodología MAGERIT, metodología de análisis y gestión de riesgos de tecnologías de la información, la cual mediante una serie de pasos nos mostrara el estado actual de seguridad que se encuentran los servidores de los sistemas de gestión académica.

2.3.1.2 Justificación Social

Los sistemas de gestión académica, fueron desarrollados e implementados pensando en permitir a los estudiantes matricularse y acceder a sus historial académico desde la comodidad de una pc con conexión a internet. Lo cual nos conlleva a tomar en cuenta la seguridad de la información que se maneja en el proceso.

2.3.1.3 Justificación Económica

La aplicación de la metodología MAGERIT permitirá disponer de un plan de mitigación actualizado que nos detalle los riegos que están expuestos los servidores del sistema, ya que pudieran ser víctimas de agentes externos o internos generando daño en los equipos o pérdidas de información.

2.3.1.4 Justificación Tecnológica

En la actualidad la tecnología forma parte del día a día y con la automatización de procesos se va facilitando la vida al ser humano. La UNPRG no es ajena a las innovaciones tecnológicas, a través de sus sistemas de gestión académica que han tomado un papel importante en la comunidad universitaria, en lo referente a la sistematización del proceso de matrícula.

2.3.1.5 Justificación Institucional

En búsqueda de mantener una buena imagen institucional, conservando la confianza y eficacia en los procesos principales de gestión académica, como es el proceso de matrícula que rige durante toda una carrera universitaria. La UNPRG debe considerar la mitigación de riesgos presente principalmente en este proceso, para así brindar un mejor servicio.

2.3.2 Importancia

La importancia de modernizar y normalizar las políticas del plan de mitigación de riesgos, significara obtener la información acerca de los riegos que se presentan y las medidas que deben tomarse en búsqueda de mejorar la seguridad de la información reduciendo los riesgos a los están expuesto los servidores de los sistemas de gestión académica, centrándose en los servidores principales involucrados en el servicio.

De esta manera mejorar la imagen institucional, apoyando el avance tecnológico y facilitando la realización del proceso de gestión académica tanto para alumnos, como para docente.

2.4 Objetivos de la Investigación

2.4.1 Objetivo General

Identificar los riesgos que se presentan en los servidores de los sistemas de Gestión Académica de la Universidad Nacional Pedro Ruiz Gallo aplicando la metodología MAGERIT para el Análisis y Gestión de riesgos, proponiendo las medidas que deben adoptarse para el control de estos riesgos.

2.4.2 Objetivos Específicos

- Conocer y analizar el estado actual de los servidores de los sistemas de Gestión Académica.
- Desarrollar la metodología MAGERIT utilizando la herramienta PILAR aplicada a los servidores de los sistemas de Gestión Académica.
- Conocer e identificar los riesgos en los servidores de los sistemas de Gestión Académica.
- Definir un plan de mitigación frente a los riesgos identificados durante el desarrollo del presente proyecto de tesis.
- Determinar el costo que involucra aplicar la metodología MAGERIT y la herramienta PILAR en los servidores de los sistemas de Gestión Académica.

2.5 Limitaciones de la Investigación

- La aplicación de la metodología tiene como resultado un plan de seguridad o mitigación de riesgos, donde se plasmas los resultados obtenidos del análisis, sugerencias y conclusiones del proceso de gestión.
- El período de tiempo de recolección de información comprende los primeros meses del 2014 y una actualización de datos de inicios del 2015.
- Para el desarrollo de la tesis se utilizó la Herramienta Pilar en su versión de prueba, pero se consideró el costo de su versión de licencia pagada como un referente en costos para una futura implementación.

CAPITULO III:
MARCO METODOLÓGICO

CAPITULO III: MARCO METODOLÓGICO

3.1 Tipo de Investigación

Investigación Tecnológica

La Investigación Tecnología, entendida esta como una estructura de instrumentos, técnicas y procedimientos organizados con la finalidad de la descripción y producción, tanto de problemáticas tecnológicas, como de soluciones del mismo orden. Se deben construir elementos metodológicos específicos, para así producir conocimientos y soluciones inherentes a la demanda tanto de la tecnología en funcionamiento como de la nueva producción de esta.

Basándose en conceptos anteriores se define a este tipo de investigación como la mas idónea para la realización de la presente tesis.

3.2 Hipótesis

Se busca que con la aplicación de la metodología Magerit para el análisis y gestión de riesgos en los servidores de los Sistemas de Gestión Académica, y su respectiva herramienta PILAR identificar los riesgos que se presentan y se defir las medidas que deben adoptarse para mejorar la seguridad.

3.3 Variables

3.3.1 Variable Independiente

En el cuadro se hace mención a la variable independiente su definición, indicadores y los instrumentos de medición que se utilizaran para lograr el estudio.

Variable	***Definición***	***Indicadores***	***Instrumentos de medición***
Aplicación de la Metodología MAGERIT	*Aplicación de la metodología Magerit, metodología de análisis y gestión de riesgos en los servidores de los sistemas de gestión académica de la U.N.P.R.G.*	*Planificación del proyecto*	*Entrevista y cuestionarios*
		Análisis de riesgos	*Cuestionarios y observación*
		Gestión de riesgos	*Resultados y observación*

Cuadro 4: Descripción de la variable independiente

Fuente: Elaborada por el autor.

3.3.2 Variable Dependiente

En el cuadro se hace mención a la variable dependiente su definición, indicadores y los instrumentos de medición que se utilizaran para lograr el estudio.

Variable	***Definición***	***Indicadores***	***Instrumentos de medición***
Usuario	*Estudiante, catedrático o personal administrativo de la U.N.P.R.G., que tenga o necesite la información almacenada en los servidores de gestión académica.*	*Situación actual de los servidores*	*Análisis de documentos, encuestas*

Cuadro 5: Descripción de la variable dependiente

Fuente: Elaborada por el autor.

CAPITULO IV:
MARCO TEÓRICO

CAPITULO IV: MARCO TEÓRICO

4.1 Antecedentes de la Investigación

4.1.1 Antecedente 1

(Ferrero Recaséns, 2006). En su proyecto de tesis Análisis Y Gestión De Riegos Del Servicio IMAT Del Sistema De Información De I.C.A.I. plantea como principal objetivo realizar la definición concreta del sistema y la influencia que este posee sobre la organización, para ello utilizo la metodología MAGERIT (Metodología para el Análisis y Gestión de Riesgos de los Sistemas de Información), que ofrece un método estructurado y sistemático para la realización de un AGR (Análisis y Gestión de Riesgos), otra gran ventaja de aplicar Magerit es la posibilidad que permite usar una herramienta informática diseñada específicamente para Magerit. Esta herramienta, EAR, que facilita el análisis. Al momento de obtener la información necesaria estudio y planteo los objetivos y estrategias que se puedan adoptar para la seguridad del sistema de TI. Durante el desarrollo del proyecto el autor resalto la importancia del funcionamiento y la seguridad de los sistemas de información en las organizaciones. El resultado del proyecto de tesis fue un informe de mitigación de riesgos en el cual plasma el estado actual que se encuentra el sistema y las mejoras que se puedan realizar referentes al sistema y a la seguridad del mismo.

4.1.2 Antecedente 2

(Marquina Llivisaca, 2010). En su proyecto de tesis Análisis Y Gestión De Riesgos Para El Servidor RADIUS Del Laboratorio De La Facultad De Ingeniería De Sistemas, presenta como uno de los objetivos primordiales la importancia que tiene la seguridad de un servidor que almacena información y permite la comunicación en el laboratorio de la facultad de ingeniería de sistemas. Utilizo la metodología Magerit y su herramienta PILAR, que le proporciono un análisis y gestión de riesgos confiable y completo, que no da lugar a la improvisación, ni dependerá de la arbitrariedad del analista, apoyándose en los informes de las guías técnicas. Contiene la planificación del proyecto en base al cual se realiza el análisis y gestión de riesgos, para esto se realiza una descripción de la situación actual de servidor y de su infraestructura. A demás una descripción de la metodología Magerit y PILAR.

La planificación del proceso de análisis y gestión de riesgos, estimando el impacto que puede causar. El plan de desarrollo del plan de mitigación basado en los resultados obtenidos para buscar la mejorar de la seguridad informática.

4.1.3 Antecedente 3

(Espinosa Criollo, Roldán González, & Collaguazo Lapo, 2012). En su proyecto de tesis Centro De Gestión De Riesgos Para Monitoreo De Redes, En La Facultad De Ingeniería, Ciencias Físicas Y Matemáticas. Hacen mención que La facultad no disponía de un inventario de activos ni de la valoración de cada uno de ellos, razón por la cual fue necesario conocer los activos informáticos y su riesgo, para proteger la información, este estudio se lo realizó mediante la Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información (Magerit v2.0).

Partiendo de los resultados obtenidos en la valoración de activos, desarrollaron módulos para monitorear servidores aplicaciones, de bases de datos y dispositivos de interconexión denominada Centro de Gestión de Riesgos para Monitoreo de Redes (CGRMR), que ayudará a visualizar y conocer eventos generados en la red, detectar los posibles problemas como caídas de servicio y ataques de intrusos, para que el administrador de la red pueda tomar medidas correctivas.

4.1.4 Antecedente 4

(Gaona Vásquez, 2013). En su proyecto de tesis Aplicación de la Metodología Magerit para el Análisis y Gestión de la Seguridad de la información aplicado a la empresa Pesquera e Industrial Bravito SAC. En la ciudad de Machala. Busco la información actual de la seguridad de la información. Utilizándola la Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Durante el proceso de Análisis se permitió establecer la situación actual y real de la organización con respecto al sistema de información. Obtuvo como resultado al finalizar el proceso de análisis y gestión de riesgos acerca de la organización, y un plan de mitigación que aportara para el desarrollo, seguridad y mejora de los sistemas de información.

4.2 Desarrollo de la Temática

Diseño adaptado de los procesos principales que plantea la metodología Magerit a la estructura del presente proyecto de tesis. Del cual se distribuye de una manera distinta, el proceso 1 se encuentra plasmado en los primeros capítulos del proyecto de tesis, los procesos 2 y 3 se desarrollaron en el capítulo de aplicación de la metodología y plan de mitigación.

4.2.1 Planificación

- ✓ Datos generales de la organización
- ✓ Problemática de la investigación
- ✓ Marco metodológico
- ✓ Marco teórico

4.2.2 Método de análisis de riesgos

4.2.2.1 Caracterización de los activos

- ✓ Identificación de los activos
- ✓ Dependencias entre activos
- ✓ Valoración de los activos

4.2.2.2 Caracterización de las amenazas

- ✓ Identificación de las amenazas
- ✓ Valoración de las amenazas

4.2.2.3 Caracterización de las salvaguardas

- ✓ Identificación de las salvaguardas pertinentes
- ✓ Valoración de las salvaguardas

4.2.2.4 Estimación del estado de riesgo

- ✓ Estimación del impacto
- ✓ Estimación del riesgo

4.2.3 Proceso de Gestión de Riesgos

- ✓ Toma de decisiones
- ✓ Plan de Mitigación

4.3 Metodología MAGERIT V3.0

4.3.1 Introducción

MAGERIT es la metodología de análisis y gestión de riesgos de los Sistemas de Información elaborada por el Consejo Superior de Administración Electrónica (CSAE), Ministerio De Hacienda Y Administración Pública – Gobierno De España, como respuesta a la percepción de que la Administración y en general toda la sociedad, dependen de forma creciente de las tecnologías de la información para el cumplimiento de su misión.

La razón de ser de MAGERIT está directamente relacionada con la generalización del uso de las tecnologías de la información, que supone unos beneficios evidentes para los ciudadanos; pero también da lugar a ciertos riesgos que deben minimizarse con medidas de seguridad que generen confianza.

MAGERIT interesa a todos aquellos que trabajan con información digital y sistemas informáticos para tratarla. Si dicha información, o los servicios que se prestan gracias a ella, son valiosos, MAGERIT les permitirá saber cuánto valor está en juego y les ayudará a protegerlo. Conocer el riesgo al que están sometidos los elementos de trabajo es, simplemente, imprescindible para poder gestionarlos. Con MAGERIT se persigue una aproximación metódica que no deje lugar a la improvisación, ni dependa de la arbitrariedad del analista.

Siguiendo la terminología de la normativa ISO 31000, MAGERIT responde a lo que se denomina "Proceso de Gestión de los Riesgos", sección 4.4 ("Implementación de la Gestión de los Riesgos") dentro del "Marco de Gestión de Riesgos". En otras palabras, MAGERIT implementa el Proceso de Gestión de Riesgos dentro de un marco de trabajo para que los órganos de gobierno tomen decisiones teniendo en cuenta los riesgos derivados del uso de tecnologías de la información.

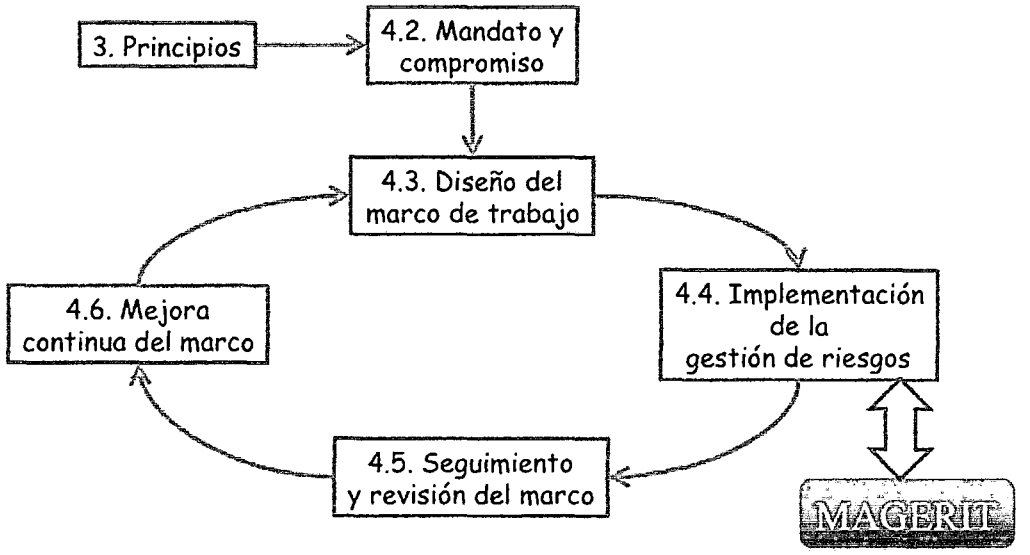

Figura 5: ISO 31000 - marco de trabajo para la gestión de riesgos
Fuente: MAGERIT – versión 3.0. Libro I: Método. Gobierno de España – Ministerio De Hacienda Y Relaciones Públicas. 2012

4.3.2 Objetivos

MAGERIT persigue los siguientes objetivos:

4.3.2.1 Directos

- ✓ Concienciar a los responsables de las organizaciones de información de la existencia de riesgos y de la necesidad de gestionarlos.
- ✓ Ofrecer un método sistemático para analizar los riesgos derivados del uso de tecnologías de la información y comunicaciones (TIC).
- ✓ Ayudar a descubrir y planificar el tratamiento oportuno para mantener los riesgos bajo control.

4.3.2.2 Indirectos

- ✓ Preparar a la Organización para procesos de evaluación, auditoría, certificación o acreditación, según corresponda en cada caso

4.3.3 Organización de las Guías

Esta versión 3 de Magerit se ha estructurado en dos libros y una guía de técnicas:

- ✓ Libro I : Método
- ✓ Libro II :Catálogo de elementos
- ✓ Guía de Técnicas: Recopilación de técnicas de diferente tipo que pueden ser de utilidad para la aplicación del método.

4.3.3.1 Libro I

Este libro se estructura de la siguiente forma:

- ✓ El capítulo 2 presenta los conceptos informalmente. En particular se enmarcan las actividades de análisis y tratamiento dentro de un proceso integral de gestión de riesgos.

- ✓ El capítulo 3 concreta los pasos y formaliza las actividades de análisis de los riesgos.
- ✓ El capítulo 4 describe opciones y criterios de tratamiento de los riesgos y formaliza las actividades de gestión de riesgos.
- ✓ El capítulo 5 se centra en los proyectos de análisis de riesgos, proyectos en los que nos ve-remos inmersos para realizar el primer análisis de riesgos de un sistema y eventualmente cuando hay cambios sustanciales y hay que rehacer el modelo ampliamente.
- ✓ El capítulo 6 formaliza las actividades de los planes de seguridad, a veces denominados planes directores o planes estratégicos.
- ✓ El capítulo 7 se centra en el desarrollo de sistemas de información y cómo el análisis de riesgos sirve para gestionar la seguridad del producto final desde su concepción inicial hasta su puesta en producción, así como a la protección del propio proceso de desarrollo.
- ✓ El capítulo 8 se anticipa a algunos problemas que aparecen recurrentemente cuando se realizan análisis de riesgos.

Los apéndices recogen material de consulta:

1. Un glosario.
2. Referencias bibliográficas consideradas para el desarrollo de esta metodología,
3. Referencias al marco legal que encuadra las tareas de análisis y gestión en la Administración Pública Española.
4. El marco normativo de evaluación y certificación.
5. Las características que se requieren de las herramientas, presentes o futuras, para soportar el proceso de análisis y gestión de riesgos.
6. Una guía comparativa de cómo Magerit versión 1 ha evolucionado a la versión 2 y a esta versión 3.

4.3.3.2 Libro II

En libro aparte, se propone un catálogo, abierto a ampliaciones, que marca unas pautas en cuanto a:

- ✓ Tipos de activos
- ✓ Dimensiones de valoración de los activos
- ✓ Criterios de valoración de los activos
- ✓ Amenazas típicas sobre los sistemas de información
- ✓ Salvaguardas a considerar para proteger sistemas de información

Se persiguen dos objetivos:

1. Por una parte, facilitar la labor de las personas que acometen el proyecto, en el sentido de ofrecerles elementos estándar a los que puedan adscribirse rápidamente, centrándose en lo específico del sistema objeto del análisis.
2. Por otra, homogeneizar los resultados de los análisis, promoviendo una terminología y unos criterios uniformes que permitan comparar e incluso integrar análisis realizados por diferentes equipos.

4.3.3.3 Guía de Técnicas

En libro aparte, aporta luz adicional y orientación sobre algunas técnicas que se emplean habitualmente para llevar a cabo proyectos de análisis y gestión de riesgos:

- Técnicas específicas para el análisis de riesgos
  - ✓ Análisis mediante tablas
  - ✓ Análisis algorítmico
  - ✓ Arboles de ataque

- Técnicas generales
  - ✓ Técnicas gráficas
  - ✓ Sesiones de trabajo: entrevistas, reuniones y presentaciones
  - ✓ Valoración Delphi Se trata de una guía de consulta.

Según el lector avance por las tareas del proyecto, se le recomendará el uso de ciertas técnicas específicas, de las que esta guía busca ser una introducción, así como proporcionar referencias para que el lector profundice en las técnicas presentadas.

4.3.4 Método de Análisis de Riesgos y Proceso de Gestión de Riesgos

4.3.4.1 Método de Análisis de Riesgos

El análisis de riesgos es una aproximación metódica para determinar el riesgo siguiendo unos pasos pautados:

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 (o expectativa de materialización) de la amenaza.

Con el objeto de organizar la presentación, se introducen los conceptos de "impacto y riesgo potenciales" entre los pasos 2 y 3. Estas valoraciones son "teóricas": en el caso de que no hubiera salvaguarda alguna desplegada. Una vez obtenido este escenario teórico, se incorporan las salvaguardas del paso 3, derivando estimaciones realistas de impacto y riesgo. La siguiente figura recoge este primer recorrido, cuyos pasos se detallan en las siguientes secciones:

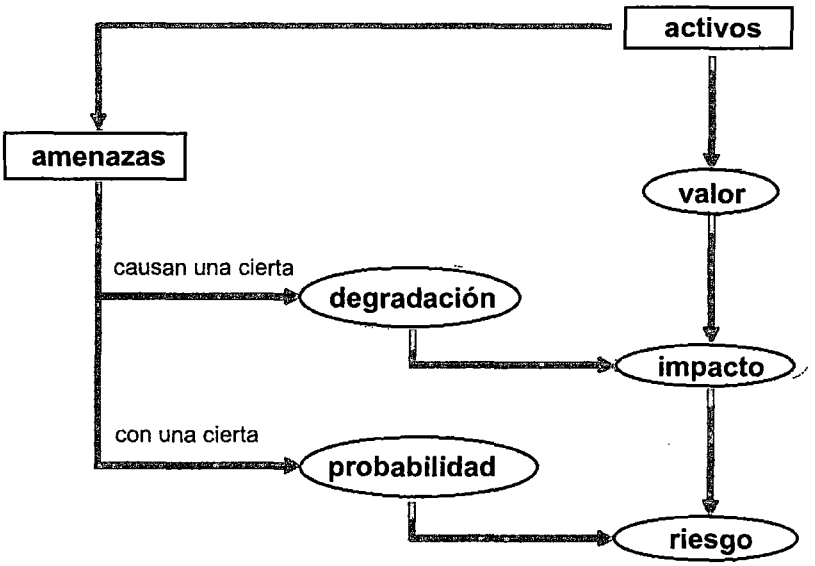

Gráfico 2: Elementos del análisis de riesgos potenciales
Fuente: MAGERIT – versión 3.0. Libro I: Método. Gobierno de España – Ministerio De Hacienda Y Relaciones Públicas. 2012

4.3.4.1.1 Paso 1: Activos

Componente o funcionalidad de un sistema de información susceptible de ser atacado accidentalmente con consecuencias para la organización, incluye:
En un sistema de información hay 2 cosas esenciales:

- ✓ La información que maneja
- ✓ Los servicios que presta.

Estos activos esenciales marcan los requisitos de seguridad para todos los demás componentes del sistema.

- ✓ Datos que materializan la información.
- ✓ Servicios auxiliares que se necesitan para poder organizar el sistema.
- ✓ Las aplicaciones informáticas *(software)* que permiten manejar los datos.
- ✓ Los equipos informáticos *(hardware)* y que permiten hospedar datos, aplicaciones y servicios.
- ✓ Los soportes de información que son dispositivos de almacenamiento de datos.
- ✓ El equipamiento auxiliar que complementa el material informático.
- ✓ Las redes de comunicaciones que permiten intercambiar datos.
- ✓ Las instalaciones que acogen equipos informáticos y de comunicaciones.
- ✓ Las personas que explotan u operan todos los elementos anteriormente citados.

Dependencias

Los activos esenciales son la información y los servicios prestados; pero estos activos dependen de otros activos más prosaicos como pueden ser los equipos, las comunicaciones, las instalaciones y las frecuentemente olvidadas personas que trabajan con aquellos.

De manera que los activos vienen a formar árboles o grafos de dependencias donde la seguridad de los activos que se encuentran más arriba en la estructura o 'superiores' depende de los activos que se encuentran más abajo o 'inferiores'. Estas estructuras reflejan de arriba hacia abajo las dependencias, mientas que de abajo hacia arriba la propagación del daño caso de materializarse las amenazas.
Aunque en cada caso hay que adaptarse a la Organización objeto del análisis, con frecuencia se puede estructurar el conjunto de activos en capas, donde las capas superiores dependen de las inferiores:

- Activos esenciales
  - Información que se maneja
  - Servicios prestados

- Servicios internos
  - Que estructuran ordenadamente el sistema de información

- El equipamiento informático
  - Aplicaciones (software)
  - Equipos informáticos (hardware)
  - Comunicaciones
  - Soportes de información: discos, cintas, etc.

- El entorno: activos que se precisan para garantizar las siguientes capas
  - Equipamiento y suministros: energía, climatización, etc.
  - Mobiliario

- Los servicios subcontratados a terceros

- Las instalaciones físicas

- El personal
  - Usuarios
  - Operadores y administradores
  - Desarrolladores

Valoración

¿Por qué interesa un activo? Por lo que vale.

No se está hablando de lo que cuestan las cosas, sino de lo que valen. Si algo no vale para nada, prescíndase de ello. Si no se puede prescindir impunemente de un activo, es que algo vale; eso es lo que hay que averiguar pues eso es lo que hay que proteger.
La valoración se puede ver desde la perspectiva de la 'necesidad de proteger' pues cuanto más valioso es un activo, mayor nivel de protección requeriremos en la dimensión (o dimensiones) de seguridad que sean pertinentes.

El valor puede ser propio, o puede ser acumulado. Se dice que los activos inferiores en un esquema de dependencias, acumulan el valor de los activos que se apoyan en ellos.

Dimensiones

De un activo puede interesar calibrar diferentes dimensiones:

- Su **confidencialidad**: ¿qué daño causaría que lo conociera quien no debe? Esta valoración es típica de datos.
- Su **integridad:** ¿qué perjuicio causaría que estuviera dañado o corrupto? Esta valoración es típica de los datos, que pueden estar manipulados, ser total o parcialmente falso o, incluso, faltar datos.
- Su **disponibilidad:** ¿qué perjuicio causaría no tenerlo o no poder utilizarlo? Esta valoración es típica de los servicios.
- La **autenticidad**: ¿qué perjuicio causaría no saber exactamente quien hace o ha hecho cada cosa?
- La **trazabilidad** del uso del servicio: ¿qué daño causaría no saber a quién se le presta tal servicio? O sea, ¿quién hace qué y cuándo?

Valoración cualitativa

Las escalas cualitativas permiten avanzar con rapidez, posicionando el valor de cada activo en un orden relativo respecto de los demás. Es frecuente plantear estas escalas como "órdenes de magnitud" y, en consecuencia, derivar estimaciones del orden de magnitud del riesgo.

La limitación de las valoraciones cualitativas es que no permiten comparar valores más allá de su orden relativo. No se pueden sumar valores.

La "Guía de Técnicas" presenta un modelo de análisis basado en valoraciones cualitativas.

Valoración cuantitativa

Las valoraciones numéricas absolutas cuestan mucho esfuerzo; pero permiten sumar valores numéricos de forma absolutamente "natural". La interpretación de las sumas no es nunca motivo de controversia.

Si la valoración es dineraria, además se pueden hacer estudios económicos comparando lo que se arriesga con lo que cuesta la solución respondiendo a las preguntas:

¿Vale la pena invertir tanto dinero en esta salvaguarda?

¿Qué conjunto de salvaguardas optimizan la inversión?

¿En qué plazo de tiempo se recupera la inversión?

¿Cuánto es razonable que cueste la prima de un seguro?

La "Guía de Técnicas" presenta un modelo de análisis basado en valoraciones cuantitativas.

Criterios de valoración

Para valorar los activos vale, teóricamente, cualquier escala de valores. A efectos prácticos es sin embargo muy importante que

- Se use una escala común para todas las dimensiones, permitiendo comparar riesgos. Se use una escala logarítmica, centrada en diferencias relativas de valor, que no en diferencias absolutas.
- Se use un criterio homogéneo que permita comparar análisis realizados por separado.

Si la valoración es económica, hay poco más que hablar: dinero. Pero frecuentemente la valoración es cualitativa, quedando a discreción del usuario; es decir, respondiendo a criterios subjetivos.

Se ha elegido una escala detallada de diez valores, dejando en valor 0 como determinante de lo que sería un valor despreciable (a efectos de riesgo). Si se realiza un análisis de riesgos de poco detalle, se puede optar por la tabla simplificada de menos niveles. Ambas escalas, detallada y simplificada se correlacionan como se indica a continuación:

Tabla 1: Escala detallada de los criterios de valoración.

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: MAGERIT – versión 3.0 Libro II: Catalogo. Gobierno de España – Ministerio de Hacienda y Relaciones Públicas 2012

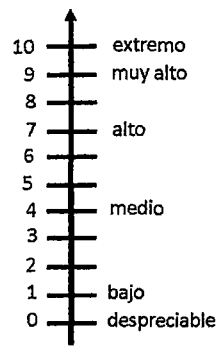

Figura 6: escala simplificada de los criterios de valoración
Fuente: MAGERIT – versión 3.0. Libro II: Catalogo. Gobierno de España – Ministerio De Hacienda Y Relaciones Públicas. 2012

El valor de la interrupción del servicio

Casi todas las dimensiones mencionadas anteriormente permiten una valoración simple, cualitativa o cuantitativa. Pero hay una excepción, la disponibilidad.

No es lo mismo interrumpir un servicio una hora o un día o un mes. Puede que una hora de detención sea irrelevante, mientras que un día sin servicio causa un daño moderado; pero un mes detenido suponga la terminación de la actividad. Y lo malo es que no existe proporcionalidad entre el tiempo de interrupción y las consecuencias.

4.3.4.1.2 Paso 2: Amenazas

El siguiente paso consiste en determinar las amenazas que pueden afectar a cada activo. Las amenazas son "cosas que ocurren". Y, de todo lo que puede ocurrir, interesa lo que puede pasarle a nuestros activos y causar un daño.

Identificación de las amenazas

El capítulo 5 del "Catálogo de Elementos" presenta una relación de amenazas típicas.

De origen natural

Hay accidentes naturales (terremotos, inundaciones).

Ante esos avatares el sistema de información es víctima pasiva, pero de todas formas tendremos en cuenta lo que puede suceder.

Del entorno (de origen industrial)

Hay desastres industriales (contaminación, fallos eléctricos) ante los cuales el sistema de información es víctima pasiva; pero no por ser pasivos hay que permanecer indefensos.

Defectos de las aplicaciones

Hay problemas que nacen directamente en el equipamiento propio por defectos en su diseño o en su implementación, con consecuencias potencialmente negativas sobre el sistema. Frecuentemente se denominan vulnerabilidades técnicas o, simplemente, 'vulnerabilidades'

Causadas por las personas de forma accidental

Las personas con acceso al sistema de información pueden ser causa de problemas no intencionados, típicamente por error o por omisión.

Causadas por las personas de forma deliberada

Las personas con acceso al sistema de información pueden ser causa de problemas intencionados: ataques deliberados; bien con ánimo de beneficiarse indebidamente, bien con ánimo de causar daños y perjuicios a los legítimos propietarios.

No todas las amenazas afectan a todos los activos, sino que hay una cierta relación entre el tipo de activo y lo que le podría ocurrir.

Valoración de las amenazas

Cuando un activo es víctima de una amenaza, no se ve afectado en todas sus dimensiones, ni en la misma cuantía.

Una vez determinado que una amenaza puede perjudicar a un activo, hay que valorar su influencia en el valor del activo, en dos sentidos:

Degradación: cuán perjudicado resultaría el [valor del] activo

Probabilidad: cuán probable o improbable es que se materialice la amenaza
La degradación mide el daño causado por un incidente en el supuesto de que ocurriera.

La degradación se suele caracterizar como una fracción del valor del activo y así aparecen expresiones como que un activo se ha visto "totalmente degradado", o "degradado en una pequeña fracción". Cuando las amenazas no son intencionales, probablemente baste conocer la fracción físicamente perjudicada de un activo para calcular la pérdida proporcional de valor que se pierde. Pero cuando la amenaza es intencional, no se puede pensar en proporcionalidad alguna pues el atacante puede causar muchísimo daño de forma selectiva.
La probabilidad de ocurrencia es más compleja de determinar y de expresar. A veces se modela cualitativamente por medio de alguna escala nominal:

Tabla 2: Degradación del valor

MA	Muy alta	Casi seguro	Fácil
A	Alta	Muy alto	Medio
M	Media	Posible	Difícil
B	Baja	Poco probable	Muy difícil
MB	Muy baja	Muy raro	Extremadamente difícil

Fuente: MAGERIT – versión 3.0. Libro I: Método. Gobierno de España – Ministerio De Hacienda Y Relaciones Públicas. 2012

A veces se modela numéricamente como una frecuencia de ocurrencia. Es habitual usar 1 año como referencia, de forma que se recurre a la tasa anual de ocurrencia como medida de la probabilidad de que algo ocurra. Son valores típicos:

Tabla 3: Probabilidad de ocurrencia

MA	100	Muy frecuente	A diario
A	10	Frecuente	Mensualmente
M	1	Normal	Una vez al año
B	1/10	Poco frecuente	Cada varias años
MB	1/100	Muy poco frecuente	Siglos

Fuente: MAGERIT – versión 3.0. Libro I: Método. Gobierno de España – Ministerio De Hacienda Y Relaciones Públicas. 2012

4.3.4.1.3 Determinación del Impacto Potencial

Se denomina impacto a la medida del daño sobre el activo derivado de la materialización de una amenaza. Conociendo el valor de los activos (en varias dimensiones) y la degradación que causan las amenazas, es directo derivar el impacto que estas tendrían sobre el sistema.
La única consideración que queda hacer es relativa a las dependencias entre activos. Es frecuente que el valor del sistema se centre en la información que maneja y los servicios que presta; pero las amenazas suelen materializarse en los medios. Para enlazar unos con otros recurriremos al grafo de dependencias.

Impacto Acumulado

Es el calculado sobre un activo teniendo en cuenta

- Su valor acumulado (el propio mas el acumulado de los activos que dependen de él)
- Las amenazas a que está expuesto

El impacto acumulado se calcula para cada activo, por cada amenaza y en cada dimensión de valoración, siendo una función del valor acumulado y de la degradación causada.

El impacto es tanto mayor cuanto mayor es el valor propio o acumulado sobre un activo.

El impacto es tanto mayor cuanto mayor sea la degradación del activo atacado.

El impacto acumulado, al calcularse sobre los activos que soportan el peso del sistema de información, permite determinar las salvaguardas de que hay que dotar a los medios de trabajo: protección de los equipos, copias de respaldo, etc.

Impacto Repercutido

Es el calculado sobre un activo teniendo en cuenta

- Su valor propio
- Las amenazas a que están expuestos los activos de los que depende

El impacto repercutido se calcula para cada activo, por cada amenaza y en cada dimensión de valoración, siendo una función del valor propio y de la degradación causada.

El impacto es tanto mayor cuanto mayor es el valor propio de un activo.

El impacto es tanto mayor cuanto mayor sea la degradación del activo atacado.

El impacto es tanto mayor cuanto mayor sea la dependencia del activo atacado.

El impacto repercutido, al calcularse sobre los activos que tienen valor propio, permite determinar las consecuencias de las incidencias técnicas sobre la misión del sistema de información. Es pues una presentación gerencial que ayuda a tomar una de las decisiones críticas de un análisis de riesgos: aceptar un cierto nivel de riesgo.

Agregación de valores de Impacto

Los párrafos anteriores determinan el impacto que sobre un activo tendría una amenaza en una cierta dimensión. Estos impactos singulares pueden agregarse bajo ciertas condiciones:

- Puede agregarse el impacto repercutido sobre diferentes activos,
- Puede agregarse el impacto acumulado sobre activos que no sean dependientes entre sí, y no hereden valor de un activo superior común,
- No debe agregarse el impacto acumulado sobre activos que no sean independientes, pues ello supondría sobre ponderar el impacto al incluir varias veces el valor acumulado de activos superiores,
- Puede agregarse el impacto de diferentes amenazas sobre un mismo activo, aunque con-viene considerar en qué medida las diferentes amenazas son independientes y pueden ser concurrentes,
- Puede agregarse el impacto de una amenaza en diferentes dimensiones.

4.3.4.1.4 Determinación del Riesgo Potencial

Se denomina riesgo a la medida del daño probable sobre un sistema. Conociendo el impacto de las amenazas sobre los activos, es directo derivar el riesgo sin más que tener en cuenta la probabilidad de ocurrencia. El riesgo crece con el impacto y con la probabilidad, pudiendo distinguirse una serie de zonas a tener en cuenta en el tratamiento del riesgo (que veremos más adelante):

- Zona 1 – riesgos muy probables y de muy alto impacto
- Zona 2 – franja amarilla: cubre un amplio rango desde situaciones improbables y de impacto medio, hasta situaciones muy probables pero de impacto bajo o muy bajo.
- Zona 3 – riesgos improbables y de bajo impacto.
- Zona 4 – riesgos improbables pero de muy alto impacto

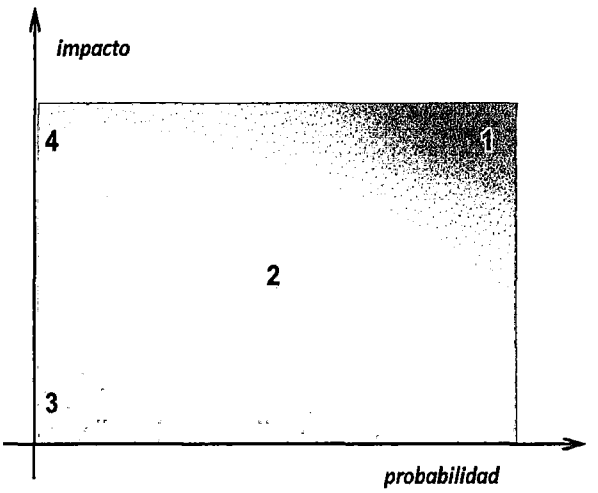

Gráfico 3: El riesgo en función del impacto y la probabilidad
Fuente: MAGERIT – versión 3.0. Libro I: Método. Gobierno de España – Ministerio De Hacienda Y Relaciones Públicas. 2012

Riesgo Acumulado

Es el calculado sobre un activo teniendo en cuenta

- El impacto acumulado sobre un activo debido a una amenaza y
- La probabilidad de la amenaza

El riesgo acumulado se calcula para cada activo, por cada amenaza y en cada dimensión de valoración, siendo una función del valor acumulado, la degradación causada y la probabilidad de la amenaza.

El riesgo acumulado, al calcularse sobre los activos que soportan el peso del sistema de información, permite determinar las salvaguardas de que hay que dotar a los medios de trabajo: protección de los equipos, copias de respaldo, etc.

Riesgo Repercutido

Es el calculado sobre un activo teniendo en cuenta

- El impacto repercutido sobre un activo debido a una amenaza y
- La probabilidad de la amenaza

El riesgo repercutido se calcula para cada activo, por cada amenaza y en cada dimensión de valoración, siendo una función del valor propio, la degradación causada y la probabilidad de la amenaza.
El riesgo repercutido, al calcularse sobre los activos que tienen valor propio, permite determinar las consecuencias de las incidencias técnicas sobre la misión del sistema de información. Es pues una presentación gerencial que ayuda a tomar una de las decisiones críticas de un análisis de riesgos: aceptar un cierto nivel de riesgo.

Agregación de Riesgos

Los párrafos anteriores determinan el riesgo que sobre un activo tendría una amenaza en una cierta dimensión. Estos riesgos singulares pueden agregarse bajo ciertas condiciones:

- Puede agregarse el riesgo repercutido sobre diferentes activos.
- Puede agregarse el impacto acumulado sobre activos que no sean dependientes entre sí, y no hereden valor de un activo superior común.
- No debe agregarse el riesgo acumulado sobre activos que no sean independientes, pues ello supondría sobre ponderar el riesgo al incluir varias veces el valor acumulado de activos superiores.
- Puede agregarse el riesgo de diferentes amenazas sobre un mismo activo, aunque conviene considerar en qué medida las diferentes amenazas son independientes y pueden ser concurrentes.
- Puede agregarse el riesgo de una amenaza en diferentes dimensiones.

4.3.4.1.5 Paso 3: Salvaguardas

En los pasos anteriores no se han tomado en consideración las salvaguardas desplegadas. Se miden, por tanto, los impactos y riesgos a que estarían expuestos los activos si no se protegieran en absoluto. En la práctica no es frecuente encontrar sistemas desprotegidos: las medidas citadas indican lo que ocurriría si se retiraran las salvaguardas presentes. Se definen las salvaguardas o contra medidas como aquellos procedimientos o mecanismos tecnológicos que reducen el riesgo. Hay amenazas que se conjurar simplemente organizándose adecuadamente, otras requieres elementos técnicos (programas o equipos), otra seguridad física y, por último, está la política de personal. El capítulo 6 del "Catálogo de Elementos" presenta una relación de salvaguardas adecuadas para cada tipo de activos.

Selección de Salvaguardas

Ante el amplio abanico de posibles salvaguardas a considerar, es necesario hacer una criba inicial para quedarnos con aquellas que son relevantes para lo que hay que proteger. En esta criba se deben tener en cuenta los siguientes aspectos:

1. Tipo de activos a proteger, pues cada tipo se protege de una forma específica
2. Dimensión o dimensiones de seguridad que requieren protección
3. Amenazas de las que necesitamos protegernos
4. Si existen salvaguardas alternativas

Además, es prudente establecer un principio de proporcionalidad y tener en cuenta:

1. El mayor o menor valor propio o acumulado sobre un activo, centrándonos en lo más valioso y obviando lo irrelevante.
2. La mayor o menor probabilidad de que una amenaza ocurra, centrándonos en los riesgos más importantes (ver zonas de riesgo).
3. La cobertura del riesgo que proporcionan salvaguardas alternativas.

Esto lleva a dos tipos de declaraciones para excluir una cierta salvaguarda del conjunto de las que conviene analizar:

- **No aplica** – se dice cuando una salvaguarda no es de aplicación porque técnicamente no es adecuada al tipo de activos a proteger, no protege la dimensión necesaria o no protege frente a la amenaza en consideración
- **No se justifica** – se dice cuando la salvaguarda aplica, pero es desproporcionada al riesgo que tenemos que proteger.

Como resultado de estas consideraciones dispondremos de una "declaración de aplicabilidad" o relación de salvaguardas que deben ser analizadas como componentes nuestro sistema de protección.

Efecto de las Salvaguardas

Las salvaguardas entran en el cálculo del riesgo de dos formas:

Reduciendo la probabilidad de las amenazas

Se llaman salvaguardas preventivas. Las ideales llegan a impedir completamente que la amenaza se materialice.

Limitando el daño causado

Hay salvaguardas que directamente limitan la posible degradación, mientras que otras permiten detectar inmediatamente el ataque para frenar que la degradación avance. Incluso algunas salvaguardas se limitan a permitir la pronta recuperación del sistema cuando la amenaza lo destruye. En cualquiera de las versiones, la amenaza se materializa; pero las con-secuencias se limitan

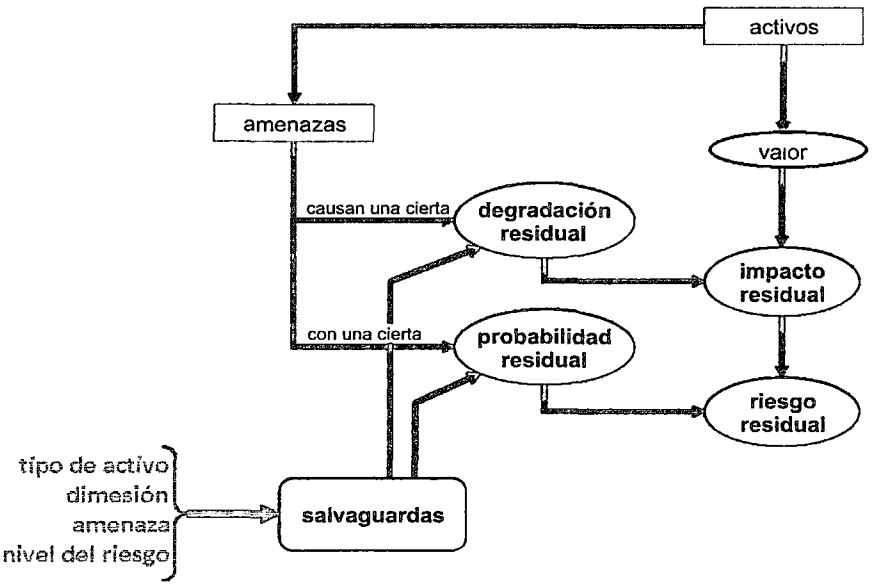

Gráfico 4: Elementos de análisis del riesgo residual
Fuente: MAGERIT – versión 3.0. Libro I: Método. Gobierno de España – Ministerio De Hacienda Y Relaciones Públicas. 2012

Tipo de Protección

Esta aproximación a veces resulta un poco simplificadora, pues es habitual hablar de diferentes tipos de protección prestados por las salvaguardas:

[PR] Prevención

Diremos que una salvaguarda es preventiva cuando reduce las oportunidades de que un incidente ocurra. Si la salvaguarda falla y el incidente llega a ocurrir, los daños son los mismos. Ejemplos: autorización previa de los usuarios, gestión de privilegios, planificación de capacidades, metodología segura de desarrollo de software, pruebas en pre-producción, segregación de tareas.

[DR] Disuasión

Diremos que una salvaguarda es disuasoria cuando tiene un efecto tal sobre los atacantes que estos no se atreven o se lo piensan dos veces antes de atacar. Son salvaguardas que actúan antes del incidente, reduciendo las probabilidades de que ocurra; pero que no tienen influencia sobre los daños causados caso de que el atacante realmente se atreva. Ejemplos: vallas elevadas, guardias de seguridad, avisos sobre la persecución del delito o persecución del delincuente.

[EL] Eliminación

Diremos que una salvaguarda elimina un incidente cuando impide que éste tenga lugar. Son salvaguardas que actúan antes de que el incidente se haya producido. No reducen los daños caso de que la salvaguarda no sea perfecta y el incidente llegue a ocurrir.

Ejemplos: eliminación de cuentas estándar, de cuentas sin contraseña, de servicios innecesarios; en general, todo lo que tenga que ver con la fortificación o bastionado, cifrado de la información, armarios ignífugos.

[IM] Minimización del impacto / Limitación del impacto

Se dice que una salvaguarda minimiza o limita el impacto cuando acota las consecuencias de un incidente. Ejemplos: desconexión de redes o equipos en caso de ataque, detención de servicios en caso de ataque, seguros de cobertura, cumplimiento de la legislación vigente.

[CR] Corrección

Diremos que una salvaguarda es correctiva cuando, habiéndose producido un daño, lo re-para. Son salvaguardas que actúan después de que el incidente se haya producido y por tanto reducen los daños.

Véase: recuperación más abajo. Ejemplos: gestión de incidentes, líneas de comunicación alternativas, fuentes de alimentación redundantes.

[RC] Recuperación

Diremos que una salvaguarda ofrece recuperación cuando permite regresar al estado anterior al incidente. Son salvaguardas que no reducen las probabilidades del incidente, pero acotan los daños a un periodo de tiempo.

Ejemplos: copias de seguridad (back-up).

[MN] Monitorización

Son las salvaguardas que trabajan monitorizando lo que está ocurriendo o lo que ha ocurrido. Si se detectan cosas en tiempo real, podemos reaccionar atajando el incidente para limitar el impacto; si se detectan cosas a posteriori, podemos aprender del incidente y mejorar el sistema de salvaguardas de cara al futuro.

Ejemplos: registros de actividad, registro de descargas de web.

[DC] Detección

Diremos que una salvaguarda funciona detectando un ataque cuando informa de que el ataque está ocurriendo. Aunque no impide el ataque, sí permite que entren en operación otras medidas que atajen la progresión del ataque, minimizando daños. Ejemplos: anti-virus, IDS, detectores de incendio.

[AW] Concienciación

Son las actividades de formación de las personas anexas al sistema que pueden tener una influencia sobre él. La formación reduce los errores de los usuarios, lo cual tiene un efecto preventivo. También mejora las salvaguardas de todo tipo pues los que las operan lo hacen con eficacia y rapidez, potenciando su efecto o, al menos, no menoscabándolo por una mala operación. Ejemplos: cursos de concienciación, cursos de formación.

[AD] Administración

Se refiere a las salvaguardas relacionadas con los componentes de seguridad del sistema. Una buena administración evita el desconocimiento de lo que hay y por

tanto impide que haya puertas desconocidas por las que pudiera tener éxito un ataque. En general pueden considerarse medidas de tipo preventivo.

Ejemplos: inventario de activos, análisis de riesgos, plan de continuidad.

La siguiente tabla relaciona cada uno de estos tipos de protección con el modelo anterior de reducción de la degradación y de la probabilidad:

Efecto	Tipo
Preventivas: reducen la probabilidad	[PR] Preventivas
	[DR] Disuasorias
	[EL] Eliminatorias
Acotan la degradación	[IM] Minimizadoras
	[CR] Correctivas
	[RC] Recuperativas
Consolidan el efecto de las demás	[MN] De monitorización
	[DC] De detección
	[AW] De concienciación
	[AD] Administrativas

Cuadro 6: Tipos de salvaguardas

Fuente: MAGERIT – versión 3.0. Libro I: Método. Gobierno de España – Ministerio De Hacienda Y Relaciones Públicas. 2012

Eficacia de la protección

Las salvaguardas se caracterizan, además de por su existencia, por su eficacia frente al riesgo que pretenden conjurar. La salvaguarda ideal es 100% eficaz, eficacia que combina 2 factores:

Desde el punto de vista técnico

- es técnicamente idónea para enfrentarse al riesgo que protege
- se emplea siempre

Desde el punto de vista de operación de la salvaguarda

- está perfectamente desplegada, configurada y mantenida
- existen procedimientos claros de uso normal y en caso de incidencias
- los usuarios están formados y concienciados
- existen controles que avisan de posibles fallos

Entre una eficacia del 0% para aquellas que faltan y el 100% para aquellas que son idóneas y que están perfectamente implantadas, se estimará un grado de eficacia real en cada caso concreto. Para medir los aspectos organizativos, se puede emplear una escala de madurez que recoja en forma de factor corrector la confianza que merece el proceso de gestión de la salvaguarda:

Tabla 4: Eficacia y madurez de las salvaguardas

Factor	Nivel	Significado
0%	L0	Inexistente
	L1	Inicial/ad hoc
	L2	Reproducible, pero intuitivo
	L3	Proceso definido
	L4	Gestionando y medible
100%	L5	Optimizado

Fuente: MAGERIT – versión 3.0. Libro I: Método. Gobierno de España – Ministerio De Hacienda Y Relaciones Públicas. 2012

Vulnerabilidades

Se denomina vulnerabilidad a toda debilidad que puede ser aprovechada por una amenaza, o más detalladamente a las debilidades de los activos o de sus medidas de protección que facilitan el éxito de una amenaza potencial.

Traducido a los términos empleados en los párrafos anteriores, son vulnerabilidades todas las ausencias o ineficacias de las salvaguardas pertinentes para salvaguardar el valor propio o acumulado sobre un activo. A veces se emplea el término "insuficiencia" para resaltar el hecho de que la eficacia medida de la salvaguarda es insuficiente para preservar el valor del activo expuesto a una amenaza.

4.3.4.1.6 Paso 4: Impacto Residual

Dado un cierto conjunto de salvaguardas desplegadas y una medida de la madurez de su proceso de gestión, el sistema queda en una situación de posible impacto que se denomina residual. Se dice que hemos modificado el impacto, desde un valor potencial a un valor residual.

El cálculo del impacto residual es sencillo. Como no han cambiado los activos, ni sus dependencias, sino solamente la magnitud de la degradación, se repiten los cálculos de impacto con este nuevo nivel de degradación.

La magnitud de la degradación tomando en cuenta la eficacia de las salvaguardas, es la proporción que resta entre la eficacia perfecta y la eficacia real.

El impacto residual puede calcularse acumulado sobre los activos inferiores, o repercutido sobre los activos superiores.

4.3.4.1.7 Paso 5: Riesgo Residual

Dado un cierto conjunto de salvaguardas desplegadas y una medida de la madurez de su proceso de gestión, el sistema queda en una situación de riesgo que se denomina residual. Se dice que hemos modificado el riesgo, desde un valor potencial a un valor residual. El cálculo del riesgo residual es sencillo. Como no han cambiado los activos, ni sus dependencias, sino solamente la magnitud de la degradación y la probabilidad de las amenazas, se repiten los cálculos de riesgo usando el impacto residual y la probabilidad residual de ocurrencia.

La magnitud de la degradación se toma en consideración en el cálculo del impacto residual. La magnitud de la probabilidad residual tomando en cuenta la eficacia de las salvaguardas, es la proporción que resta entre la eficacia perfecta y la eficacia real. El riesgo residual puede calcularse acumulado sobre los activos inferiores, o repercutido sobre los activos superiores.

4.3.4.1.8 Documentación

Documentación intermedia

- Resultados de las entrevistas.
- Documentación de otras fuentes: estadísticas, observaciones de expertos y observaciones de los analistas.
- Información existente utilizable por el proyecto.
- Documentación auxiliar: planos, organigramas, requisitos, especificaciones, análisis funcionales, cuadernos de carga, manuales de usuario, manuales de explotación, diagramas de flujo de información y de procesos, modelos de datos, etc.
- Informes y evaluaciones de defectos de los productos, procedentes de fabricantes o de centros de respuesta a incidentes de seguridad (CERTs).

Documentación final

- **Modelo de valor**
  Informe que detalla los activos, sus dependencias, las dimensiones en las que son valiosos y la estimación de su valor en cada dimensión.
- **Mapa de riesgos:**
  Informe que detalla las amenazas significativas sobre cada activo, caracterizándolas por su frecuencia de ocurrencia y por la degradación que causaría su materialización sobre el activo.
- **Declaración de aplicabilidad:**
  Informe que recoge las contramedidas que se consideran apropiadas para defender el sistema de información bajo estudio.
- **Evaluación de salvaguardas:**
  Informe que detalla las salvaguardas existentes calificándolas en su eficacia para reducir el riesgo que afrontan.
- **Informe de insuficiencias o vulnerabilidades:**
  Informe que detalla las salvaguardas necesarias pero ausentes o insuficientemente eficaces.
- **Estado de riesgo:**
  Informe que detalla para cada activo el impacto y el riesgo, potenciales y residuales, frente a cada amenaza.

4.3.4.2 Proceso de Gestión de Riesgos

A la vista de los impactos y riesgos a que está expuesto el sistema, hay que tomar una serie de decisiones condicionadas por diversos factores:

- La gravedad del impacto y/o del riesgo.

- Las obligaciones a las que por ley esté sometida la Organización.
- Las obligaciones a las que por reglamentos sectoriales esté sometida la Organización.
- Las obligaciones a las que por contrato esté sometida la Organización.

Dentro del margen de maniobra que permita este marco, pueden aparecer consideraciones adicionales sobre la capacidad de la Organización para aceptar ciertos impactos de naturaleza intangible tales como:

- Imagen pública de cara a la Sociedad (aspectos reputacionales)
- Política interna: relaciones con los propios empleados, tales como capacidad de contratar al personal idóneo, capacidad de retener a los mejores, capacidad de soportar rotaciones de personas, capacidad de ofrecer una carrera profesional atractiva, etc.
- Relaciones con los proveedores, tales como capacidad de llegar a acuerdos ventajosos a corto, medio o largo plazo, capacidad de obtener trato prioritario, etc.
- Relaciones con los clientes o usuarios, tales como capacidad de retención, capacidad de incrementar la oferta, capacidad de diferenciarse frente a la competencia, ...
- Relaciones con otras organizaciones, tales como capacidad de alcanzar acuerdos estratégicos, alianzas, etc.
- Nuevas oportunidades de negocio, tales como formas de recuperar la inversión en seguridad
- Acceso a sellos o calificaciones reconocidas de seguridad

Todas las consideraciones anteriores desembocan en una calificación de cada riesgo significativo, determinándose si.

1. Es **crítico** en el sentido de que requiere atención urgente.
2. Es **grave** en el sentido de que requiere atención.
3. Es **apreciable** en el sentido de que pueda ser objeto de estudio para su tratamiento.
4. Es **asumible** en el sentido de que no se van a tomar acciones para atajarlo.

La opción 4, aceptación del riesgo, siempre es arriesgada y hay que tomarla con prudencia y justificación. Las razones que pueden llevar a esta aceptación son:

- Cuando el impacto residual es asumible.
- Cuando el riesgo residual es asumible.
- Cuando el coste de las salvaguardas oportunas es desproporcionado en comparación al impacto y riesgo residuales.

La calificación de los riesgos tendrá consecuencias en las tareas subsiguientes, siendo un factor básico para establecer la prioridad relativa de las diferentes actuaciones.

El análisis de riesgos determina impactos y riesgos. Los impactos recogen daños absolutos, independientemente de que sea más o menos probable que se dé la circunstancia. En cambio, el riesgo pondera la probabilidad de que ocurra. El impacto refleja el daño posible (lo peor que puede ocurrir), mientras que el riesgo refleja el daño probable (lo que probablemente ocurra). El resultado del análisis es sólo un

análisis. A partir de el disponemos de información para tomar decisiones conociendo lo que queremos proteger (activos valorados=, de qué lo queremos proteger (amenazas valoradas) y qué hemos hecho por protegerlo (salvaguardas valoradas). Todo ello sintetizado en los valores de impacto y riesgo. A partir de aquí, las decisiones son de los órganos de gobierno de la Organización que actuarán en 2 pasos:

- Paso 1: Evaluación
- Paso 2: Tratamiento

El siguiente grafico resume las posibles decisiones que se pueden tomar tras haber estudiado los riesgos. La caja 'estudio de los riesgos' pretende combinar el análisis con la evaluación.

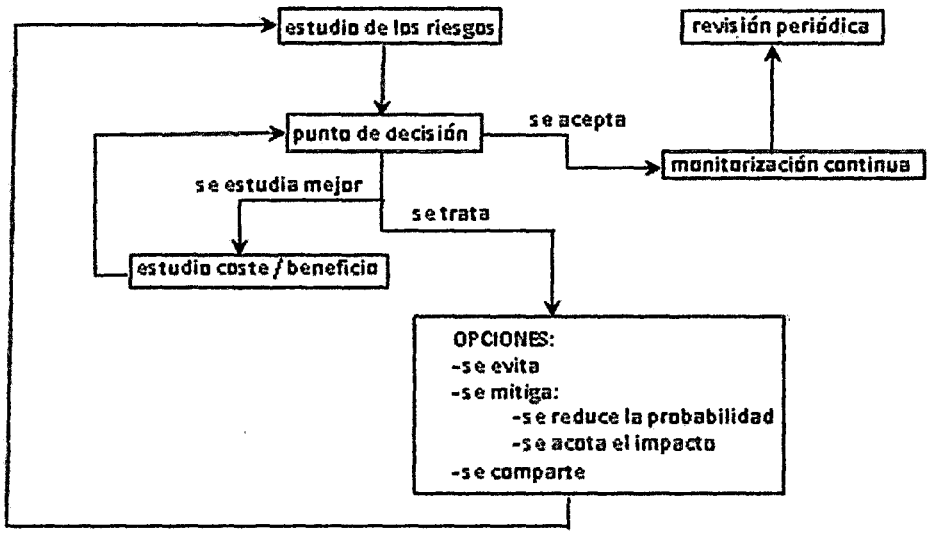

Gráfico 5: Decisiones de tratamiento de los riesgos
Fuente: MAGERIT – versión 3.0. Libro I: Método. Gobierno de España – Ministerio De Hacienda Y Relaciones Públicas. 2012

4.3.4.2.1 Evaluación: Interpretación de los valores de impacto y riesgo residuales

Impacto y riesgo residual son una medida del estado presente, entre la inseguridad potencial (sin salvaguarda alguna) y las medidas adecuadas que reducen impacto y riesgo a valores aceptables. Los párrafos siguientes se refieren conjuntamente a impacto y riesgo. Si el valor residual es igual al valor potencial, las salvaguardas existentes no valen para nada, típicamente no porque no haya nada hecho, sino porque hay elementos fundamentales sin hacer. Es importante entender que un valor residual es sólo un número. Para su correcta interpretación debe venir acompañado de la relación de lo que se debería hacer y no se ha hecho; es decir, de las vulnerabilidades que presenta el sistema. Los responsables de la toma de decisiones deberán prestar cuidadosa atención a esta relación de tareas pendientes, que se denomina **Informe de Insuficiencias o de vulnerabilidades.**

4.3.4.2.2 Aceptación del riesgo

La Dirección de la Organización sometida al análisis de riesgos debe determinar el nivel de impacto y riesgo aceptable. Más propiamente dicho, debe aceptar la responsabilidad de las insuficiencias. Esta decisión no es técnica. Puede ser una

decisión política o gerencial o puede venir determinada por ley o por compromisos contractuales con proveedores o usuarios. Estos niveles de aceptación se pueden establecer por activo o por agregación de activos (en un determinado departamento, en un determinado servicio, en una determinada dimensión.)

4.3.4.2.3 Tratamiento

La Dirección puede decidir aplicar algún tratamiento al sistema de seguridad desplegado para proteger el sistema de información. Hay dos grandes opciones: •

- Reducir el riesgo residual (aceptar un menor riesgo).
- Ampliar el riesgo residual (aceptar un mayor riesgo).

Para tomar una u otra decisión hay que enmarcar los riesgos soportados por el sistema de información dentro de un contexto más amplio que cubre un amplio espectro de consideraciones de las que podemos apuntar algunas sin pretender ser exhaustivos:

- Cumplimiento de obligaciones; sean legales, regulación pública o sectorial, compromisos in-ternos, misión de la Organización, responsabilidad corporativa, etc.
- Posibles beneficios derivados de una actividad que en sí entraña riesgos condicionantes técnicos, económicos, culturales, políticos, etc.
- Equilibrio con otros tipos de riesgos: comerciales, financieros, regulatorios, medioambientales, laborales,...

En condiciones de riesgo residual extremo, casi la única opción es reducir el riesgo. En condiciones de riesgo residual aceptable, podemos optar entre aceptar el nivel actual o ampliar el riesgo asumido. En cualquier caso hay que mantener una monitorización continua de las circunstancias para que el riesgo formal cuadre con la experiencia real y reaccionemos ante cualquier desviación significativa.

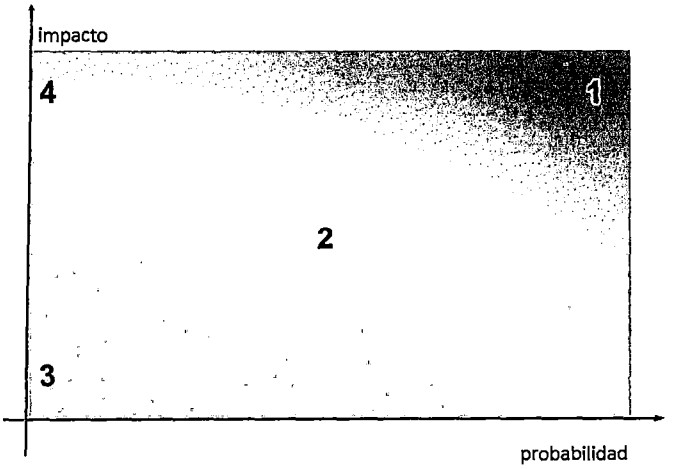

Gráfico 6: Zonas de riesgo
Fuente: MAGERIT – versión 3.0. Libro I: Método. Gobierno de España – Ministerio De Hacienda Y Relaciones Públicas. 2012

4.3.4.2.4 Opciones de Tratamiento del Riesgo: Eliminación

La eliminación de la fuente de riesgo es una opción frente a un riesgo que no es aceptable. En un sistema podemos eliminar varias cosas, siempre que no afecten a la

esencia de la Organización. Es extremadamente raro que podamos prescindir de la información o los servicios esenciales por cuanto constituyen la misión de la Organización. Cambiar estos activos supone reorientar la misión de la Organización.
Más viable es prescindir de otros componentes no esenciales, que están presentes simple y llanamente para implementar la misión, pero no son parte constituyente de la misma. Esta opción puede tomar diferentes formas:

- Eliminar cierto tipo de activos, emplean otros en su lugar. Por ejemplo: cambiar de sistema operativo, de fabricante de equipos,...
- Reordenar la arquitectura del sistema (el esquema de dependencias en nuestra terminología) de forma que alteremos el valor acumulado en ciertos activos expuestos a grandes amenazas. Por ejemplo: segregar redes, desdoblar equipos para atender a necesidades concretas, alejando lo más valioso de lo más expuesto.

Las decisiones de eliminación de las fuentes de riesgo suponen realizar un nuevo análisis de riesgos sobre el sistema modificado.

4.3.4.2.5 Opciones de Tratamiento del Riesgo: Mitigación

La mitigación del riesgo se refiere a una de dos opciones:

- Reducir la degradación causada por una amenaza (a veces se usa la expresión 'acotar el impacto')
- Reducir la probabilidad de que una amenaza de materializa

En ambos casos lo que hay que hacer es ampliar o mejorar el conjunto de salvaguardas. En términos de madurez de las salvaguardas: subir de nivel.

4.3.4.2.6 Opciones de Tratamiento del Riesgo: Compartición

Tradicionalmente se ha hablado de 'transferir el riesgo'. Como la transferencia puede ser parcial o total, es más general hablar de 'compartir el riesgo'. Hay dos formas básicas de compartir riesgo:

- Riesgo cualitativo: se comparte por medio de la externalización de componentes del sistema, de forma que se reparten responsabilidades: unas técnicas para el que opera el componen-te técnico; y otras legales según el acuerdo que se establezca de prestación del servicio.
- Riesgo cuantitativo: se comparte por medio de la contratación de seguros, de forma que a cambio de una prima, el tomador reduce el impacto de las posibles amenazas y el asegurador corre con las consecuencias. Hay multitud de tipos y cláusulas de seguros para concretar el grado de responsabilidad de cada una de las partes.

Cuando se comparten riesgos cambia, bien el conjunto de componentes del sistema, bien su valoración, requiriéndose un nuevo análisis del sistema resultante.

4.3.4.2.7 Opciones de Tratamiento del Riesgo: Financiación

Cuando se acepta un riesgo, la Organización hará bien en reservar fondos para el caso de que el riesgo se concrete y haya que responder de sus consecuencias. A

veces de habla de 'fondos de contingencia' y también puede ser parte de los contratos de aseguramiento. Normalmente esta opción no modifica nada del sistema y nos vale el análisis de riesgos disponible.

4.3.4.2.8 Documentación del proceso

Documentación interna

- Definición de roles, funciones y esquemas de reporte
- Criterios de valoración de la información
- Criterios de valoración de los servicios
- Criterios de evaluación de los escenarios de impacto y riesgo

Documentación para otros

- Plan de Seguridad

4.3.5 Plan de seguridad

Esta sección trata de cómo llevar a cabo planes de seguridad, entendiendo por tales proyectos para materializar las decisiones adoptadas para el tratamiento de los riesgos.

Estos planes reciben diferentes nombres en diferentes contextos y circunstancias:

- Plan de mejora de la seguridad
- Plan director de seguridad
- Plan estratégico de seguridad
- Plan de adecuación (en concreto es el nombre que se usa en el ENS)

Se identifican 3 tareas:

Ps – Plan De Seguridad

PS.1 – Identificación de proyectos de seguridad

PS.2 – Plan de ejecución

PS.3 – Ejecución

Cuadro 7: Plan de seguridad
Fuente: MAGERIT – versión 3.0. Libro I: Método. Gobierno de España – Ministerio De Hacienda Y Relaciones Públicas. 2012

4.4 Herramienta Pilar 5.4.5

Procedimiento Informático Lógico de Análisis de Riesgos, PILAR, es una aplicación implementada en java basada en la metodología MAGERIT, desarrollada por el Centro Criptológico Nacional y con un gran calado en la administración pública española. La versión vigente es la 5.4.5. Su licencia de prueba es de 30 días, no obstante para uso en entorno privado dicha licencia tiene un coste.

La herramienta permite la realización de análisis de riesgos bajo un enfoque tanto cualitativo como cuantitativo (empleando valores simbólicos o económicos respectivamente) y la realización de análisis de impacto en el ámbito de la continuidad de negocio.

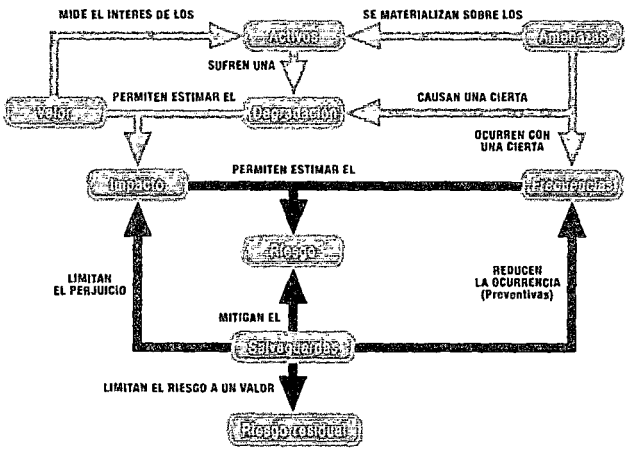

Gráfico 7: Diagrama de los proceso de análisis y gestión de riesgos
Fuente: recogida de la página web: https://www.ccn-cert.cni.es/publico/herramientas/pilar-5.3.1/ - EAR / PILAR - Entorno de Análisis de Riesgos.

4.4.1 Análisis y Gestión de riesgos

Se analizan los riesgos en varias dimensiones:

- Confidencialidad
- Integridad
- Disponibilidad
- autenticidad
- trazabilidad

Para tratar el riesgo se proponen:

- salvaguardas (o contramedidas)
- normas de seguridad
- procedimientos de seguridad

Analizándose el riesgo residual a lo largo de diversas etapas de tratamiento

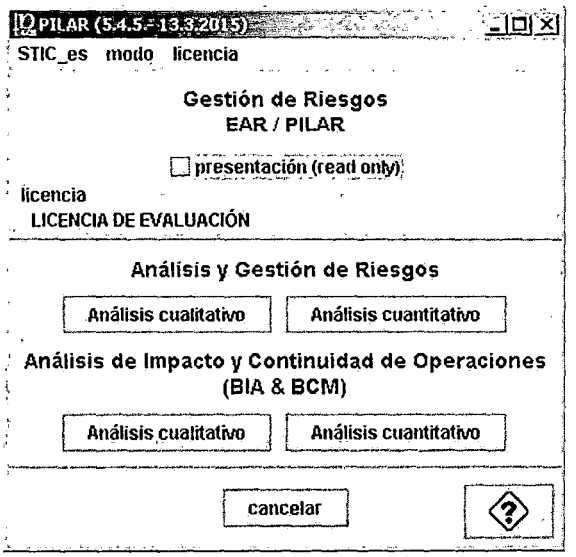

Figura 7: Herramienta Pilar - Pantalla de Principal
Fuente: Herramienta Pilar en su versión 5.4.5

4.5 Criterios de Selección de la Metodología Magerit

Para la elaboración del análisis y gestión de riesgos en los servidores, existen varias guías informales, aproximaciones metodológicas, estándares y herramientas de soporte que buscan gestionar y mitigar los riegos. Las principales metodologías de análisis y gestión de riesgos de uso habitual en el mercado de la seguridad de las tecnologías de la información son: MAGERIT, OCTAVE, CRAMM, IRAM, para determinar por qué MAGERIT es un buena elección para el desarrollo del AGR se presenta un cuadro comparativo.

		MAGERIT	OCTAVE	CRAMM	IRAM
Alcance considerado	Análisis de riesgos	SI	SI	SI	SI
	Gestión de riesgos	SI	SI	SI	SI
Tipo de análisis	Cuantitativo	SI	NO	SI	SI
	Cualitativo	SI	NO	SI	SI
	Mixto	SI	NO	NO	NO

Cuadro 8: Comparativa de Metodologías de Análisis y Gestión de Riesgos
Fuente: Elaborada por el autor basado en estudios comparativos de la metodología teniendo cono principal fuente a la Tesis: Análisis De Riesgos De Seguridad Informática, Universidad Politécnica - Madrid.

MAGERIT es la metodología recomendada para el análisis y gestión de riesgos, el cual permite realizar una evolución profunda de la seguridad de los sistemas de información.

4.6 Criterios de Selección de la Herramienta Pilar

En la selección de la herramienta para el AGR, para el presente proyecto, se tomó en cuenta el análisis comparativo de las herramientas disponibles, como se observa en el cuadro siguiente.

Herramientas	Metodología	Idiomas	Estándares
CRAMM	Evaluación de riesgos de CRAMM	Inglés, holandés, checo	ISO 27001
TOOLKIT	----------	Inglés, portugués	ISO 27000
RISICARE	MEHARI	Francés, ingles	ISO 17799,ISO 27001
ORICO	OGRCM	Español, ingles	.....
PILAR	MAGERIT	Español, ingles	ISO 2701, ISO 1540, ISP 17999,ISO 1995

Cuadro 9: Análisis Comparativo De Las Herramientas AGR.
Fuente: Elaborada por el autor basado en estudios comparativos de la metodología teniendo cono principal fuente a la Tesis: Análisis De Riesgos De Seguridad Informática, Universidad Politécnica - Madrid.

Del análisis, se selecciona la herramienta PILAR, por los siguientes motivos:

- Contiene los modelos de la madurez CMMI.
- Se basa en normas, estándares, código de buenas prácticas para la gestión de la seguridad.

Para la utilización de la herramienta PILAR, es necesario disponer de una licencia de uso, en el caso del presente proyecto se solicitó una licencia de evaluación de 30 días con el apoyo del asesor de tesis.

CAPITULO V:
DESARROLLO DEL ANÁLISIS Y GESTIÓN DE RIESGOS EN LOS SERVIDORES DE LOS SISTEMAS DE GESTIÓN ACADÉMICA – UNPRG

CAPITULO V: DESARROLLO DEL ANÁLISIS Y GESTIÓN DE RIESGOS EN LOS SERVIDORES DE LOS SISTEMAS DE GESTIÓN ACADÉMICA – UNPRG

En este capítulo se aplica la metodología Magerit mediante:

- Método de Análisis de riesgos (MAR)
- Proceso de Gestión de riesgos (PGR)

Adaptando la estructura de procesos, actividades y tareas que plantea Magerit, ya antes mencionadas en el capítulo anterior, a la estructura diseñada en la presente tesis, ya que no todas las unidades de estudio son iguales.

Teniendo en cuenta que se realiza un análisis cualitativo por que el servicio de gestión académica ofrecido no persigue ningún fin lucrativo, es decir no se recibe ningún pago por su uso, lo cual hace que el estudio no se centre en aumentar ganancias y disminuir perdidas sino en plantear mejoras en la seguridad informática de los servidores.

El desarrollo del proyecto de análisis y gestión de riesgo de los servidores de los sistemas de gestión académica, se realiza mediante la metodología Magerit y con el uso de la herramienta PILAR 5.4.5 en su versión de prueba o de evaluación. Por lo cual se muestra el desarrollo de la metodología Magerit y a la par capturas de pantallas de su ejecución usando la herramienta Pilar.

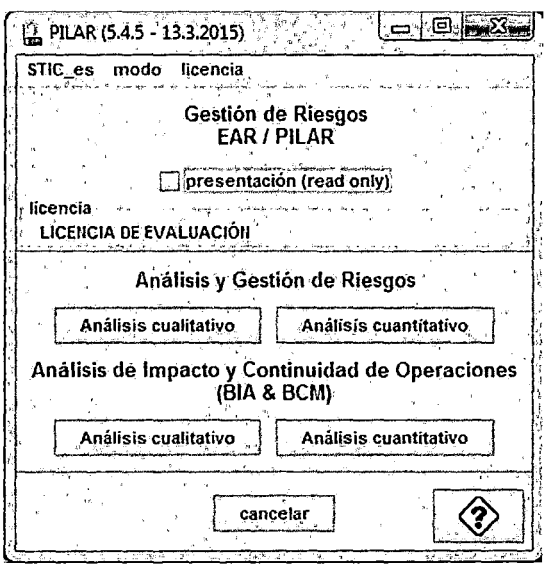

Figura 8: AGRSGA-UNPRG – Pilar 5.4.5
Fuente: Obtenido de la ejecución del Proyecto en la herramienta Pilar 5.4.5.

Datos del Proyecto

Código: AGRSGA-UNPRG

Nombre: APLICACIÓN DE MAGERIT EN LOS SERVIDORES DE LOS S.G.A. – UNPRG

Descripción: Aplicación De La Metodología Magerit Para El Análisis Y Gestión De Riesgos En Los Servidores De Los Sistemas De Gestión Académica De La Universidad Nacional Pedro Ruiz Gallo.

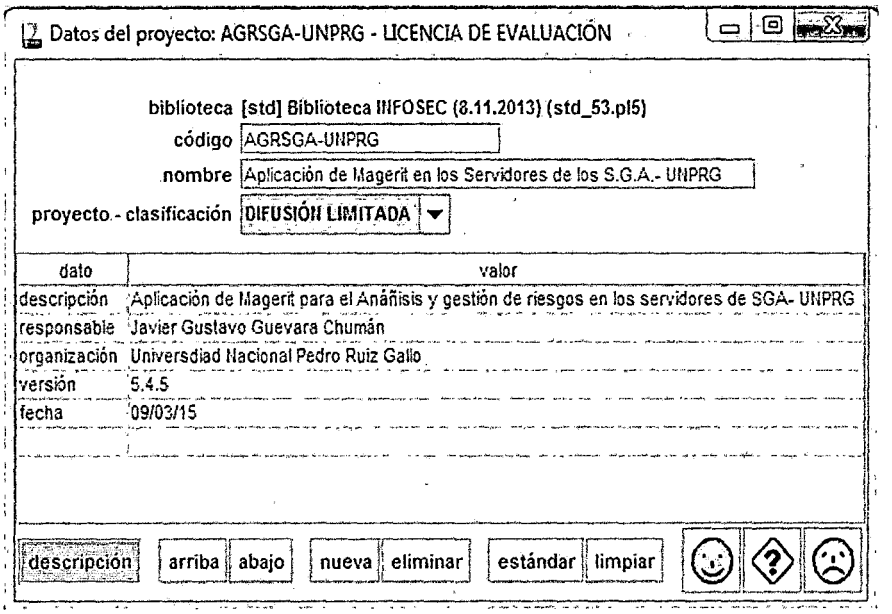

Figura 9: Datos del Proyecto AGRSGA-UNPRG – Pilar 5.4.5.
Fuente: Obtenido de la ejecución del Proyecto en la herramienta Pilar 5.4.5.

5.1 Método de Análisis de Riesgos

Para la ejecución del proceso y la aplicación correcta de la metodología Magerit, el cual tiene como objetivos principales la identificación y estimación de los activos y de las posibles amenazas que asechan a los servidores, la recolección de la información fue obtenida a través de entrevistas, cuestionarios, aplicados a los administradores del área de servidores de la red telemática- Dirección Universitaria de Informática y Sistemas-UNPRG.

Este proceso se desarrollara a través de un análisis cualitativo por lo ya expuesto.

A continuación una figura que muestra la pantalla de trabajo para el proceso de análisis de riesgos usando la herramienta Pilar 5.4.5.

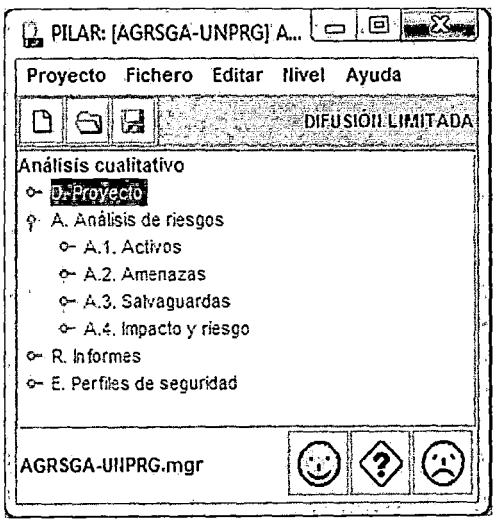

Figura 10: Análisis De Riesgos - AGRSGA-UNPRG
Fuente: Obtenido De La Ejecución Del Proyecto En La Herramienta Pilar 5.4.5.

5.1.1 MAR 1: Caracterización de los Activos

El objetivo de las tareas englobadas en esta actividad es reconocer los activos que componen los procesos y definir las dependencias entre ellos. Así mismo realizar una valoración según la importancia que tenga cada activo para el caso de estudio.

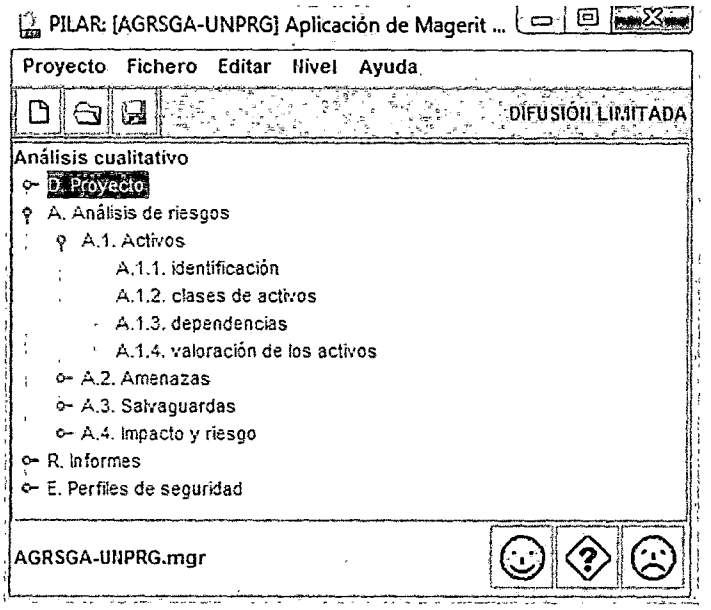

Figura 11: Caracterización de los activos - AGRSGA-UNPRG
Fuente: Obtenido De La Ejecución Del Proyecto En La Herramienta Pilar 5.4.5.

5.1.1.1 Tarea MAR 1.1: Identificación de los Activos

La tarea tiene como objetivo, identificar los activos dentro del dominio, determinando sus características y atributos del activo a tratar. Que son el código, nombre y una descripción.

Para el desarrollo de la tarea se toma en cuenta lo siguiente:

- En el caso del código se considera 4 letras que en su mayor parte son las primeras letras de las palabras que forman el nombre de cada activo.
- Para los nombres se considera la actividad principal o el software que tenían instalados que formaban parte del objeto de estudio.
- En la descripción se considera el mismo caso que en el de los nombres.

El desarrollo a través de la herramienta Pilar, basada en la metodología Magerit, facilita la organización de los activos mediante el uso de capas generales, pero para el mejor entendimiento del objeto de estudio se realiza la estructuración mediante el tipo de activos, lo cual también se permite en la herramienta Pilar.

Los activos se agrupan en 8 capas según su tipo, como son servicios, software, hardware, redes de comunicaciones, soportes de información, equipamiento auxiliar, instalaciones y personal; teniendo como eje central los servidores de los sistemas de gestión académica, la Figura 2 muestra los elementos relevantes que también se consideran durante el estudio. A continuación se realiza la identificación de los activos para el Análisis de riesgos en los servidores de los sistemas de gestión académica de la universidad Nacional Pedro Ruiz Gallo.

5.1.1.1.1 [S] Servicios

[gmat] Gestión de Matricula y notas de los alumnos - UNPRG

El servicio de gestión de matrícula, contiene desde la programación de los cursos, horarios y docente; hasta la matricula por ciclo de los alumnos.

El servicio de gestión de notas, abarca los calificativos de cada asignatura matriculada por cada alumno al final del ciclo y la posibilidad de ver el historial académico y los avances que se tienen en el transcurso del tiempo con referencia a su carrera profesional.

5.1.1.1.2 [SW] Software (las aplicaciones informáticas)

[sgap] Sistema de Gestión Académica para PreGrado

Actas Virtuales, El sistema de actas virtuales, es el sistema de gestión académica para pregrado. Esta desarrollado bajo la plataforma JAVA y utiliza una base de datos elaborada en ORACLE.

[sega] Sistema de Gestión Académica

OCCA, Es la aplicación del sistema de gestión académica. Esta desarrollado bajo la plataforma visual Basic y utiliza una base de datos elaborada en sql server.

5.1.1.1.3 [HW] Hardware (los equipos informáticos)

Los medios materiales, físicos, destinados a soportar directamente o indirectamente los servicios.

[serv]servidores

[seap] servidor de aplicaciones

Es el servidor encargado de almacenar las aplicaciones entre ellas al sistema de gestión académica para pregrado.

[sapb] servidor de aplicaciones - backup

Es el servidor de soporte del servidor de aplicaciones, encargado de almacenar las aplicaciones entre ellas al sistema de gestión académica para pregrado.

[sebd] servidor de base de datos

Es el servidor que almacena la base de datos del sistema de gestión académica para pregrado.

[sapd] servidor de aplicaciones 2

Es el servidor encargado de almacenar las aplicaciones entre ellas al sistema de gestión académica.

[sbdo] servidor de base de datos - OCCA

Es el servidor que almacena la base de datos del sistema de gestión académica.

[srbo] servidor de base de datos- backup -OCCA

Es el servidor que brinda soporte al servidor base de datos - OCCA, almacena la base de datos del sistema de gestión académica.

[sacd] servidor Directorio de Usuarios

Es el servidor que brinda soporte a la red de computadoras.

[sanv] servidor Antivirus

Es el servidor que brinda soporte al antivirus dentro de la red de computadoras.

[spro] servidor Proxy

Es el servidor encargado de la validad de los acceso y permisos a la red de computadoras.

[sred] soporte de la red

[conm] switch

Switch principal de la red - UNPRG, el cual se configura y se administra el acceso y restricciones a la red. Mediante el cual permite tener un control de los equipos que se conectan y los permisos que se les debe otorgar.

[cotf] firewall

Servidor que se configura y se administra el acceso y restricciones a las aplicaciones que se encuentran alojadas en los servidores de la UNPRG y a internet.

[rout] router

Router principal de la red - UNPRG, realiza el enrutamiento de la red y permite acceso al servicio de internet.

5.1.1.1.4 [COM] Redes de Comunicaciones

Incluye tanto instalaciones dedicadas como servicios de comunicaciones contratadas.

[rlan] red local

La red de la UNPRG abarca todas las oficinas, que cuenten con equipos informáticos, la ciudad universitaria, del centro pre, secretaria general entre otros.

[intr] internet

Servicio brindado por terceros, a través de líneas dedicadas que son distribuidas para los diferentes servicios que se tiene en la universidad.

5.1.1.1.5 [MEDIA] Soportes de Información

Se consideran dispositivos físicos que permitan almacenar información de forma permanente o, al menos, durante largos periodos de tiempo.

[disk] discos

Los discos (DVD/CD) son utilizados para almacenar información, que en caso que se presenten problemas se tiene una fuente confiable.

[prin] Documentación Impresa

La impresión de las constancias de matrículas y las constancias de notas son algunos de los documentos que se guardan en físico en archivos debidamente identificados.

5.1.1.1.6 [AUX] Equipamiento auxiliar

Se consideran otros equipos que sirven de soporte, sin estar directamente relacionados con datos.

[upsi]sistemas de alimentación ininterrumpida

Sistema de alimentación ininterrumpida (UPS), encargados de brindar energía por un tiempo determinado a los servidores en caso que la energía eléctrica se pierda.

[grue] grupo electrógeno

1 Motor generador de energía que funciona cuando hay una pérdida de energía eléctrica o algún problema eléctrico, se aproximó u uso por promedio de 2 días de autonomía sin ser recargado.

[eqcs]equipo de aire acondicionado

Es un equipo de aire acondicionado encargado de mantener a una temperatura adecuada el data center.

[cabl] cableado

[clec] cableado eléctrico

Conexiones del circuito eléctrico

[cart] cableado de red

Conexiones de cables de comunicaciones

5.1.1.1.7 [L] Instalaciones

[sase]Sala de Servidores

Es el local de la UNPRG, Red Telemática, donde se encuentran los equipos que brindan los servicios y el personal encargado de tener en funcionamiento óptimo los equipos.

5.1.1.1.8 [P] Personal

[user]Usuarios Finales

Alumnos, docentes y Trabajadores Administrativos, Los alumnos que ingresan al portal web para matricularse, ver sus notas, etc.; el personal administrativo principalmente de las oficinas de OAP y dirección de escuelas.

[admc] administrador de comunicaciones y seguridad

Ing. Vladimir Sabino Gonzáles Mechán.

Al culminar la tarea se obtiene la lista de los 27 activos como se muestra en el siguiente cuadro.

ACTIVOS
[S] Servicios
[gmat] Gestión de Matricula y notas de los alumnos – UNPRG
[SW] Software
[sgap] Sistema de Gestión Académica para Pre-Grado
[sega] Sistema de Gestión Académica
[HW] Hardware
[serv]servidores
[seap] servidor de aplicaciones
[sapb] servidor de aplicaciones – backup
[sebd] servidor de base de datos
[sapd] servidor de aplicaciones 2
[sbdo] servidor de base de datos – OCCA
[srbo] servidor de base de datos- backup –OCCA
[sacd] servidor Directorio de Usuarios
[sanv] servidor Antivirus
[spro] servidor Proxy
[sred] soporte de la red
[conm] switch
[cotf] firewall
[rout] router
[COM] Redes de Comunicaciones
[rlan] red local
[intr] internet
[MEDIA] Soportes de Información
[disk] discos
[prin] Documentación Impresa
[AUX] Equipamiento auxiliar
[upsi]sistemas de alimentación ininterrumpida
[grue] grupo electrógeno
[eqcs]equipo de aire acondicionado
[cabl] cableado
[clec] cableado eléctrico
[cart] cableado de red
[L] Instalaciones
[sase]Sala de Servidores
[P] Personal
[user]Usuarios Finales
[admc] administrador de comunicaciones y seguridad

Cuadro 10: Lista de Activos – AGRSGA-UNPRG.
Fuente: Obtenido De La Ejecución Del Proyecto En La Herramienta Pilar 5.4.5.

Las figuras de las estadísticas obtenidas a través de la herramienta Pilar según parámetros: por dominio, por capas y por fuente (**Anexo 3**).
El cuadro completo de cada activo y a la clase que pertenece, la tarea está incluida en la identificación de activos en la metodología Magerit pero para la Herramienta Pilar es denominada clasificación de activos, con mayor detalle ver el **Anexo 4.**

5.1.1.2 Tarea MAR 1.2: Dependencias entre los Activos

Una vez los activos son identificados hay que valorar las dependencias entre activos, es decir la medida en que un activo de orden superior se puede ver perjudicado por una amenaza materializada sobre un activo de orden inferior.

En la siguiente tabla, teniendo en cuenta las dependencias para operar, funcionalidad y de almacenamiento de datos, se determina la siguiente matriz de dependencias entre activos (según el tipo de activos que corresponda):

Tabla 5: Diagrama de dependencia de activos según su tipo

	[S]	[SW]	[HW]	[COM]	[MEDIA]	[AUX]	[L]	[P]
[S]	-	X	X	X		X	X	X
[SW]		-						X
[HW]			-				X	X
[COM]				-			X	X
[MEDIA]					-			X
[AUX]						-	X	X
[L]							-	X
[P]								-

Fuente: Elaborado por el usuario basado en las actividades de la metodología Magerit.

Donde:

[S]: Servicios
[SW]: Software
[HW]: Hardware
[COM]: Redes de Comunicaciones
[MEDIA]: Soportes de Información
[AUX]: Equipamiento auxiliar
[L] Instalaciones
[P] Personal

En el **Anexo 5** la lista completa de los activos y los activos de los que dependen.

El siguiente grafico muestra los activos y su dependencia, también llamado mapa de dependencia entre activos en Pilar, en el **Anexo 6** podemos encontrar información como estadísticas y más gráficos referentes a la tarea realizada en Pilar.

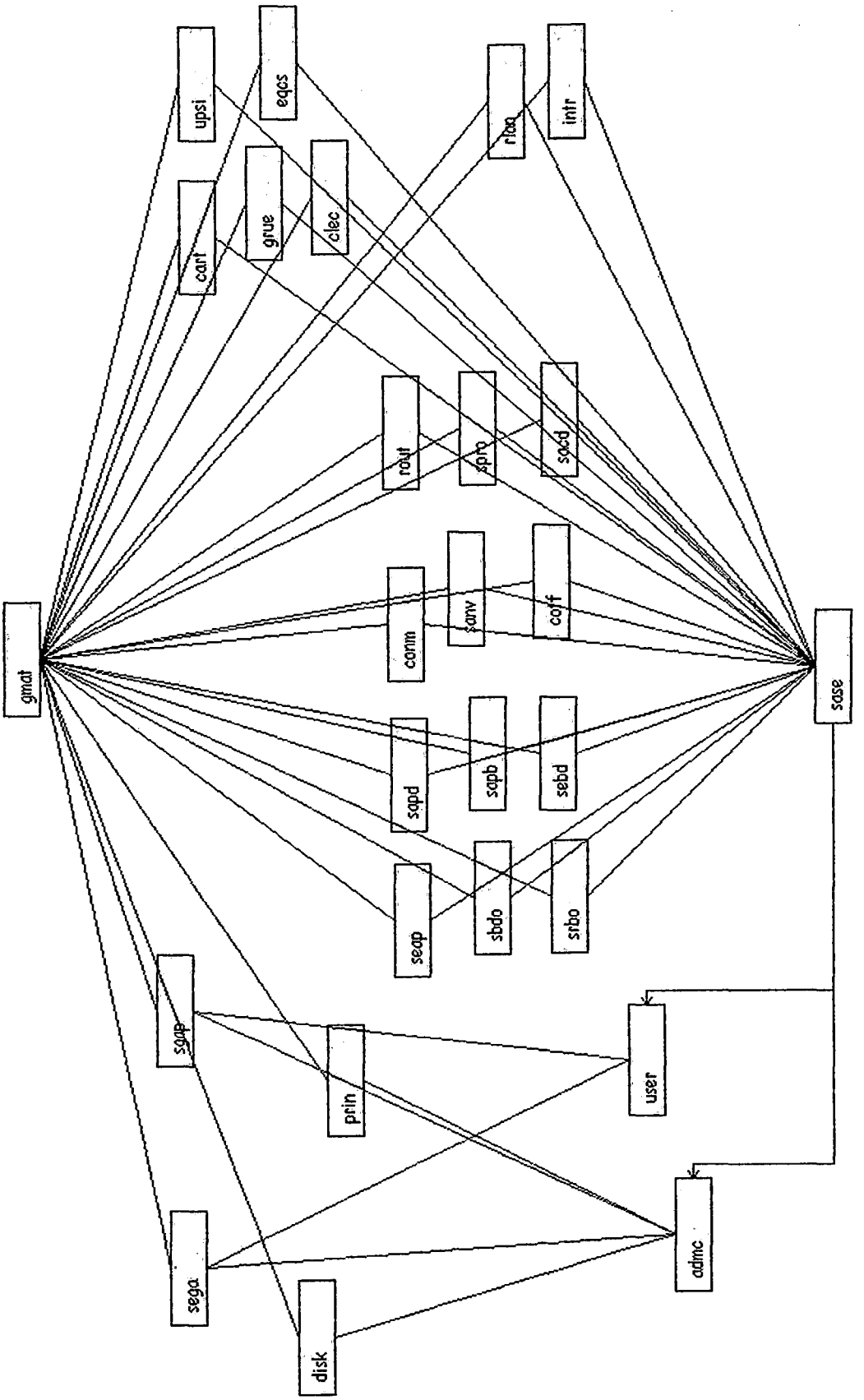

Gráfico 8: Dependencia de Activos – AGRSGA-UNPRG.
Fuente: Proyecto Pilar AGRSGA-UNPRG

5.1.1.3 Tarea MAR 1.3: Valoración de los Activos

La tarea tiene como objetivos: Identificar en que dimensión es valioso el activo para la institución la estimación de la valoración en cada dimensión.

La valoración de los activos se muestra a continuación:

Tabla 6: Valoración de Activos- AGRSGA-UNPRG

ACTIVOS	[D]	[I]	[C]	[A]	[T]
[S] Servicios					
[gmat] Gestión de Matricula y notas de los alumnos – UNPRG	A+	A+	A+	A+	A+
[SW] Software					
[sgap] Sistema de Gestión Académica para PreGrado	A			A-	A-
[sega] Sistema de Gestión Académica	A			A-	A-
[HW] Hardware					
[serv]servidores					
[seap] servidor de aplicaciones	A				A-
[sapb] servidor de aplicaciones – backup	A-				M
[sebd] servidor de base de datos	A	A	A-		A-
[sapd] servidor de aplicaciones 2	A				M
[sbdo] servidor de base de datos – OCCA	A	A	A-		A-
[srbo] servidor de base de datos- backup –OCCA	A-	A-	M+		A-
[sacd] servidor Directorio de Usuarios	M+				
[sanv] servidor Antivirus	M				
[spro] servidor Proxy	A-				A-
[sred] soporte de la red					
[conm] switch	M+				
[cotf] firewall	A-				M+
[rout] router	A-				M+
[COM] Redes de Comunicaciones					
[rlan] red local	A				M
[intr] internet	A-				M
[MEDIA] Soportes de Información					
[disk] discos	B+		A-		
[prin] Documentación Impresa	M+	M+	A-	M+	
[AUX] Equipamiento auxiliar					
[upsi]sistemas de alimentación ininterrumpida	M				
[grue] grupo electrógeno	M				
[eqcs]equipo de aire acondicionado	M+				
[cabl] cableado					
[clec] cableado eléctrico	A-				
[cart] cableado de red	A-				
[L] Instalaciones					
[sase]Sala de Servidores	M+				M
[P] Personal					
[user]Usuarios Finales					
[admc] administrador de comunicaciones y seguridad					

Fuente: obtenido de la aplicación del proyecto utilizando la herramienta Pilar 5.4.5.

Se consideran dos datos importantes como dimensiones y criterios de valoración.

Dimensiones

- [D]Disponibilidad
- [I] Integridad de los datos
- [C]Confidencialidad de los datos
- [A]Autenticidad de los usuarios y de la información
- [T]Trazabilidad del servicio y de los datos

Criterios de la valoración

Véase en la tabla 1 Escala detallada de los criterios de valoración.

El valor puede ser propio, o puede ser acumulado. Se dice que los activos inferiores en un esquema de dependencias, acumulan el valor de los activos que se apoyan en ellos.

Tabla 7: Tabla de criterios de valoración - Pilar

CRITERIOS		
10	Nivel 10	10
9	Nivel 9	9
A+	Nivel alto +	8
A	Nivel alto	7
A-	Nivel alto -	6
M+	Nivel medio +	5
M	Nivel medio	4
M-	Nivel medio -	3
B+	Nivel bajo +	2
B	Nivel bajo	1
0	Sin valor apreciable	0

Fuente: obtenido de la aplicación del proyecto utilizando la herramienta Pilar 5.4.5.

Tabla 8: Valoración de Activos - Valor Acumulado – AGRSGA-UNPRG.

ACTIVOS	[D]	[I]	[C]	[A]	[T]
[S] Servicios					
[gmat] Gestión de Matricula y notas de los alumnos – UNPRG	A+	A+	A+	A+	A+
[SW] Software					
[sgap] Sistema de Gestión Académica para PreGrado	A+	A+	A+	A+	A+
[sega] Sistema de Gestión Académica	A+	A+	A+	A+	A+
[HW] Hardware					
[serv]servidores					
[seap] servidor de aplicaciones	A+	A+	A+	A+	A+
[sapb] servidor de aplicaciones – backup	A+	A+	A+	A+	A+
[sebd] servidor de base de datos	A+	A+	A+	A+	A+
[sapd] servidor de aplicaciones 2	A+	A+	A+	A+	A+
[sbdo] servidor de base de datos – OCCA	A+	A+	A+	A+	A+
[srbo] servidor de base de datos- backup –OCCA	A+	A+	A+	A+	A+
[sacd] servidor Directorio de Usuarios	A+	A+	A+	A+	A+
[sanv] servidor Antivirus	A+	A+	A+	A+	A+
[spro] servidor Proxy	A+	A+	A+	A+	A+
[sred] soporte de la red					
[conm] switch	A+	A+	A+	A+	A+
[cotf] firewall	A+	A+	A+	A+	A+
[rout] router	A+	A+	A+	A+	A+
[COM] Redes de Comunicaciones					
[rlan] red local	A+	A+	A+	A+	A+
[intr] internet	A+	A+	A+	A+	A+
[MEDIA] Soportes de Información					
[disk] discos	A+	A+	A+	A+	A+
[prin] Documentación Impresa	A+	A+	A+	A+	A+
[AUX] Equipamiento auxiliar					
[upsi]sistemas de alimentación ininterrumpida	A+				
[grue] grupo electrógeno	A+				
[eqcs]equipo de aire acondicionado	A+				
[cabl] cableado					
[clec] cableado eléctrico	A+	A+	A+	A+	A+
[cart] cableado de red	A+	A+	A+	A+	A+
[L] Instalaciones					
[sase]Sala de Servidores	A+	A+	A+	A+	A+
[P] Personal					
[user]Usuarios Finales	A+	A+	A+	A+	A+
[admc] administrador de comunicaciones y seguridad	A+	A+	A+	A+	A+

Fuente: obtenido de la aplicación del proyecto utilizando la herramienta Pilar 5.4.5.

5.1.2 MAR 2: Caracterización de las Amenazas

El objetivo es esta actividad es identificar las posibles amenazas que se pueden materializar sobre los activo y estimar la frecuencia de ocurrencia y degradación que causa.

En la siguiente figura se muestra la pantalla de trabajo para la caracterización de las amenazas. En el desarrollo usando la herramienta Pilar se presenta una opción de determinar la proporción de los factores para determinar las amenazas, para el estudio se toma la configuración pre determinada y se prosigue a la tarea siguiente.

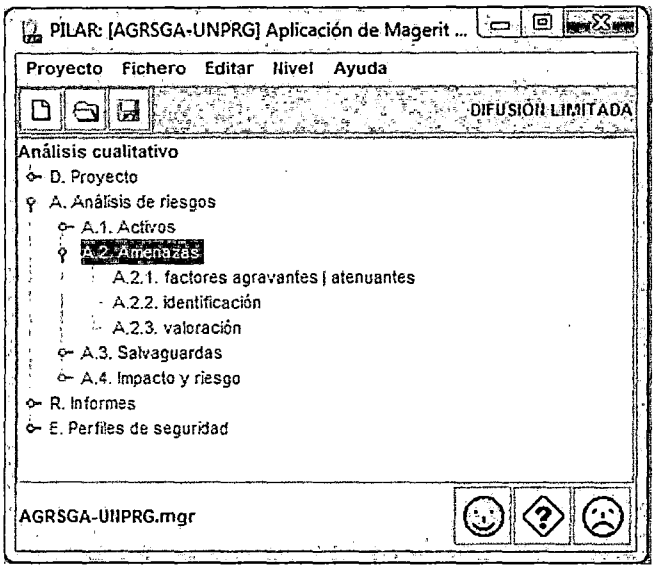

Figura 12: Pantalla de trabajo de caracterización de las amenazas
Fuente: obtenido de la aplicación del proyecto utilizando la herramienta Pilar 5.4.5

5.1.2.1 Tarea MAR 2.1: Identificación de las Amenazas

El objetivo de la tarea es identificar las amenazas relevantes sobre cada activo.
La herramienta Pilar estandarizada por Magerit. Las amenazas están clasificadas en cuatro grupos:

- [N] Desastres Naturales
- [I] De origen industrial
- [E] Errores y fallos no intencionados
- [A]Ataque deliberados

Se identifican las amenazas sobre cada activo, la siguiente lista muestra las amenazas que se identifican sobre los servidores de los sistemas de gestión académica.

[N] Desastres Naturales
[N.1]Fuego
[N.2]Daños por agua
[N.*]Desastres naturales
[I] De origen industrial
[I.5]Avería de origen físico o lógico
[I.6]Corte del suministro eléctrico
[I.7]Condiciones inadecuadas de temperatura o humedad
[E] Errores y fallos no intencionados
[E.2]Errores del administrador del sistema/ seguridad
[E.23]Errores de mantenimiento – hardware
[E.24]Caída del sistema por agotamiento de recursos
[E.25]Perdida de equipos
[A]Ataque deliberados
[A.6]Abuso de privilegios de acceso
[A.7]Uso no previsto
[A.11]Acceso no autorizado

[A.23]Manipulación del hardware
[A.24]Denegación de servicios
[A.25]Robo de equipos
[A.26]Ataque destructivos

El resultado de la tarea: Lista completa de los activos con sus respectivas amenazas se ubica en el **Anexo 8.** La lista de las Amenazas que se emplean en la Metodología Magerit y Herramienta Pilar se encuentra en el **Anexo 7.**

5.1.2.2 Tarea MAR 2.1: Valoración de las Amenazas

En la tarea Valoración de las Amenazas, se estima la frecuencia y la degradación de la materialización de las amenazas sobre cada activo identificado.

- Probabilidad de ocurrencia: representa la tasa anual de ocurrencia, de cada cuanto se materializa una amenaza.
- Porcentaje de degradación: significa el daño causado por un incidente.

La herramienta Pilar, tiene tablas de valores para la probabilidad de ocurrencia y el porcentaje de degradación, las cuales van a la par con las establecidas en la metodología Magerit. Para el estudio se usan las tablas propuestas por la herramienta Pilar.

Tabla 9: Probabilidad

Como describir la probabilidad de que se materialice una amenaza.

Potencia	Probabilidad	Nivel	Facilidad	Frec.
XL extra grande	CS casi seguro	MA muy alto	F fácil	100
L grande	MA muy alta	A alto	M medio	10
M medio	P posible	M medio	D difícil	1
S pequeño	PP poco probable	B bajo	MD muy difícil	0.1
XS muy pequeño	MR muy rara	MB muy bajo	ED extremadamente difícil	0.01

Fuente: obtenida del manual de usuarios de pilar.

Tabla 10: Degradación

Como describir las consecuencias de la materialización de una amenaza.

Nivel		Porcentaje
T	total	100%
MA	muy alta	90%
A	Alta	50%
M	media	10%
B	Baja	1%

Fuente: obtenida del manual de usuarios de pilar.

Posteriormente esta degradación se extiende debido a la dependencia entre activos, obteniendo el impacto y el riesgo, tanto acumulado como repercutido antes de aplicar las salvaguardas.

Si un activo A depende de otro B, el valor del impacto acumulado de A se acumula B en la proporción en la que depende. Por otro lado, el impacto repercutido indica que el daño en B en A en la proporción en la que A depende de B.

Impacto = Valor x Degradación

Riesgo = Impacto x Frecuencia

La Tabla muestra la valoración de las amenazas de los activos según sus dimensiones.

Tabla 11: valoración de las amenazas - AGRSGA-UNPRG

ACTIVOS / AMENAZAS	[D]	[I]	[C]	[A]	[T]
[S] Servicios					
[gmat] Gestión de Matricula y notas de los alumnos – UNPRG	A	A	A	A	A
[SW] Software					
[sgap] Sistema de Gestión Académica para PreGrado	A	A	A	A	
[sega] Sistema de Gestión Académica	A	A	A	A	
[HW] Hardware					
[serv]servidores					
[seap] servidor de aplicaciones	A	M	A		
[sapb] servidor de aplicaciones – backup	A	M	A		
[sebd] servidor de base de datos	A	M	A		
[sapd] servidor de aplicaciones 2	A	M	A		
[sbdo] servidor de base de datos – OCCA	A	M	A		
[srbo] servidor de base de datos- backup -OCCA	A	M	A		
[sacd] servidor Directorio de Usuarios	A	M	A		
[sanv] servidor Antivirus	A	M	A		
[spro] servidor Proxy	A	M	A		
[sred] soporte de la red					
[conm] switch	A	M	A		
[cotf] Firewall	A	M	A		
[rout] router	A	M	A		
[COM] Redes de Comunicaciones					
[rlan] red local	A	M	A	A	
[intr] internet	A	M	A	A	
[MEDIA] Soportes de Información					
[disk] discos	A	M	M		
[prin] Documentación Impresa	A	M	M		
[AUX] Equipamiento auxiliar					
[upsi] Sistema de alimentación ininterrumpida	B				
[grue] grupo electrógeno	B				
[eqcs]equipo de aire acondicionado	B				
[cabl] cableado					
[clec] cableado eléctrico	A	B	A		
[cart] cableado de red	A	B	A		
[L] Instalaciones					
[sase]Sala de Servidores	A	M	A		
[P] Personal					
[user]Usuarios Finales	M	A	M		
[admc] administrador de comunicaciones y seguridad	A	M	A		

Fuente: Fuente: Proyecto Pilar AGRSGA-UNPRG

El resultado de la tarea: Lista completa de los activos con la valoración de sus respectivas amenazas, se ubica en el **Anexo 9**.

5.1.3 MAR 3: Caracterización de las Salvaguardas

En esta actividad se identifican las salvaguardas efectivas para la organización junto con la eficacia que tiene cada una de ellas para mitigar el riesgo. En el desarrollo de la metodología se definen varias etapas, para el estudio se a determinado las siguiente:

- Primera etapa llamada POTENCIAL (potencial), desde el inicio de la creación del proyecto hasta la caracterización de amenazas.
- Segunda etapa llamada SITUACIÓN ACTUAL (actual), toma los resultados de la primera etapa incluyendo la influencia de las salvaguardas implantadas hasta el momento.
- Tercera etapa OBJETIVO (objetivo), recoge los datos de las dos etapas anteriores pero también hace referencia a los posibles resultados tras el plan de mitigación. Esta etapa se desarrolla en el proceso Gestión de Riesgos.

En la herramienta Pilar para el desarrollo de la actividad se toma en cuenta los siguientes cuadros:

Abreviaturas	Aspecto (que trata la salvaguarda)
G	para Gestión
T	para Técnico
F	para seguridad Física
P	Para gestión del Personal

Cuadro 11: Aspecto de las Salvaguardas
Fuente: obtenida del manual de usuarios de pilar.

Abreviatura	Tipo de protección de salvaguardas
PR	Prevención
DR	Disuasión
EL	Eliminación
IM	Minimización del impacto
CR	Corrección
RC	Recuperación
AD	Administrativa
AW	Concienciación
DC	Detención
MN	Monitorización

Cuadro 12: Tipo de protección de salvaguardas
Fuente: obtenida del manual de usuarios de pilar.

PILAR	Valoración		
		Máximo peso	Critica
		Peso alto	Muy importante
		Peso normal	Importante
		Peso bajo	Interesante

Cuadro 13: Peso relativo de salvaguardas
Fuente: obtenida del manual de usuarios de pilar.

5.1.3.1 Tarea MAR 3.1: Identificación de las Salvaguardas Existentes

En esta tarea se identifican las salvaguardas establecidas para proteger a los activos, utilizando la herramienta Pilar, se valora a traves de las recomendaciones de la herramienta, que tan necesario es establecer una salvaguarda en un rango estimado de 0 a 10. Se considera el agrupamiento de Salvaguardas que realiza Magerit y Pilar, se explica cada agrupamiento de salvaguardas, el porque se escoje, sobre que activos se aplica, y a que amenazas enfrenta. se identifica el grado de seguridad implementado en la institucion, para ello se indaga una serie de aspectos generales e individuales considerando cada activo.

- **Protecciones Generales.**

  Se escoge esta salvaguarda por que define el uso controles y herramientas de identificacion , autenticidad , monitorizacion de accesos. La salvaguarda se aplica sobre activos como : Servicios, Software, Hardware, Redes de Comunicaciones, Soportes de Información, Equipamiento auxiliar, Instalaciones y Personal . hace frente a amenazas como: Errores de los usuarios, Errores de administrador del sistema / de la seguridad, difusión de software dañino, alteración de la información, errores de secuencia, alteración de la información, destrucción de la información, fugas de información, vulnerabilidades de los programas, perdida de equipos, indisponibilidad del personal, suplantación de la identidad, abuso de privilegios de acceso, uso no previsto, acceso no autorizado, manipulación del software y manipulación del hardware.

- **Protección de los Servicios.**

  La salvaguarda plantea el aseguramiento de la disponibilidad, así como la gestión de cambios y aplicación de perfiles de seguridad buscando brindar un servicio con un alto grado de calidad. Hace frente a amenazas como: errores de los usuarios, errores del administrador del sistema / de la seguridad, alteración de la información, fugas de información, caída del sistema por agotamiento de recursos, abuso de privilegios de acceso, uso no previsto, acceso no autorizado, destrucción de información y denegación de servicio.

- **Protección de las aplicaciones informáticas.**

  La salvaguarda plantea la gestión del uso y seguridad de los software utilizados para brindar el servicio final. Hace frente a amenazas como: errores de los usuarios, errores del administrador del sistema / de la seguridad, difusión de software dañino, destrucción de la información, vulnerabilidad de los programas, errores de mantenimientos / actualización, abuso de privilegios de acceso, uso no previsto y manipulación de programas.

- **Protección de los equipos informáticos**

  La salvaguarda plantea el aseguramiento de la disponibilidad, seguridad, mantener equipos operativos al aplicar cambios y operaciones. Hace frente a amenazas como: Desastres naturales, daños causados por fuego, agua, contaminación medioambiental, contaminación electromagnética, averías de

origen físico o lógico, condiciones inadecuadas de temperatura o humedad, errores del administrador del sistema / de la seguridad, errores de mantenimiento / actualización de equipos, caída del sistema por agotamiento de recursos, perdida de equipos, abuso de privilegios de acceso, uso no previsto, acceso no autorizado, manipulación de hardware y robo de equipos.

- **Protección de las comunicaciones.**

  La salvaguarda gestiona la integridad y confidencialidad de los datos intercambiados, el acceso al servicio, perfiles de seguridad, para ellos asegurar la disponibilidad y el correcto uso de las conexiones entrantes y salientes. Hace frente a amenazas como: fallo de servicios de comunicaciones, errores del administrador de sistema / de la seguridad, errores de re-encaminamiento, errores de secuencia, alteración de la información, fugas de información, caída del sistema por agotamiento de recursos, suplantación de la identidad, abuso de privilegios de acceso, uso no previsto, acceso no autorizado, análisis de tráfico, interceptación de información, modificación de la información, destrucción de la información y denegación de servicio.

- **Protección de los soportes de información**

  La salvaguarda gestiona la seguridad de los dispositivos físicos o documentos y la integridad de la información que almacenan. Hace frente a amenazas como: desastres naturales, desastres ocasionados por incendios, agua, industriales, contaminación medioambiental, avería de origen físico o lógico, degradación de los soportes de almacenamiento de la información, errores de los usuarios, alteración de la información, fugas de información, revelación de información y ataques destructivos.

- **Elementos auxiliares**

  La salvaguarda gestión la implementación de planes de seguridad que involucran al suministro eléctrico, la climatización y las protecciones del cableado de red. Hace frente a amenazas como: desastres naturales, desastres por fuego, agua, contaminación medioambiental, contaminación electromagnética, averías de origen físico o lógico, corte del suministro eléctrico, condiciones inadecuadas de temperaturas o humedad, errores de los usuarios, errores del administrador del sistema / de la seguridad, errores de mantenimiento, perdida de equipos, indisponibilidad del personal, uso n previsto, acceso no autorizado, robo de equipos y ataque destructivos.

- **Protección de las instalaciones**

  La salvaguarda plantea el control de los accesos y el estado del diseño de los ambiente. Hace frente a amenazas como: desastres naturales, fuego, agua, contaminación ambiental, contaminación electromagnética, suplantación de identidad, abuso de privilegios de acceso, uso no previsto, acceso no autorizado, ataque destructivo y ocupación enemiga.

- **Gestión del personal**

  La salvaguarda planeta formación y concienciación, disponibilidad del personal. Hace frente a amenazas como: alteración de la información, destrucción de la información, fugas de información, indisponibilidad del personal, extorción e ingeniería social.

- **Adquisicion / desarrollo**

  La salvaguarda plantea la compra o el desarrollo de aplicaciones, equipos informáticos, de comunicaciones, de soporte de información o comunicaciones que aporten a la mejora del servicio. Hace frente a amenazas como: errores de usuarios, errores del administrador del sistema / de la seguridad, difusión de software dañino, alteración de información, fugas de información, vulnerabilidad de los sistemas, errores de mantenimiento / actualización de programas, perdida de equipos, abuso de privilegios de acceso y uso no previsto.

Tabla 12: Lista de salvaguardas existentes y valoración de Pilar.

[base]UNPRG : [F-ASUNPRG] Administración de servidores – UNPRG				
Asp	Tdp		Salvaguardas	Recom
G	PR		[H]Protecciones Generales	7
G	PR		[S]Protección de los servicios	6
G	PR		[SW]Protección de las Aplicaciones informáticas	7
G	PR		[HW]Protección de los Equipos Informáticos	7
G	PR		[COM]Protección de las Comunicaciones	8
G	PR		[MP] Protección de los soportes de información	7
G	PR		[AUX]Elementos Auxiliares	6
F	PR		[L]Protección de las instalaciones	7
P	PR		[PS]Gestión del Personal	6
G	AD		[NEW]Adquisición / desarrollo	4

Fuente: Proyecto Pilar AGRSGA-UNPRG

5.1.3.2 Tarea MAR 3.2: Valoración de las Salvaguardas

El objetivo de la tarea es valorar las salvaguardas implementadas.

Se determina las salvaguardas implantadas actualmente, modelándolas a los agrupamientos planteados por Magerit y Pilar.

- **Protecciones Generales.**

  La Universidad como institucion posee politicas de seguridad para sus procesos, el area en estudio hereda parte de estas politicas, al hacer mencion del area se hace referencia al area de administracion de red, donde existe un responsable encargado de la seguridad y del funcionamiento de los servicio que se brindan, el cual informa al jefe de la ocifina central de informacion donde pertenece la area.

  Las salvaguardas implementadas son:

- **Control de acceso lógico**, existe implementados servidores proxy y firewall, con objetivos de control, restricciones de acceso a usuarios y aplicaciones.
- **Segregación de tareas**, la atención de servicios son realizadas por el encargado del área.
- **Herramienta contra código dañino**, un servidor antivirus esta implementado, pero presenta serios problemas de actualización.
- **Herramienta de monitorización de tráfico**, existe implementaba una herramienta pero en versión de prueba y uso interno para establecer el tráfico de la red.

➢ **Protección de los Servicios.**

La normativa implementada para el uso del servicio de gestión académica es ajustada al agrupamiento de la metodología Magerit. Las salvaguardas implementadas son:

- **Aseguramiento de la disponibilidad,** se coordina la elaboración de un cronograma de matrícula intentando reducir el flujo de visitar.
- **Aceptación y puesta en operación,** al inicio y fin del ciclo son las temporadas donde el servicio es mar requerido.
- **Se aplican perfiles de seguridad,** el acceso se realiza a través de la solicitud de una clave y contraseña.

➢ **Protección de las aplicaciones informáticas.**

Con respecto a los sistemas de gestión académica y sistema de gestión académica para pre-grado, las salvaguardas implementadas son:

- **Copias de seguridad (backup),** se accede a los sistemas a través de dos servidores que los almacenan.
- **Se aplican perfiles de seguridad,** el acceso se realiza a través de la solicitud de una clave y contraseña.
- **Cambios (actualizaciones y mantenimiento),** los datos son almacenados en servidores de base de datos para contar con la información actualizada.

➢ **Protección de los equipos informáticos**

Para el estudio se consideran: los servidores que contienen las aplicaciones y las bases de datos de los sistemas de Gestión Académica, los servidores que aportan a la seguridad como antivirus, control de acceso de usuario. También el switch y router principales, uno permite el acceso de usuarios que se encuentren en la red local de la Universidad y el otro permite acceder a los servicios a través de la red de internet.

- **Se aplican perfiles de seguridad,** los equipos se encuentran instalados en la sala de servidores, se accede a los servidores a través de los sistemas de gestión académica.

- **Aseguramiento de la disponibilidad,** el servidor de aplicación (sistema de gestión académica para Pre-Grado)cuenta con un servidores de soporte de aplicación y un servidor de base de datos, el sistema de gestión académica con un servidor de aplicaciones, un servidor de base de datos y un servidor de soporte de base de datos.
  El servidor de antivirus encargado de la seguridad, el servidor proxy y el firewall encargados de la gestión de usuarios y accesos.
- **Cambios (actualizaciones y mantenimiento),** el mantener la funcionalidades necesarias para gestionar el servicio.

➢ **Protección de las comunicaciones.**

- **Protección de la integridad de los datos intercambiados,** la red local de la Universidad interconectan todas las dependencias para manejar datos en tiempo administrables.
- **Internet,** el acceso a través de internet a los sistemas de gestión académica, se utiliza el servicio dedicado de una empresa pero con el uso de varias líneas.

➢ **Protección de los soportes de información**

La información se encuentra almacenada en servidores, también en discos como backup y en forma física almacenada en folios ordenados por periodos.

- **Aseguramiento de la disponibilidad,** cada facultad cuenta con los documentos sobre el proceso de matrícula y notas finales, archivados los cuales son aun utilizados para constatar la información generada por los sistemas o en caso que no se puede acceder a ellos.

➢ **Elementos auxiliares**

En la sala de servidores se cuenta con varios UPS, 1 sistema de climatización y 1 grupo electrógeno.

- **Aseguramiento de la disponibilidad,** se realiza un seguimiento regular del estado de los elementos.
- **Instalación,** los elementos se encuentran en su mayoría ubicados en a la sala de servidores.
- **Suministro eléctrico,** se cuenta con un generados de energiza que brinda soporte a la sala de servidores.
- **Climatización,** un sistema climático encargado de mantener a una temperatura adecuada la sala de servidores.
- **Protección del cableado,** todas las conexiones partes desde la sala de servidores hacia todas las áreas distribuidas en los ambientes de la Universidad.

➢ **Protección de las instalaciones**

Se cuenta con un solo local donde se encuentran la sala de servidores, y el área de administración de soporte y mantenimiento de los mismos.

- **Control de los accesos físicos,** el ambiente se mantiene cerrado, las llaves de la única puerta de acceso solo las tienen algunos trabajadores, entre ellos el administrador de red.
- **Aseguramiento de la disponibilidad,** la opción del ingreso a la sala de servidores es manejada por el administrador, en conjunto con el encargado de la oficina a la que pertenece esta área.

➢ **Gestión del personal**

La red telemática cuenta actualmente con un encargado, y el apoyo de practicantes que son estudiantes de los últimos ciclos de las carreras de Ing. en Computación e Informática, Ing. de Sistemas e Ing. Electrónica de la casa de estudios.

- **Formación y concienciación,** es la salvaguarda implementada, se gestiona la formación a los usuarios del uso adecuado de las propiedades de la Universidad, considerando los servicios que ofrece y las instalaciones del campus.

➢ **Adquisición / desarrollo**

La administración de red telemática, posee proyectos en prueba como: servidores, con mejor software y hardware que los actuales, para repotenciar algunos servicios como el de protección de acceso, antivirus, aplicaciones, etc. Un proyecto de construcción de nuevos ambientes destinados a esta área.

- **Equipos y aplicaciones:** se realizan proyectos de prueba para la implementación de servidores que mejoren la seguridad y el servicio ofrecido, y configuraciones para los equipos de comunicaciones.
- **Comunicaciones:** buscándose establecer el correcto uso de las líneas de comunicaciones para disminuir el riesgo de pérdida de conexión.

Para el caso la valoración de salvaguardas se considera la etapa actual en donde se considera el valor que representa las salvaguardas implantadas actualmente. Se utiliza los datos de valoración de la tabla 4.

Tabla 13: Valoración de las Salvaguardas - AGRSGA-UNPRG

Asp	Tdp		Salvaguardas	Recom.	Actual
G	PR		[H]Protecciones Generales	7	L2
G	PR		[S]Protección de los servicios	6	L2
G	PR		[SW]Protección de las Aplicaciones informáticas	7	L2
G	PR		[HW]Protección de los Equipos Informáticos	7	L2
G	PR		[COM]Protección de las Comunicaciones	8	L2
G	PR		[MP] Protección de los soportes de información	7	L2
G	PR		[AUX]Elementos Auxiliares	6	L2
F	PR		[L]Protección de las instalaciones	7	L2
P	PR		[PS]Gestión del Personal	6	L2
G	AD		[NEW]Adquisición / desarrollo	4	L2

Fuente: Proyecto Pilar AGRSGA-UNPRG.

5.1.4 MAR 4: Estimación del Estado de Riesgo

En esta tarea se combinan los descubrimientos de las tareas anteriores para derivar estimaciones del estado de riesgo de la Organización.

Esta actividad consta de tres tareas:

- Estimación del impacto
- Estimación del riesgo

El objetivo de estas tareas es disponer de una estimación fundada de lo que puede ocurrir (impacto) y de lo que probablemente ocurra (riesgo).

5.1.4.1 Tarea MAR 4.1: Estimación del Impacto

En esta tarea se estima el impacto al que están expuestos los activos:

- el impacto potencial, al que está expuesto el sistema teniendo en cuenta el valor de los activos y la valoración de las amenazas; pero no las salvaguardas actualmente desplegadas
- el impacto residual, al que está expuesto el sistema teniendo en cuenta el valor de los activos y la valoración de las amenazas, así como la eficacia de las salvaguardas actualmente desplegadas

Tabla 14: Estimación del Impacto

CRITERIOS			
10	Nivel 10	10	
9	Nivel 9	9	
A+	Nivel alto +	8	
A	Nivel alto	7	
A-	Nivel alto -	6	
M+	Nivel medio +	5	
M	Nivel medio	4	
M-	Nivel medio -	3	
B+	Nivel bajo +	2	
B	Nivel bajo	1	
0	Sin valor apreciable	0	

Fuente: Manual del Usuario de Pilar.

5.1.4.1.1 Impacto Potencial

Se denomina impacto a la medida del daño sobre el activo derivado de la materialización de una amenaza. Conociendo el valor de los activos (en varias dimensiones) y la degradación que causan las amenazas, es directo derivar el impacto que estas tendrían sobre el sistema.

El impacto acumulado se calcula para cada activo, por cada amenaza y en cada dimensión de valoración, siendo una función del valor acumulado y de la degradación causada.

Tabla 15: Impacto Potencial

	[D]	[I]	[C]	[A]	[T]
ACTIVOS	[A]	[A]	[A]	[A]	
[S] Servicios	[A]	[A]	[A]	[A]	
[gmat] Gestión de Matricula y notas de los alumnos – UNPRG	[A]	[A]	[A]	[A]	
[SW] Software	[A]	[A]	[A]	[A]	
[sgap] Sistema de Gestión Académica para PreGrado	[A]	[A]	[A]	[A]	
[sega] Sistema de Gestión Académica	[A]	[A]	[A]	[A]	
[HW] Hardware	[A]	[A-]	[A]		
[serv]servidores	[A]	[A-]	[A]		
[seap] servidor de aplicaciones	[A]	[A-]	[A]		
[sapb] servidor de aplicaciones – backup	[A]	[M+]	[A]		
[sebd] servidor de base de datos	[A]	[M+]	[A]		
[sapd] servidor de aplicaciones 2	[A]	[M+]	[A]		
[sbdo] servidor de base de datos – OCCA	[A]	[M+]	[A]		
[srbo] servidor de base de datos- backup –OCCA	[A]	[M+]	[A]		
[sacd] servidor Directorio de Usuarios	[A]	[A-]	[A]		
[sanv] servidor Antivirus	[A]	[M+]	[A]		
[spro] servidor Proxy	[A]	[M+]	[A]		
[sred] soporte de la red	[A]	[M+]	[A]		
[conm] switch	[A]	[M+]	[A]		
[cotf] firewall	[A]	[M+]	[A]		
[rout] router	[A]	[M+]	[A]		
[COM] Redes de Comunicaciones	[A]	[A-]	[A]	[A]	
[rlan] red local	[A]	[A-]	[A]	[A]	
[intr] internet	[A]	[A-]	[A]	[A]	
[MEDIA] Soportes de Información	[A]	[M]	[M+]		
[disk] discos	[A]	[M]	[M+]		
[prin] Documentación Impresa	[A]	[M]	[M+]		
[AUX] Equipamiento auxiliar	[A]	[B+]	[A]		
[upsi]sistemas de alimentación ininterrumpida	[B+]				
[grue] grupo electrógeno	[B+]				
[eqcs]equipo de aire acondicionado	[B+]				
[cabl] cableado	[A]	[B+]	[A]		
[clec] cableado eléctrico	[A]	[B+]	[A]		
[cart] cableado de red	[A]	[B+]	[A]		
[L] Instalaciones	[A]	[M+]	[A]		
[sase]Sala de Servidores	[A]	[M+]	[A]		
[P] Personal	[A]	[A]	[A]		
[user]Usuarios Finales	[M+]	[A]	[A-]		
[admc] administrador de comunicaciones y seguridad	[A]	[M+]	[A]		

Fuente: Proyecto Pilar AGRSGA-UNPRG

5.1.4.1.2 Impacto Residual

Dado un cierto conjunto de salvaguardas desplegadas y una medida de la madurez de su proceso de gestión, el sistema queda en una situación de posible impacto que se denomina residual. Se dice que hemos modificado el impacto, desde un valor potencial a un valor residual. El cálculo del impacto residual es sencillo. Como no han cambiado los activos, ni sus dependencias, sino solamente la magnitud de la degradación, se repiten los cálculos de impacto con este nuevo nivel de

degradación. La magnitud de la degradación tomando en cuenta la eficacia de las salvaguardas, es la proporción que resta entre la eficacia perfecta y la eficacia real.

Tabla 16: Impacto Residual

	[D]	[I]	[C]	[A]	[T]
ACTIVOS	[A]	[A-]	[A]	[A]	
[S] Servicios	[A]	[A-]	[A-]	[A-]	
[gmat] Gestión de Matricula y notas de los alumnos – UNPRG	[A]	[A-]	[A-]	[A-]	
[SW] Software	[A]	[A-]	[A-]	[A-]	
[sgap] Sistema de Gestión Académica para PreGrado	[A]	[A-]	[A-]	[A-]	
[sega] Sistema de Gestión Académica	[A]	[A-]	[A-]	[A-]	
[HW] Hardware	[A]	[M+]	[A]		
[serv]servidores	[A]	[M+]	[A]		
[seap] servidor de aplicaciones	[A]	[M-]	[A]		
[sapb] servidor de aplicaciones – backup	[A]	[M-]	[A]		
[sebd] servidor de base de datos	[A]	[M-]	[A]		
[sapd] servidor de aplicaciones 2	[A]	[M-]	[A]		
[sbdo] servidor de base de datos – OCCA	[A]	[M-]	[A]		
[srbo] servidor de base de datos- backup –OCCA	[A]	[M-]	[A]		
[sacd] servidor Directorio de Usuarios	[A]	[M+]	[A]		
[sanv] servidor Antivirus	[A]	[M+]	[A]		
[spro] servidor Proxy	[A]	[M+]	[A]		
[sred] soporte de la red	[A]	[M+]	[A]		
[conm] switch	[A]	[M+]	[A]		
[cotf] firewall	[A]	[M+]	[A]		
[rout] router	[A]	[M+]	[A]		
[COM] Redes de Comunicaciones	[M]	[M+]	[A]	[A]	
[rlan] red local	[M]	[M+]	[A]	[A]	
[intr] internet	[M]	[M+]	[A]	[A]	
[MEDIA] Soportes de Información	[M+]	[B+]	[M-]		
[disk] discos	[M+]	[B+]	[M-]		
[prin] Documentación Impresa	[M+]	[B+]	[M-]		
[AUX] Equipamiento auxiliar	[A]	[B+]	[A]		
[upsi]sistemas de alimentación ininterrumpida	[B+]				
[grue] grupo electrógeno	[B+]				
[eqcs]equipo de aire acondicionado	[B+]				
[cabl] cableado	[A]	[B+]	[A]		
[clec] cableado eléctrico	[A]	[B+]	[A]		
[cart] cableado de red	[A]	[B+]	[A]		
[L] Instalaciones	[A]	[B+]	[M]		
[sase]Sala de Servidores	[A]	[B+]	[M]		
[P] Personal	[M]	[M]	[M]		
[user]Usuarios Finales	[B+]	[M]	[M-]		
[admc] administrador de comunicaciones y seguridad	[M]	[B+]	[M]		

Fuente: Proyecto Pilar AGRSGA-UNPRG

5.1.4.2 Tarea MAR 4.2 Estimación del Riesgo

En esta tarea se estima el riesgo al que están sometidos los activos del sistema: el riesgo potencial, al que está sometido el sistema teniendo en cuenta el valor de los activos y la valoración de las amenazas; pero no las salvaguardas actualmente desplegadas.

El riesgo residual, al que está sometido el sistema teniendo en cuenta el valor de los activos y la valoración de las amenazas, así como la eficacia de las salvaguardas actualmente desplegadas

Tabla 17: Criterios de Estimación del Riesgo

CRITERIOS			
9	Nivel 9	9	
A+	Nivel alto +	8	
A	Nivel alto	7	
A-	Nivel alto -	6	
M+	Nivel medio +	5	
M	Nivel medio	4	
M-	Nivel medio -	3	
B+	Nivel bajo +	2	
B	Nivel bajo	1	
0	Sin valor apreciable	0	

Fuente: Proyecto Pilar AGRSGA-UNPRG

5.1.4.2.1 Riesgo Potencial

Se denomina riesgo a la medida del daño probable sobre un sistema. Conociendo el impacto de las amenazas sobre los activos, es directo derivar el riesgo sin más que tener en cuenta la probabilidad de ocurrencia.

El riesgo acumulado se calcula para cada activo, por cada amenaza y en cada dimensión de valoración, siendo una función del valor acumulado, la degradación causada y la probabilidad de la amenaza.

Tabla 18: Riesgo Potencial

	[D]	[I]	[C]	[A]	[T]
ACTIVOS	{6,0}	{6,0}	{5,7}	{5,1}	
[S] Servicios	{6,0}	{6,0}	{5,1}	{5,1}	
[gmat] Gestión de Matricula y notas de los alumnos – UNPRG	{6,0}	{6,0}	{5,1}	{5,1}	
[SW] Software	{5,1}	{5,1}	{5,1}	{5,1}	
[sgap] Sistema de Gestión Académica para PreGrado	{5,1}	{5,1}	{5,1}	{5,1}	
[sega] Sistema de Gestión Académica	{5,1}	{5,1}	{5,1}	{5,1}	
[HW] Hardware	{6,0}	{4,4}	{5,1}		
[serv]servidores	{6,0}	{4,4}	{5,1}		
[seap] servidor de aplicaciones	{6,0}	{4,4}	{5,1}		
[sapb] servidor de aplicaciones – backup	{6,0}	{3,9}	{5,1}		
[sebd] servidor de base de datos	{6,0}	{3,9}	{5,1}		
[sapd] servidor de aplicaciones 2	{6,0}	{3,9}	{5,1}		
[sbdo] servidor de base de datos – OCCA	{6,0}	{3,9}	{5,1}		
[srbo] servidor de base de datos- backup –OCCA	{6,0}	{3,9}	{5,1}		
[sacd] servidor Directorio de Usuarios	{6,0}	{4,4}	{5,1}		
[sanv] servidor Antivirus	{6,0}	{3,9}	{5,1}		
[spro] servidor Proxy	{6,0}	{3,9}	{5,1}		
[sred] soporte de la red	{6,0}	{3,9}	{5,1}		
[conm] switch	{6,0}	{3,9}	{5,1}		
[cotf] firewall	{6,0}	{3,9}	{5,1}		
[rout] router	{6,0}	{3,9}	{5,1}		
[COM] Redes de Comunicaciones	{6,0}	{4,4}	{5,1}	{5,1}	
[rlan] red local	{6,0}	{4,4}	{5,1}	{5,1}	
[intr] internet	{6,0}	{4,4}	{5,1}	{5,1}	
[MEDIA] Soportes de Información	{5,1}	{3,4}	{3,9}		
[disk] discos	{5,1}	{3,4}	{3,9}		
[prin] Documentación Impresa	{5,1}	{3,4}	{3,9}		
[AUX] Equipamiento auxiliar	{5,1}	{2,1}	{5,1}		
[upsi]sistemas de alimentación ininterrumpida	{3,0}				
[grue] grupo electrógeno	{3,0}				
[eqcs]equipo de aire acondicionado	{3,0}				
[cabl] cableado	{5,1}	{2,1}	{5,1}		
[clec] cableado eléctrico	{5,1}	{2,1}	{5,1}		
[cart] cableado de red	{5,1}	{2,1}	{5,1}		
[L] Instalaciones	{5,1}	{4,5}	{5,7}		
[sase]Sala de Servidores	{5,1}	{4,5}	{5,7}		
[P] Personal	{5,1}	{5,1}	{5,3}		
[user]Usuarios Finales	{3,9}	{5,1}	{5,3}		
[admc] administrador de comunicaciones y seguridad	{5,1}	{3,9}	{5,1}		

Fuente: Proyecto Pilar AGRSGA-UNPRG

5.1.4.2.2 Riesgo Residual

Dado un cierto conjunto de salvaguardas desplegadas y una medida de la madurez de su proceso de gestión, el sistema queda en una situación de riesgo que se denomina residual. Se dice que hemos modificado el riesgo, desde un valor potencial a un valor residual. El cálculo del riesgo residual es sencillo. Como no han cambiado los activos, ni sus dependencias, sino solamente la magnitud de la degradación y la probabilidad de las amenazas, se repiten los cálculos de riesgo usando el impacto residual y la probabilidad residual de ocurrencia.

La magnitud de la degradación se toma en consideración en el cálculo del impacto residual.

Tabla 19: Riesgo Residual

	[D]	[I]	[C]	[A]	[T]
ACTIVOS	{5,2}	{3,8}	{4,3}	{4,3}	
[S] Servicios	{5,1}	{3,8}	{3,8}	{3,8}	
[gmat] Gestión de Matricula y notas de los alumnos – UNPRG	{5,1}	{3,8}	{3,8}	{3,8}	
[SW] Software	{4,3}	{3,8}	{3,8}	{3,8}	
[sgap] Sistema de Gestión Académica para PreGrado	{4,3}	{3,8}	{3,8}	{3,8}	
[sega] Sistema de Gestión Académica	{4,3}	{3,8}	{3,8}	{3,8}	
[HW] Hardware	{5,2}	{3,1}	{4,3}		
[serv]servidores	{5,2}	{3,1}	{4,3}		
[seap] servidor de aplicaciones	{5,2}	{2,2}	{3,5}		
[sapb] servidor de aplicaciones – backup	{5,2}	{1,7}	{3,5}		
[sebd] servidor de base de datos	{5,2}	{1,7}	{3,5}		
[sapd] servidor de aplicaciones 2	{5,2}	{1,7}	{3,5}		
[sbdo] servidor de base de datos – OCCA	{5,2}	{1,7}	{3,5}		
[srbo] servidor de base de datos- backup –OCCA	{5,2}	{1,7}	{3,5}		
[sacd] servidor Directorio de Usuarios	{4,5}	{3,1}	{4,3}		
[sanv] servidor Antivirus	{4,5}	{3,1}	{4,3}		
[spro] servidor Proxy	{4,5}	{3,1}	{4,3}		
[sred] soporte de la red	{5,2}	{3,1}	{4,3}		
[conm] switch	{5,2}	{3,1}	{4,3}		
[cotf] firewall	{5,2}	{3,1}	{4,3}		
[rout] router	{5,2}	{3,1}	{4,3}		
[COM] Redes de Comunicaciones	{3,6}	{3,1}	{4,3}	{4,3}	
[rlan] red local	{3,6}	{3,1}	{4,3}	{4,3}	
[intr] internet	{3,6}	{3,1}	{4,3}	{4,3}	
[MEDIA] Soportes de Información	{2,9}	{1,2}	{1,7}		
[disk] discos	{2,9}	{1,2}	{1,7}		
[prin] Documentación Impresa	{2,9}	{1,2}	{1,7}		
[AUX] Equipamiento auxiliar	{4,3}	{1,3}	{4,3}		
[upsi]sistemas de alimentación ininterrumpida	{2,1}				
[grue] grupo electrógeno	{2,1}				
[eqcs]equipo de aire acondicionado	{2,1}				
[cabl] cableado	{4,3}	{1,3}	{4,3}		
[clec] cableado eléctrico	{4,3}	{1,3}	{4,3}		
[cart] cableado de red	{4,3}	{1,3}	{4,3}		
[L] Instalaciones	{4,1}	{2,0}	{3,2}		
[sase]Sala de Servidores	{4,1}	{2,0}	{3,2}		
[P] Personal	{2,6}	{2,7}	{2,8}		
[user]Usuarios Finales	{1,4}	{2,7}	{2,8}		
[admc] administrador de comunicaciones y seguridad	{2,6}	{1,4}	{2,6}		

Fuente: Proyecto Pilar AGRSGA-UNPRG

5.1.4.3 Interpretación de los resultados

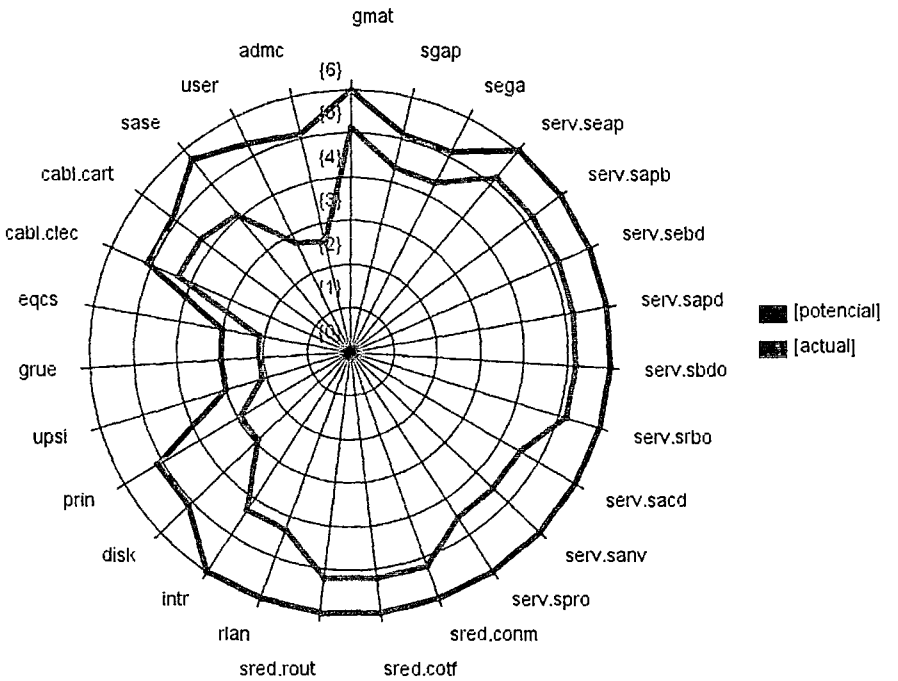

Figura 13: Identificación de riesgos por activo.
Fuente: Proyecto Pilar AGRSGA-UNPRG

En la figura se observa, el resultado de todas las actividades que se trabajan sobre los activos, las amenazas y las salvaguardas. Como indica la leyenda, la línea de color rojo son los riesgos que están expuestos los activos, en la siguiente etapa representaba por la línea color azul es el resultado de la aplicación de las salvaguardas existentes, teniendo en consideración que se maximiza la presencia de amenazas para realizar un estudio de la situación actual que se encuentra el objeto de estudio. Los activos con los niveles más altos son sin duda alguna los servidores principales que participan en la generación del servicio de los sistemas de gestión académica y equipos de comunicación de redes.

5.2 Proceso de Gestión de Riesgos

Realizado ya el método de análisis de riesgos se obtiene los resultados del impacto y riesgo que están expuestos los activos. Una calificación de cada riesgo significativo, determinándose si:

1. Es **crítico** en el sentido de que requiere atención urgente
2. Es **grave** en el sentido de que requiere atención
3. Es **apreciable** en el sentido de que pueda ser objeto de estudio para su tratamiento
4. Es **asumible** en el sentido de que no se van a tomar acciones para atajarlo

La opción 4, aceptación del riesgo, siempre es arriesgada y hay que tomarla con prudencia y justificación. Las razones que pueden llevar a esta aceptación son:

. cuando el impacto residual es asumible

. cuando el riesgo residual es asumible

. cuando el coste de las salvaguardas oportunas es desproporcionado en comparación al impacto y riesgo residuales

La calificación de los riesgos tendrá consecuencias en las tareas subsiguientes, siendo un factor básico para establecer la prioridad relativa de las diferentes actuaciones.

5.2.1 Toma de Decisiones

5.2.1.1 Identificación de riesgos críticos

Se selecciona a los activos que poseen un nivel de riesgo mayor, con lo cual se sustenta el tema de estudio planteado en la presente tesis, la siguiente tabla se muestran.

Tabla 20: Identificación de riesgos críticos (actual)

	[D]	[I]	[C]
[HW] Hardware	{5,2}	{3,1}	{4,3}
[serv]servidores	{5,2}	{3,1}	{4,3}
[seap] servidor de aplicaciones	{5,2}	{2,2}	{3,5}
[sapb] servidor de aplicaciones – backup	{5,2}	{1,7}	{3,5}
[sebd] servidor de base de datos	{5,2}	{1,7}	{3,5}
[sapd] servidor de aplicaciones 2	{5,2}	{1,7}	{3,5}
[sbdo] servidor de base de datos – OCCA	{5,2}	{1,7}	{3,5}
[srbo] servidor de base de datos- backup –OCCA	{5,2}	{1,7}	{3,5}
[sred] soporte de la red	{5,2}	{3,1}	{4,3}
[conm] switch	{5,2}	{3,1}	{4,3}
[cotf] firewall	{5,2}	{3,1}	{4,3}
[rout] router	{5,2}	{3,1}	{4,3}

Fuente: Proyecto Pilar AGRSGA-UNPRG

5.2.1.2 Calificación del riesgo

Se gestiona a los activos con riesgos críticos.

En la tarea anterior se identificaron los activos, como están organizados en grupos: servidores y soporte de la red.

Los servidores presentan valor de riesgo acumulado similar, los soportes de red también presentan amenazas similares con alto riesgo acumulado, por lo cual se generaliza indicando en los casos necesarios la diferencia en aplicar la salvaguarda, las salvaguardas ordenadas de mayor valor de riesgo a menor son:

[E.24]Caída del sistema por agotamiento de recursos

En el caso de los servidores de aplicaciones y base de datos, no es suficiente con los servidores de soporte y el control de acceso, por la gran cantidad de solicitudes de acceso a la vez.

El soporte de la red, incluye a 3 activos, a pesar de no presentarse las amenazas con mucha frecuencia su impacto es alto.

La medida que debe tomarse para mejorar la salvaguardas implantada son:

- ✓ La migración de los sistemas a otros servidores con mayor capacidad y mejor tecnología.

- ✓ La verificación del correcto funcionamiento de los sistemas de gestión académica.
- ✓ Configuración de los equipos adecuadamente para que no se presente problemas de conexión o de modificación de datos.

[I.5]Avería de origen físico o lógico
En ambos casos mantener los equipos organizados y ubicados en zonas adecuadas, de tal que no puedan sufrir accidente por caída, golpe, etc.

[A.26]Ataque destructivos
La amenazas con un valor bajo en posibilidad de presentarse, pero al ser así su impacto es alto, las medidas a tomar son la mejora en la seguridad de donde se encuentren los activos.

[I.6]Corte del suministro eléctrico
Es una amenaza con una alta posibilidad que se presente, a pesar de ello no depende al 100% de la Universidad, porque se puede dar por problemas de parte de la empresa eléctrica.
Las medidas son:

- Mantener en buen estado las conexiones eléctricas.
- Adquirir un generador eléctrico más para prolongar las horas de soporte de fluido eléctrico en caso de pérdida o fallo del servicio eléctrico.

[I.7]Condiciones inadecuadas de temperatura o humedad
En caso de los activos con mayor grado de riesgos, todos están ubicados en la sala de servidores, por lo cual las medidas deben darse sobre el ambiente, como la adquisición de un nuevo sistema de climatización para remplazar o apoyar al actualmente instalado.

[A.25]Robo de equipos y [E.25] Perdida de equipos
Son amenazas que se califican con un valor medio de posibilidades que ocurra, a pesar que son casos poco probables, se considera así por el alto grado de impacto sobre los activos. En este caso también las medidas a tomar son: mejorar seguridad en la sala de servidores.

[A.11]Acceso no autorizado y [A.6] Abuso de privilegios de acceso
Son amenazas que involucran a los usuarios, la forma que utilizan el acceso, privilegios o restricciones que se les asignan. Las medidas a tomar son: generar concientización sobre el adecuado uso del acceso y el cuales son su pro y sus contras.

[A.23]Manipulación del hardware y [E.23] Errores de mantenimiento – hardware
Son amenazas que al presentarse involucran directamente la encargado, como primera opción que sería una actividad mal hecha por el encargado o los

practicantes, o la intromisión de alguna otra persona que busca dañar o comprometer el estado físico de los equipos. Las medias a tomar son:

- La importancia en la seguridad de la sala de servidores
- La concientización y el monitoreo de las labores realizadas con los equipos.

[E.2]Errores del administrador del sistema/ seguridad

Esta amenaza se considera con una baja posibilidad que ocurra, las medidas a tomar son:

- Mantener los procesos a realizar optimizados o anotados, de tal forma que se puedan estandarizar.

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

Para los activos escogidos, como se encuentran ubicados en la sala de servidores, las medidas de seguridad se deben tomar frente a los desastres generados por la naturaleza o mano del hombre son:

- Establecer un plan de seguridad frente a desastres naturales.
- Planear actividades de prevención frente a accidentes ocasionados en la sala de servidores.

5.2.2 Elaboración del plan de mitigación

El plan de mitigación, es una actividad del proceso de Gestión de Riesgos, que menciona las decisiones que se van realizando en la mejora de la seguridad, en un determinado tiempo para un caso específico.

5.2.2.1 Plan de mitigación

El plan de mitigación, es una de las tareas que tienen como objetivo principal ordenar en un rango de los impactos y/o riesgos que se van a mitigar, con una prioridad relevante a los activos que se encuentren en una situación crítica, como también la disponibilidad del personal para la implementación y ejecución de la tarea de dicho plan.

El plan de mitigación, tiene que basarse en los perfiles de seguridad que recomienda la metodología Magerit, para conseguir una mitigación del impacto y/o riesgo de manera secuencial y completa.

Valoración según el Código de buenas prácticas para la Gestión de la Seguridad de la Información

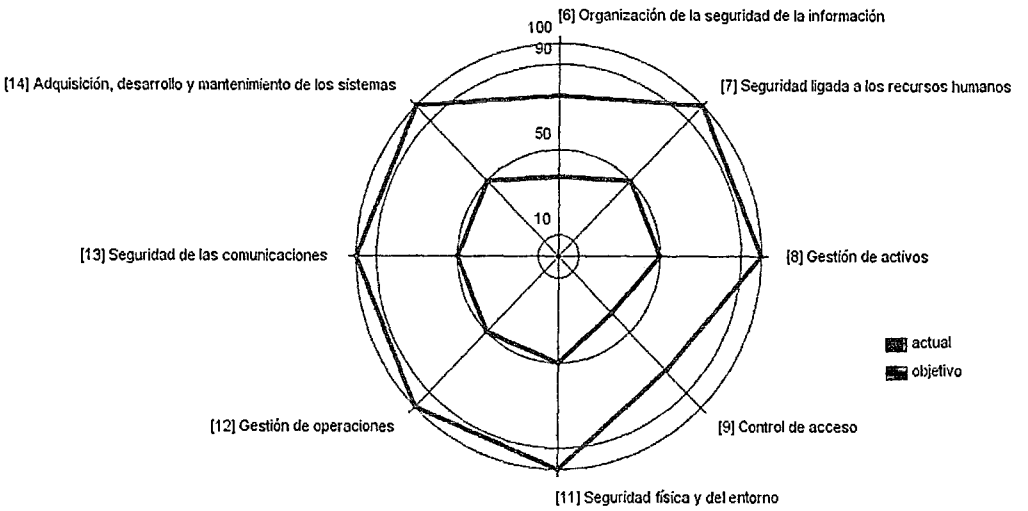

Figura 14: Gestión de seguridad
Fuente: Proyecto Pilar AGRSGA-UNPRG

En la elaboración del plan de mitigación, se consideran los siguientes aspectos, los activos a tratar. Acciones y cronogramas.

Activos

Para el plan de mitigación, se lista a los activos que se van a mitigar en sus correspondientes planes de seguridad, para el desarrollo se incluyen casi todos los activos, principalmente con que involucran directamente con el objetivo de estudio que es la seguridad en los servidores.

Acciones

Hace referencia a planes de seguridad, perfiles de seguridad, controles de seguridad y quien es el responsable de dichas acciones.

Cronograma

Se estima un tiempo aproximado de la duración de la implementación o terminación de las actividades, planes o controles.

Aspectos

Como objetivo se busca mitigar riesgos, para mejorar la seguridad sobre los servidores de los sistemas de gestión académica.

El plan de mitigación tiene 4 aspectos generales aceptados por la gerencia de la institución:

- Evitación: para eliminar las condiciones que permiten que el riesgo este presente en todos los activos.
- Aceptación: reconocer la existencia de los riesgos, pero no tomar ninguna acción para resolverla, a excepción del desarrollo posible de los planes de contingencia.

- Mitigación: para reducir al mínimo la probabilidad de una ocurrencia del riesgo o el impacto.
- Desviación: para transferir el riesgo parcial o total a otra organización, individuo o entidad, si el caso lo diera.

Con los elementos mencionados se procede a elaborar el Plan de Mitigación.

Activos	Acciones	Tiempo Aproximado
[gmat] Gestión de Matricula y notas de los alumnos – UNPRG	Plan de contingencia del servicio de gestión académica	10 meses
[seap] servidor de aplicaciones	Plan de evaluación del desempeño de las instalaciones y equipamiento	7 meses
[sapb] servidor de aplicaciones – backup		
[sebd] servidor de base de datos		
[sapd] servidor de aplicaciones 2		
[sbdo] servidor de base de datos – OCCA		
[srbo] servidor de base de datos- backup –OCCA		
[conm] switch		
[cotf] firewall		
[rout] router		
[rlan] red local		
[intr] internet		
[upsi]sistemas de alimentación ininterrumpida		
[grue] grupo electrógeno		
[eqcs]equipo de aire acondicionado		
[clec] cableado eléctrico		
[cart] cableado de red		
[sase]Sala de Servidores		
[user]Usuarios Finales		
[admc] administrador de comunicaciones y seguridad		
[seap] servidor de aplicaciones	Plan de contingencia de las instalaciones y equipamiento	6 meses
[sapb] servidor de aplicaciones – backup		
[sebd] servidor de base de datos		
[sapd] servidor de aplicaciones 2		
[sbdo] servidor de base de datos – OCCA		
[srbo] servidor de base de datos- backup –OCCA		
[sacd] servidor Directorio de Usuarios		
[sanv] servidor Antivirus		
[spro] servidor Proxy		
[conm] switch		
[cotf] firewall		
[rout] router		
[rlan] red local		
[intr] internet		
[upsi]sistemas de alimentación ininterrumpida		

[grue] grupo electrógeno [eqcs]equipo de aire acondicionado [clec] cableado eléctrico [cart] cableado de red [sase]Sala de Servidores		
[seap] servidor de aplicaciones [sapb] servidor de aplicaciones – backup [sebd] servidor de base de datos [sapd] servidor de aplicaciones 2 [sbdo] servidor de base de datos – OCCA [srbo] servidor de base de datos- backup –OCCA [sacd] servidor Directorio de Usuarios [sanv] servidor Antivirus [spro] servidor Proxy [conm] switch [cotf] firewall [rout] router [rlan] red local [intr] internet [upsi]sistemas de alimentación ininterrumpida [grue] grupo electrógeno [eqcs]equipo de aire acondicionado [clec] cableado eléctrico [cart] cableado de red [sase]Sala de Servidores [user]Usuarios Finales [admc] administrador de comunicaciones y seguridad	Plan de recuperación de las instalaciones y equipamiento	5 meses
[user]Usuarios Finales [admc] administrador de comunicaciones y seguridad	Plan de concientización y formación de los usuarios	2 meses
[seap] servidor de aplicaciones [sapb] servidor de aplicaciones – backup [sebd] servidor de base de datos [sapd] servidor de aplicaciones 2 [sbdo] servidor de base de datos – OCCA [srbo] servidor de base de datos- backup –OCCA	Procedimientos de seguridad en los servidores	7 meses
[seap] servidor de aplicaciones [sapb] servidor de aplicaciones – backup [sebd] servidor de base de datos [sapd] servidor de aplicaciones 2 [sbdo] servidor de base de datos – OCCA [srbo] servidor de base de datos- backup –OCCA [sacd] servidor Directorio de Usuarios [sanv] servidor Antivirus [spro] servidor Proxy	Procedimientos de control de acceso	3 meses

[conm] switch		
[cotf] firewall		
[rout] router		
[rlan] red local		
[intr] internet		
[sgap] Sistema de Gestión Académica para Pre-Grado	Procedimientos de verificación y monitoreo del acceso a los sistemas de gestión académica	5 meses
[sega] Sistema de Gestión Académica		
[spro] servidor Proxy		
[conm] switch		
[cotf] firewall		
[rout] router		
[rlan] red local		
[intr] internet		

Cuadro 14 : Plan de Mitigación
Fuente: Elaborado por el Autor.

La implementación del plan de mitigación, reduce los riesgos y se muestran en la siguiente figura. La línea de color verde lo representa.

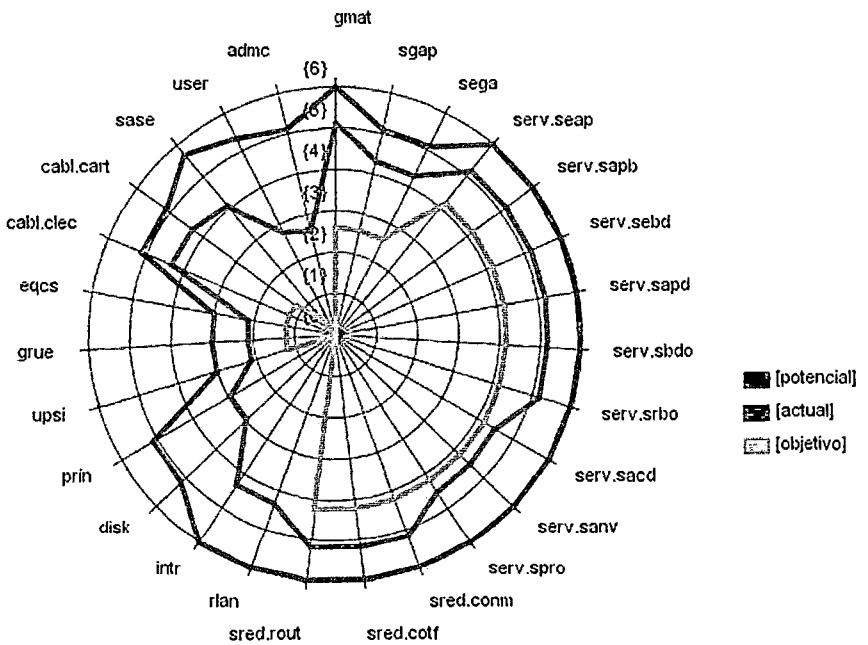

Figura 15: Riesgo Residual - Aplicación del plan de mitigación
Fuente: Proyecto Pilar AGRSGA-UNPRG

CAPITULO VI:
COSTOS Y BENEFICIOS

CAPITULO VI: COSTOS Y BENEFICIOS

6.1 Análisis de Costos

6.1.1 Costo de Software

Tabla 21: costos de software

Descripción	Costos
Windows 7 profesional	S/. 200.00
Office 2010	S/. 250.00
Manuales de la metodología MAGERIT	S/. 0.00
Herramienta Pilar	S/. 600
Total	**S/. 1 050.00**

Fuente: Elaborada Por El Autor

6.1.2 Costo de Personal

Tabla 22: Costo de Personal

Descripción	Costo x mes	Costo total(s/.).
Experto MAGERIT y PILAR	S/. 1,200.00	S/. 7,200.00
Capacitaciones	S/. 200.00	S/. 1,200.00
Analista	S/. 1 000.00	S/. 6 000.00
Total	**S/. 14 400.00 (6 meses aprox)**	

Fuente: Elaborada Por El Autor

6.1.3 Costo de Servicios

Tabla 23: Costo de Servicios

Descripción	Costo(s/.)
Transporte	S/. 1,400.00
Alimentos	S/. 750.00
Impresiones	S/. 140.00
Fotocopias	S/. 70.00
Internet y energía eléctrica	S/. 1,200.00
Espiralados	S/. 30.00
Encuadernados	S/. 60.00
Otros	S/. 100.00
Total	**S/. 3 750.00**

Fuente: Elaborada Por El Autor

6.1.4 Costo de Materiales

Tabla 24: Costo de Materiales

Descripción	Cantidad	Costo(s/.)
Papel bond A4	10 cientos	S/. 40.00
Lapiceros y lápices	6 unidades c/u	S/. 36.00
Folders	12 unidades	S/. 6.00
Sobre manila A4	12 unidades	S/. 6.00
Borrador	1 unidades	S/. 1.00
Engrapador	1 unidad	S/. 8.00
Perforador	1 unidad	S/. 8.00
Corrector	2 unidades	S/. 6.00
CD y DVD	12 unidades	S/. 12.00
Otros		S/. 20.00
Total	**S/. 143.00**	

Fuente: Elaborada Por El Autor

6.1.5 Costos de Hardware

Tabla 25: Costos de Hardware

Descripción	Costo(s/.)
Computadora (depreciación 25%)	S/. 900.00
Otros	S/. 200.00
Total	**S/. 1 100.00**

Fuente: Elaborada Por El Autor

6.1.6 Resumen de Costos

Tabla 26: Resumen de Costos

Concepto	Costo(s/.)
COSTO DE SOFTWARE	S/. 1 050.00
COSTO DE PERSONAL	S/. 14 400.00
COSTO DE SERVICIOS	S/. 3 750.00
COSTO DE MATERIALES	S/. 143.00
COSTOS DE HARDWARE	S/. 1 100.00
Total	**S/. 20 443.00**

Fuente: Elaborada Por El Autor

Un presupuesto aproximado de S/. 20 500.00 para la realización del proyecto de tesis en mención

6.2 Análisis de Viabilidad

Para el cálculo, se recurrió a una herramienta de análisis de viabilidad de Microsoft Office Excel con una macro ya dimensionado para el análisis de rentabilidad de proyectos.

6.3.1 Valor Actual Neto (VAN)

El valor actual neto consta de un procedimiento que permite calcular el valor presente de un determinado número de flujos de caja futuros, originados por una inversión.

La fórmula del V.A.N:

$$VAN = -I + \sum_{n=1}^{j} \frac{FNE}{(1+i)^n}$$

Dónde:

I: Inversión inicial

FNE: flujo neto de efectivo proyectado / año

j: vida útil del proyecto

i: tasa de descuento

n: periodo

Para hallar el VAN para la tesis se utilizan los siguientes datos:

n: 3, Considerando el tiempo de utilidad de 3 años, por el cambio y actualización constante de las tecnologías.

i: 10%

Tabla 27: Flujo Neto Efectivo Proyectado

DETALLE	PERIODOS ANUALES			
	0	1	2	3
FLUJO NETO DE EFECTIVO PROYECTADO	S/. 20,500.00	S/. 11,550.00	S/. 12,100.00	S/. 14,570.00

Fuente: elaborado por el Autor

Tabla 28: Valor Actual Neto (VAN)

n	FNE	$(1+i)^2$	FNE / $(1+i)^2$
0	-S/. 20,500.00		S/. 20,500.00
1	S/. 11,550.00	1.10	S/. 10,500.00
2	S/. 12,100.00	1.21	S/. 10,000.00
3	S/. 14,570.00	1.33	S/. 10,946.66
Total			S/. 10,946.66

Fuente: Elaborada por el Autor

Utilizando la formula el VAN=10,946.66

El VAN es mayor a 0 por lo cual la inversión es factible

6.3.2 Tasa Interna de Rentabilidad

Corresponde a aquella tasa de descuento que hace que el VAN del proyecto sea exactamente igual a cero.

La fórmula del T.I.R.:

$$0 = \sum_{n=1}^{j} \frac{FNE}{(1+tir)^n} - I$$

Dónde:

I: Inversión inicial

FNE: flujo neto de efectivo proyectado / año

j: número de periodo

tir: tasa interna de rentabilidad (TIR)

n: periodo

Para hallar el TIR en la presente Tesis, se consideran los mismos datos para hallar el VAN con la diferencia que se halla la tasa de rentabilidad.

TIR= 37.16%, el TIR encontrado es mayor a la tasa inicial de 10%, el proyecto es factible.

6.3.3 Periodo de Recuperación

Corresponde al periodo de tiempo necesario para que el flujo de caja acumulado del proyecto cubra el monto total de la inversión realizada.

La fórmula del P.R.:

$$0 = \sum_{n=1}^{pr} \frac{FNE}{(1+k)^n}$$

Dónde:

FNE: flujo neto de efectivo proyectado / año

pr: periodo de recuperación

k: tasa interna de rentabilidad (TIR)

n: periodo

Utilizando los datos anteriores en la formula, se obtiene que en dos años se recupera la inversión realizada. La realización de la tesis es factible.

6.3 Beneficios

- Un plan de mitigación que al implementarlo reduce el riego sobre los servidores mejorando así el servicio de gestión académica.
- La identificación de los riesgos que están expuestos los sistemas de gestión académica, los servidores, los equipos auxiliares, de redes de comunicación, la sala de servidores.
- El aprendizaje y aplicación de la metodología Magerit y la herramienta Pilar.

CAPITULO VII:
CONCLUSIONES

CAPITULO VII: CONCLUSIONES

- Los Servidores de los sistemas de Gestión Académica tienen medidas de seguridad implementadas, pero no se encuentran ni guiadas y documentados, y no son adecuadamente aprovechadas, por lo cual este estudio será beneficioso para reducir, minimizar o contrarrestar riesgos.

- La metodología Magerit y la herramienta Pilar aportan gran ayuda al momento del análisis y gestión de riesgos, para el desarrollo de la presente Tesis se adaptó el esquema de desarrollo de la metodología con el esquema de desarrollo del Proyecto. Durante el desarrollo se fue trabajando con la metodología Magerit y la herramienta Pilar a la par , por motivos de entendimiento no se incluyó la captura de pantallazos en el capítulo de aplicación pero si en los anexos como referencia al desarrollo en la Herramienta Pilar.

- Como resultado de la aplicación de la Metodología Magerit y Herramienta Pilar, se concluye que los servidores están expuestos a un riesgo critico mediante amenazas como: Caída del sistema por agotamiento de recursos, Avería de origen físico o lógico, Corte del suministro eléctrico, Condiciones inadecuadas de temperatura o humedad, Robo de equipos, Perdida de equipos, errores del administrador del sistema/ seguridad, Desastres naturales, a pesar de las medidas ya tomadas por la administración del área de red-telemática. Lo cual sustenta la problemática expuesta y la importancia del desarrollo de la temática. los servidores permiten la funcionalidad y generación del servicio de gestión académica.

- La elaboración de un Plan de Mitigación se realizó tomando en cuenta factores de seguridad, la importancia de la seguridad en los activos y los servidores de los sistemas de gestión académica como principal objeto de estudio.

- Se determina un aproximado a s/.20.500 nuevos soles, el costo de la aplicación de la metodología Magerit y la herramienta Pilar, en los servidores de gestión académica y su entorno. a través de un análisis de viabilidad se determina que la realización del proyecto es factible.

CAPITULO VIII:
RECOMENDACIONES

CAPITULO VIII: RECOMENDACIONES

- Se recomienda tomar en consideración la problemática y la situación actual que se encuentran los servidores de los sistemas de gestión académica.

- Se recomienda incluir la enseñanza, aplicación e implementación de la metodología Magerit u otras metodologías que involucran el análisis, gestión, monitores de la seguridad informática.

- Se recomienda poner bajo control las diferentes amenazas principalmente las que presentan un alto valor de riesgo, como la caída del sistema por agotamiento de recursos que es muy recurrente y aquellas que dañan o degradan a los servidores de los sistemas de gestión académica.

- La ejecución de un Plan de Mitigación se debe realizar lo más próximo a su elaboración, y realizarse un nuevo estudio cada determinado tiempo ya que las amenazas y salvaguardas son cambiantes con el paso del tiempo.

- Se recomienda desarrollar y ejecutar proyectos de similar envergadura, por la importancia que conlleva la seguridad informática.

CAPITULO IX:
REFERENCIAS BIBLIOGRÁFICAS

CAPITULO IX: REFERENCIAS BIBLIOGRÁFICAS

ESPINOZA , A., COLLAGUAZO, D., & ROLDAN, F. (2012). Centro De Gestión De Riesgos Para Monitoreo De Redes, En La Facultad De Ingeniería, Ciencias Físicas Y Matemáticas . QUITO, ECUADOR.

Ferrero Recaséns, E. (2006). ANÁLISIS Y GESTIÓN DE RIESGOS DEL SERVICIO IMAT DEL SISTEMA DE NFORMACIÓN DE I.C.A.I. Madrid, España.

Gaona Vásquez, K. d. (2013). APLICACIÓN DE LA METODOLOGÍA MAGERIT PARA EL ANÁLISIS Y GESTIÓN DE RIESGOS DE LA APLICADO A LA EMPRESA PESQUERA E INDUSTRIAL BRAVITO S.A. EN LA CIUDAD DE MACHALA. Cuenca, Ecuador.

Marquina Llivisaca, E. G. (21 de 10 de 2010). Análisis y gestión de riesgos para el servidor RADIUS del laboratorio de la Facultad de Ingeniería de Sistemas. Quito, Eduador: QUITO/EPN/2010.

Gobierno de España – ministerio de hacienda y relaciones públicas. Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica. (2012). MAGERIT - V3 METODOLOGIA DE ANALISIS Y GESTION DE RIESGOS DE LOS SISTEMAS DE INFORMACION. LIBRO I : METODO. ESPAÑA.

Gobierno de España – ministerio de hacienda y relaciones públicas. Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica. (2012). MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro II - Catálogo de Elementos. ESPAÑA.

Gobierno de España – ministerio de hacienda y relaciones públicas. Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica. (2012). MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro III: Guía de Técnicas. ESPAÑA.

Magerit - Libro_II_catalogo. (s.f.). Recuperado el 2015, de www.ccn-cert.cni.es/publico/herramientas/pilar5/magerit/ Libro_II_catalogo.pdf

Magerit - Libro_III_tecnicas. (s.f.). Recuperado el 2015, de www.ccn-cert.cni.es/publico/herramientas/pilar5/magerit /Libro_III_tecnicas.pdf

Magerit Libro_I_metodo. (s.f.). Recuperado el 2015, de www.ccn-cert.cni.es/publico/herramientas/pilar5 /magerit/Libro_I_metodo.pdf

Manual de pilar. (s.f.). Recuperado el 2014 - 2015, de www.pilar-tools.com/es/index.html?tools/pilar/index.html

seguridadinformaticaufps.wikispaces.com. (s.f.). Recuperado el 2014-2015, de seguridadinformaticaufps.wikispaces.com/PILAR+-+Herramienta+para+An%C3%A1lisis+y+Gesti%C3%B3n+de+Riesgos

www.ccn-cert.cn. (s.f.). Recuperado el 2014-2015, de www.ccn-cert.cni.es/index.php?option=com_wrapper&view= wrapper&Itemid=213&lang=es

CAPITULO X:
ANEXOS

CAPITULO X: ANEXOS

10.1 Glosario

- ✓ **ACTIVO:**
  Componente o funcionalidad de un sistema de información susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización. Incluye: información, datos, servicios, aplicaciones (software), equipos (hardware), comunicaciones, recursos administrativos, recursos físicos y recursos humanos.

- ✓ **AMENAZA:**
  Causa potencial de un incidente que puede causar daños a un sistema de información o a una organización.

- ✓ **ANÁLISIS DE RIESGOS:**
  Proceso sistemático para estimar la magnitud de los riesgos a que está expuesta una Organización. Identificación de las amenazas que acechan a los distintos componentes pertenecientes o relacionados con el sistema de información (conocidos como 'activos'); para determinar la vulnerabilidad del sistema ante esas amenazas y para estimar el impacto o grado de perjuicio que una seguridad insuficiente puede tener para la organización, obteniendo cierto conocimiento del riesgo que se corre.

- ✓ **ATAQUE:**
  Intento de destruir, exponer, alterar o inhabilitar un sistema de información o la información que el sistema maneja, o violar alguna política de seguridad de alguna otra manera.

- ✓ **AUDITORÍA DE SEGURIDAD:**
  Estudio y examen independiente del historial y actividades de un sistema de información, con la finalidad de comprobar la idoneidad de los controles del sistema, asegurar su conformidad con la estructura de seguridad y procedimientos operativos establecidos, a fin de detectar brechas en la seguridad y recomendar cambios en los procedimientos, controles y estructuras de seguridad.

- ✓ **AUTENTICIDAD:**
  Propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos. Contra la autenticidad de la información podemos tener manipulación del origen o el contenido de los datos. Contra la autenticidad de los usuarios de los servicios de acceso, podemos tener suplantación de identidad.

- ✓ **CONFIDENCIALIDAD:**
  Que la información llegue solamente a las personas autorizadas. Contra la confidencialidad o secreto pueden darse fugas y filtraciones de información, así como accesos no autorizados.

- ✓ **DISPONIBILIDAD:**
  Disposición de los servicios a ser usados cuando sea necesario. La carencia de disponibilidad supone una interrupción del servicio. La disponibilidad afecta directamente a la productividad de las organizaciones.

- ✓ **ESTADO DE RIESGO:**
  Caracterización de los activos por su riesgo residual; es decir, por lo que puede pasar teniendo en cuenta las salvaguardas desplegadas.

- ✓ **EVALUACIÓN DE SALVAGUARDAS:**
  Evaluación de la eficacia de las salvaguardas existentes en relación al riesgo que afrontan.

- ✓ **GESTIÓN DE RIESGOS:**
  Actividades coordinadas para dirigir y controlar una organización. Selección e implantación de salvaguardas para conocer, prevenir, impedir, reducir o controlar los riesgos identificados. Selección e implantación de las medidas o 'salvaguardas' de seguridad adecuadas para conocer, prevenir, impedir, reducir o controlar los riesgos identificados y así reducir al mínimo su potencialidad o sus posibles perjuicios. La gestión de riesgos se basa en los resultados obtenidos en el análisis de los riesgos.

- ✓ **INTEGRIDAD**
  Mantenimiento de las características de completitud y corrección de los datos. Contra la integridad, la información puede aparecer manipulada, corrupta o incompleta. La integridad afecta directamente al correcto desempeño de las funciones de una Organización.

- ✓ **MAPA DE RIESGOS**
  Relación de las amenazas a que están expuestos los activos.

- ✓ **MODELO DE VALOR**
  Caracterización del valor que representan los activos para la Organización así como de las dependencias entre los diferentes activos.

- ✓ **PLAN DE SEGURIDAD**
  Conjunto de proyectos de seguridad que permiten materializar las decisiones de gestión de riesgos.

- ✓ **PROYECTO DE SEGURIDAD**
  Agrupación de tareas orientadas a tratar el riesgo del sistema. La agrupación se realiza por conveniencia.

- ✓ **RIESGO**
  Estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la Organización. Efecto de la incertidumbre sobre la consecución de los objetivos

- ✓ **SALVAGUARDA:**
  Procedimiento o mecanismo tecnológico que reduce el riesgo.

- ✓ **SEGURIDAD:**
  La capacidad de las redes o de los sistemas de información de resistir, con un determinado nivel de confianza, los accidentes o acciones ilícitas o malintencionadas que comprometan la disponibilidad, autenticidad, integridad y confidencialidad de los datos almacenados o transmitidos y de los servicios que dichas redes y sistemas ofrecen o hacen accesibles.
- ✓ **SEGURIDAD DE LA INFORMACIÓN:**
  Confianza en que los sistemas de información están libres y exentos de todo peligro o daño inaceptables.

- ✓ **TRAZABILIDAD:**
  Aseguramiento de que en todo momento se podrá determinar quién hizo qué y en qué momento. La trazabilidad es esencial para analizar los incidentes, perseguir a los atacantes y aprender de la experiencia. La trazabilidad se materializa en la integridad de los registros de actividad.

10.2 Fichas de recojo de datos

Cuadro 15: Fichas de recojo de datos

[D] Datos /Información
[files] ficheros [backup] copias de respaldo [conf] datos de configuración (1) [int] datos de gestión interna [password] credenciales (ej. contraseñas) [auth] datos de validación de credenciales [acl] datos de control de acceso [log] registro de actividad (2) [source] código fuente [exe] código ejecutable [test] datos de prueba
1. Los datos de configuración son críticos para mantener la funcionalidad de las partes y del conjunto del sistema de información. 2. Los registros de actividad sustancian los requisitos de trazabilidad.
[S] Servicios
[anon] anónimo (sin requerir identificación del usuario) [pub] al público en general (sin relación contractual) [ext] a usuarios externos (bajo una relación contractual) [int] interno (a usuarios de la propia organización) [www] world wide web

[telnet] acceso remoto a cuenta local [email] correo electrónico
[file] almacenamiento de ficheros
[ftp] transferencia de ficheros
[edi] intercambio electrónico de datos
[dir] servicio de directorio (1)
[idm] gestión de identidades (2)
[ipm] gestión de privilegios
[pki] PKI - infraestructura de clave pública (3)

1. Localización de personas (páginas blancas), empresas o servicios (páginas amarillas); permitiendo la identificación y facilitando los atributos que caracterizan al elemento determinado.
2. Servicios que permiten altas y bajas de usuarios de los sistemas, incluyendo su caracterización y activando los servicios de aprovisionamiento asociados a sus cambios de estado respecto de la organización.
3. Servicios asociados a sistemas de criptografía de clave pública, incluyendo especialmente la gestión de certificados.

[SW]Aplicaciones (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
- [file] servidor de ficheros
- [dbms] sistema de gestión de bases de datos
- [tm] monitor transaccional
- [office] ofimática
- [av] anti virus
- [os] sistema operativo
- [hypervisor] gestor de máquinas virtuales
- [ts] servidor de terminales
- [backup] sistema de backup

HW] Equipos informáticos (hardware)

[host] grandes equipos (1)
[mid] equipos medios (2)
[pc] informática personal (3)
[mobile] informática móvil (4)
[pda] agendas electrónicas
[vhost] equipo virtual
[backup] equipamiento de respaldo (5)
[peripheral] periféricos
- [print] medios de impresión (6)
- [scan] escáneres
- [crypto] dispositivos criptográficos

[bp] dispositivo de frontera (7)
[network] soporte de la red (8)
- [modem] módems
- [hub] concentradores
- [switch] conmutadores
- [router] encaminadores
- [bridge] pasarelas
- [firewall] cortafuegos
- [wap] punto de acceso inalámbrico

[pabx] centralita telefónica
[ipphone] teléfono IP

Se caracterizan por haber pocos, frecuentemente uno sólo, ser económicamente gravosos y requerir un entorno específico para su operación. Son difícilmente reemplazables en caso de destrucción.

1. Se caracterizan por haber varios, tener un coste económico medio tanto de adquisición como de mantenimiento e imponer requerimientos estándar como entorno de operación. No es difícil reemplazarlos en caso de destrucción.
2. Se caracterizan por ser multitud, tener un coste económico relativamente pequeño e imponer solamente unos requerimientos mínimos como entorno de operación. Son fácilmente reemplazables en caso de destrucción.
3. Se caracterizan por ser equipos afectos a la clasificación como informática personal que, además, son fácilmente transportables de un sitio a otro, pudiendo estar tanto dentro del recinto propio de la organización como en cualquier otro lugar.
4. Son aquellos equipos preparados para hacerse cargo inmediato de los equipos en producción.
5. Dícese de impresoras y servidores de impresión.
6. Son los equipos que se instalan entre dos zonas de confianza.
7. Dícese de equipamiento necesario para transmitir datos: routers, módems, etc.

[COM] Redes de comunicaciones

[PSTN] red telefónica
[ISDN] rdsi (red digital)
[X25] X25 (red de datos)
[ADSL] ADSL
[pp] punto a punto
[radio] comunicaciones radio
[wifi] red inalámbrica
[mobile] telefonía móvil
[sat] por satélite
[LAN] red local
[MAN] red metropolitana
[Internet] Internet

[Media] Soporte de información

[electronic] electrónicos
- [disk] discos
- [vdisk] discos virtuales
- [san] almacenamiento en red
- [disquette] disquetes
- [cd] cederrón (CD-ROM)
- [usb] memorias USB
- [dvd] DVD
- [tape] cinta magnética
- [mc] tarjetas de memoria
- [ic] tarjetas inteligentes

[non_electronic] no electrónicos
- [printed] material impreso
- [tape] cinta de papel
- [film] microfilm
- [cards] tarjetas perforadas

[AUX]Equipamiento auxiliar

[power] fuentes de alimentación
[ups] sistemas de alimentación ininterrumpida
[gen] generadores eléctricos
[ac] equipos de climatización
[cabling] cableado

[wire] cable eléctrico [fiber] fibra óptica [robot] robots [tape] ... de cintas [disk] ... de discos [supply] suministros esenciales [destroy] equipos de destrucción de soportes de información [furniture] mobiliario: armarios, etc [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 [des] desarrolladores / programadores [prov] proveedores

Fuente: Elaborado por el Autor.

10.3 Identificación de los Activos

por dominios

dominio de seguridad	[essential]	[arch]	[availability]	[evaluated]	[D]	[keys]	[S]	[SW]	[HW]	[COM]	[Media]	[AUX]	[L]	[P]	[EXT]	[other]	total
[base] UNPRG	1	0	0	0	0	0	1	2	12	2	2	5	1	2	0	0	27
TOTAL	1	0	0	0	0	0	1	2	12	2	2	5	1	2	0	0	27

por capas

capa	[essential]	[arch]	[availability]	[evaluated]	[D]	[keys]	[S]	[SW]	[HW]	[COM]	[Media]	[AUX]	[L]	[P]	[EXT]	[other]	total
S	1	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	1
SW	0	0	0	0	0	0	0	2	0	0	0	0	0	0	0	0	2
HW	0	0	0	0	0	0	0	0	12	0	0	0	0	0	0	0	12
COM	0	0	0	0	0	0	0	0	0	2	0	0	0	0	0	0	2
MEDIA	0	0	0	0	0	0	0	0	0	0	2	0	0	0	0	0	2
AUX	0	0	0	0	0	0	0	0	0	0	0	5	0	0	0	0	5
L	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	1
P	0	0	0	0	0	0	0	0	0	0	0	0	0	2	0	0	2
TOTAL	1	0	0	0	0	0	1	2	12	2	2	5	1	2	0	0	27

por fuente

fuente	[essential]	[arch]	[availability]	[evaluated]	[D]	[keys]	[S]	[SW]	[HW]	[COM]	[Media]	[AUX]	[L]	[P]	[EXT]	[other]	total
F-ASUNPRG	1	0	0	0	0	0	1	2	12	2	2	5	1	2	0	0	27
TOTAL	1	0	0	0	0	0	1	2	12	2	2	5	1	2	0	0	27

Figura 16: Estadísticas de los Activos

Fuente: Proyecto Pilar AGRSGA-UNPRG

10.4 Clasificación de los Activos

ACTIVOS	CLASES DE ACTIVOS
[S] Servicios	
[gmat] Gestión de Matricula y notas de los alumnos – UNPRG	[essential.service]servicio [s.ext, s.int]servicio, interno
[SW] Software	
[sgap] Sistema de Gestión Académica para PreGrado	[SW.prp]desarrollo propio
[sega] Sistema de Gestión Académica	[SW.prp]desarrollo propio
[HW] Hardware	
[serv]servidores	
[seap] servidor de aplicaciones	[HW]Equipos informáticos
[sapb] servidor de aplicaciones – backup	[HW]Equipos informáticos
[sebd] servidor de base de datos	[HW]Equipos informáticos
[sapd] servidor de aplicaciones 2	[HW]Equipos informáticos
[sbdo] servidor de base de datos – OCCA	[HW]Equipos informáticos
[srbo] servidor de base de datos- backup – OCCA	[HW]Equipos informáticos
[sacd] servidor Directorio de Usuarios	[HW]Equipos informáticos
[sanv] servidor Antivirus	[HW]Equipos informáticos
[spro] servidor Proxy	[HW]Equipos informáticos
[sred] soporte de la red	
[conm] switch	[HW]Equipos informáticos
[cotf] firewall	[HW]Equipos informáticos
[rout] router	[HW]Equipos informáticos
[COM] Redes de Comunicaciones	
[rlan] red local	[COM.LAN]red local
[intr] internet	[COM.Internet]Internet.
[MEDIA] Soportes de Información	
[disk] discos	[MEDIA.electronic.disk]discos

[prin] Documentación Impresa	[MEDIA.non_electronic.printed]material impreso
[AUX] Equipamiento auxiliar	
[upsi]sistemas de alimentación ininterrumpida	[aux.ups]Sai
[grue] grupo electrógeno	[aux.gen]generadores eléctricos
[eqcs]equipo de aire acondicionado	[aux.ac]equipos de climatización
[cabl] cableado	
[clec] cableado eléctrico	[aux.cabling]cable eléctrico
[cart] cableado de red	[aux.cabling]cable eléctrico
[L] Instalaciones	
[sase]Sala de Servidores	[L.local]cuarto
[P] Personal	
[user]Usuarios Finales	[P.{ue.ui}]usuarios externos, usuarios internos
[admc] administrador de comunicaciones y seguridad	[P{com,sec}]admin. Comunicaciones, admin. Seguridad

Cuadro 16: Clasificación de los Activos

Fuente: Proyecto Pilar AGRSGA-UNPRG

10.5 Dependencia de los Activos

Activos	Dependencias
[S] Servicios	
[gmat] Gestión de Matricula y notas de los alumnos – UNPRG	[sgap] Sistema de Gestión Académica para PreGrado [sega] Sistema de Gestión Académica [serv.seap] servidor de aplicaciones [serv.sapb] servidor de aplicaciones - backup [serv.sebd] servidor de base de datos [serv.sapd] servidor de aplicaciones 2 [serv.sbdo] servidor de base de datos – OCCA [serv.srbo] servidor de base de datos- backup – OCCA [serv.sacd] servidor Directorio de Usuarios [serv.sanv] servidor Antivirus [serv.spro] servidor Proxy [conm] switch [cotf] firewall [rout] router [rlan] red local [intr] internet [disk] Discos [prin] Documentación Impresa [upsi] Sistema de alimentación Ininterrumpida [grue] Grupo Electrógeno [eqcs] Equipo de aire acondicionado [cabl.clec] cableado eléctrico [cabl.cart] cableado de red
[SW] Software	
[sgap] Sistema de Gestión Académica para PreGrado	[user] Usuarios Finales [admc]Administrador de Comunicaciones y Seguridad
[sega] Sistema de Gestión Académica	[user] Usuarios Finales [admc]Administrador de Comunicaciones y Seguridad

[HW] Hardware	
[serv]servidores	
[seap] servidor de aplicaciones	[sase]Sala de Servidores
[sapb] servidor de aplicaciones – backup	[sase]Sala de Servidores
[sebd] servidor de base de datos	[sase]Sala de Servidores
[sapd] servidor de aplicaciones 2	[sase]Sala de Servidores
[sbdo] servidor de base de datos – OCCA	[sase]Sala de Servidores
[srbo] servidor de base de datos- backup –OCCA	[sase]Sala de Servidores
[sacd] servidor Directorio de Usuarios	[sase]Sala de Servidores
[sanv] servidor Antivirus	[sase]Sala de Servidores
[spro] servidor Proxy	[sase]Sala de Servidores
[sred] soporte de la red	
[conm] switch	[sase]Sala de Servidores
[cotf] firewall	[sase]Sala de Servidores
[rout] router	[sase]Sala de Servidores
[COM] Redes de Comunicaciones	
[rlan] red local	[sase]Sala de Servidores
[intr] internet	[sase]Sala de Servidores
[MEDIA] Soportes de Información	
[disk] discos	[admc] administrador de comunicaciones y seguridad
[prin] Documentación Impresa	[admc] administrador de comunicaciones y seguridad
[AUX] Equipamiento auxiliar	
[upsi]sistemas de alimentación ininterrumpida	[sase]Sala de Servidores
[grue] grupo electrógeno	[sase]Sala de Servidores
[eqcs]equipo de aire acondicionado	[sase]Sala de Servidores
[cabl] cableado	
[clec] cableado eléctrico	[sase]Sala de Servidores
[cart] cableado de red	[sase]Sala de Servidores
[L] Instalaciones	
[sase]Sala de Servidores	[user] Usuarios Finales [admc] administrador de comunicaciones y seguridad
[P] Personal	
[user]Usuarios Finales	
[admc] administrador de comunicaciones y seguridad	

Cuadro 17: Dependencia entre los Activos
Fuente: Proyecto Pilar AGRSGA-UNPRG

10.6 Estadística de la dependencia de los Activos

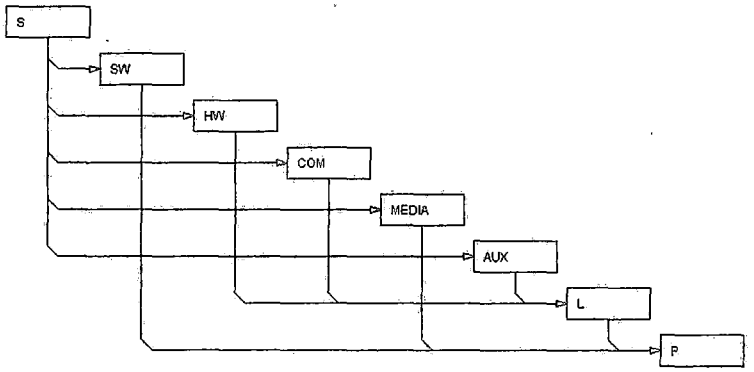

Figura 17: dependencias entre capas
Fuente: Proyecto Pilar AGRSGA-UNPRG

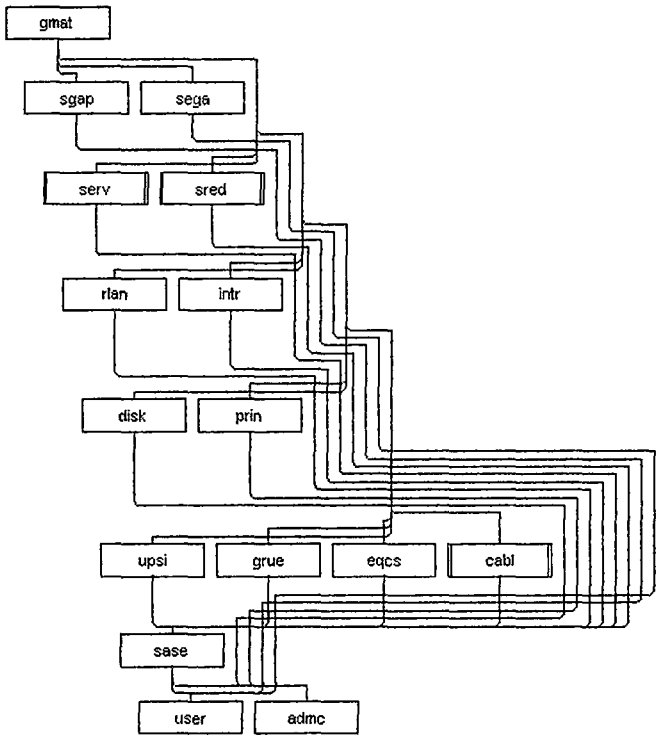

Figura 18: Dependencia entre activos- Bloques
Fuente: Proyecto Pilar AGRSGA-UNPRG

10.7 Lista de Amenazas

Amenazas
[N]Desastres naturales
[N.1]Fuego
[N.2]Daños por agua
[N.*]Desastres naturales
[N.*.1]Tormentas
[N.*.2]Tormentas eléctricas
[N.*.3]Huracanes
[N.*.4]Terremotos
[N.*.5]Tornados
[I.4.16] Ruido electromagnéticos deliberados
[I.4.21]Ruido termino accidental
[I.4.22]Ruido termino 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

[N.*.6]Ciclones
[N.*.7]Deslizamientos del terreno
[N.*.8]Meteoritos
[N.*.9]Tsunamis
[N.*.10]Tormentas de invierno y frio extremo
[N.*.11]Calor extremo
[N.*.12]Volcanes
[I]De origen industrial
[I.1]Fuego
[I.2]Daños por agua
[I.*]Desastres industriales
[I.3]Contaminación ambiental
[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] Ruido electromagnéticos accidentales
[E.4]Errores de configuración
[E.7]Deficiencias en la organización
[E.8]Difusión de software dañino
[E.8.0]Gusano
[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.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
[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 un 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.12.2]Térmica
[E]Errores y fallos no intencionados
[E.1]Errores de los usuarios
[E.2]Errores del administrador del sistema/ seguridad
[E.3]Errores de monitorización
[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
[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

[E.19.5]A los medios de comunicación
[E.19.11]Identificación de la localización
[E.20]Vulnerabilidades de los programas
[E.20.dos]Denegación de servicio
[E.20.read]Acceso de lectura
[E.20.write]Acceso de escritura
[E.20.escalation]Escalada de privilegios
[E.21]Errores de mantenimiento – software
[E.23]Errores de mantenimiento – hardware
[E.24]Caída del sistema por agotamiento de recursos
[E.25]Perdida de equipos
[A.12]Análisis de trafico
[A.12.1]Por personal interno
[A.12.2]Por subcontratistas
[A.12.3]Por personas externas
[A.13]Repudio
[A.14]Interceptación de información
[A.14.1]Por personal interno
[A.14.2]Por subcontratistas
[A.14.3]Por personas externas
[A.15]Modificación de la información
[A.18]Destrucción de la información
[A.19]Revelación de información
[A.14.1]Por personal interno
[A.14.2]Por subcontratistas
[A.14.3]Por personas externas
[A.14.4]Por personal interno
[A.14.5]Por subcontratistas
[A.14.6]Por personas externas
[A.22]Manipulación de programas
[A.22.1]Bombas lógicas
[A.22.2]Caballos de Troya
[A.22.3]KeyLogger
[A.22.4]Puertas traseras
[A.22.5]Autenticación débil
[A.22.6]Se elude la autenticación
[A.23]Manipulación del hardware
[A.24]Denegación de servicios
[A.24.1]Saturación de los canales de comunicaciones
[A.24.2] Saturación de los recursos software
[A.8]Difusión de software dañino
[A.8.0]Gusano
[A.8.1]Virus
[A.8.2]Caballos de Troya
[A.8.3]Spyware
[A.9]Encaminamiento de mensajes
[A.10]Alteración de secuencia
[A.11]Acceso no autorizado
[A.11.1]Por personal interno
[A.11.2]Por subcontratistas
[A.11.3]Por personas externas
[A.24.3] Saturación de los recursos hardware
[A.25]Robo de equipos
[A.25.1]Por personal interno
[A.25.2]Por subcontratistas
[A.25.3]Por personas externas
[A.26]Ataque destructivos
[A.26.1]Vandalismo
[A.26.2]Bombas
[A.26.3]Terrorismo
[A.27]Ocupación enemiga
[A.28]Indisponibilidad del personal
[A.28.1] Enfermedad
[A.28.2] Huelga
[A.28.3] Absentismo
[A.29]Extorsión
[A.29.1] Ataque desde el exterior
[A.29.2] Ataque desde el interior
[A.30]Ingeniería social
[A.30.1] Ataque desde el exterior
[A.30.2] Ataque desde el interior

Cuadro 18: Lista de Amenazas

Fuente: Elaborado por el Autor basado en Magerit v.3

10.8 Identificación de las Amenazas

ACTIVOS		AMENAZAS
[S] Servicios		
	[gmat] Gestión de Matricula y notas de los alumnos – UNPRG	[E.1]Errores de los usuarios [E.2]Errores del administrador del sistema / de la seguridad [E.15]Alteración de la información [E.18]Destrucción de la información [E.19]Fugas de información [E.24]Caída del sistema por agotamiento de recursos [A.5]Suplantación de la identidad [A.6]Abuso de privilegios de acceso [A.7]Uso no previsto [A.11]Acceso no autorizado [A.15]Modificación de la información [A.18]Destrucción de la información [A.19]Revelación de información [A.24]Denegación de servicio
[SW] Software		
	[sgap] Sistema de Gestión Académica para Pre-Grado	[E.1]Errores de los usuarios [E.2]Errores del administrador del sistema / de la seguridad [E.8]Difusión de software dañino [E.15]Alteración de la información [E.18]Destrucción de la información [E.19]Fugas de información [E.20]Vulnerabilidades de los programas [E.21]Errores de mantenimiento / actualización de programa [A.5]Suplantación de la identidad [A.6]Abuso de privilegios de acceso [A.7]Uso no previsto [A.8]Difusión de software dañino [A.11]Acceso no autorizado [A.15]Modificación de la información [A.18]Destrucción de la información [A.19]Revelación de información [A.22]Manipulación de programas
	[sega] Sistema de Gestión Académica	[E.1]Errores de los usuarios [E.2]Errores del administrador del sistema / de la seguridad [E.8]Difusión de software dañino [E.15]Alteración de la información [E.18]Destrucción de la información [E.19]Fugas de información [E.20]Vulnerabilidades de los programas [E.21]Errores de mantenimiento / actualización de programa [A.5]Suplantación de la identidad [A.6]Abuso de privilegios de acceso [A.7]Uso no previsto [A.8]Difusión de software dañino [A.11]Acceso no autorizado [A.15]Modificación de la información [A.18]Destrucción de la información [A.19]Revelación de información [A.22]Manipulación de programas

[HW] Hardware		
	[serv]servidores	
	[seap] servidor de aplicaciones	[N.1]Fuego [N.2]Daños por agua [N.*]Desastres naturales [I.5]Avería de origen físico o lógico [I.6]Corte del suministro eléctrico [I.7]Condiciones inadecuadas de temperatura o humedad [E.2]Errores del administrador del sistema/ seguridad [E.23]Errores de mantenimiento – hardware [E.24]Caída del sistema por agotamiento de recursos [E.25]Perdida de equipos [A.6]Abuso de privilegios de acceso [A.7]Uso no previsto [A.11]Acceso no autorizado [A.23]Manipulación del hardware [A.24]Denegación de servicios [A.25]Robo de equipos [A.26]Ataque destructivos
	[sapb] servidor de aplicaciones - backup	[N.1]Fuego [N.2]Daños por agua [N.*]Desastres naturales [I.5]Avería de origen físico o lógico [I.6]Corte del suministro eléctrico [I.7]Condiciones inadecuadas de temperatura o humedad [E.2]Errores del administrador del sistema/ seguridad [E.23]Errores de mantenimiento – hardware [E.24]Caída del sistema por agotamiento de recursos [E.25]Perdida de equipos [A.6]Abuso de privilegios de acceso [A.7]Uso no previsto [A.11]Acceso no autorizado [A.23]Manipulación del hardware [A.24]Denegación de servicios [A.25]Robo de equipos [A.26]Ataque destructivos
	[sebd] servidor de base de datos	[N.1]Fuego [N.2]Daños por agua [N.*]Desastres naturales [I.5]Avería de origen físico o lógico [I.6]Corte del suministro eléctrico [I.7]Condiciones inadecuadas de temperatura o humedad [E.2]Errores del administrador del sistema/ seguridad [E.23]Errores de mantenimiento – hardware [E.24]Caída del sistema por agotamiento de recursos [E.25]Perdida de equipos [A.6]Abuso de privilegios de acceso [A.7]Uso no previsto [A.11]Acceso no autorizado [A.23]Manipulación del hardware [A.24]Denegación de servicios [A.25]Robo de equipos [A.26]Ataque destructivos

		[sapd] servidor de aplicaciones 2	[N.1]Fuego [N.2]Daños por agua [N.*]Desastres naturales [I.5]Avería de origen físico o lógico [I.6]Corte del suministro eléctrico [I.7]Condiciones inadecuadas de temperatura o humedad [E.2]Errores del administrador del sistema/ seguridad [E.23]Errores de mantenimiento – hardware [E.24]Caída del sistema por agotamiento de recursos [E.25]Perdida de equipos [A.6]Abuso de privilegios de acceso [A.7]Uso no previsto [A.11]Acceso no autorizado [A.23]Manipulación del hardware [A.24]Denegación de servicios [A.25]Robo de equipos [A.26]Ataque destructivos
		[sbdo] servidor de base de datos - OCCA	[N.1]Fuego [N.2]Daños por agua [N.*]Desastres naturales [I.5]Avería de origen físico o lógico [I.6]Corte del suministro eléctrico [I.7]Condiciones inadecuadas de temperatura o humedad [E.2]Errores del administrador del sistema/ seguridad [E.23]Errores de mantenimiento – hardware [E.24]Caída del sistema por agotamiento de recursos [E.25]Perdida de equipos [A.6]Abuso de privilegios de acceso [A.7]Uso no previsto [A.11]Acceso no autorizado [A.23]Manipulación del hardware [A.24]Denegación de servicios [A.25]Robo de equipos [A.26]Ataque destructivos
		[srbo] servidor de base de datos-backup –OCCA	[N.1]Fuego [N.2]Daños por agua [N.*]Desastres naturales [I.5]Avería de origen físico o lógico [I.6]Corte del suministro eléctrico [I.7]Condiciones inadecuadas de temperatura o humedad [E.2]Errores del administrador del sistema/ seguridad [E.23]Errores de mantenimiento – hardware [E.24]Caída del sistema por agotamiento de recursos [E.25]Perdida de equipos [A.6]Abuso de privilegios de acceso [A.7]Uso no previsto [A.11]Acceso no autorizado [A.23]Manipulación del hardware [A.24]Denegación de servicios [A.25]Robo de equipos [A.26]Ataque destructivos

		[sacd] servidor Directorio de Usuarios	[N.1]Fuego [N.2]Daños por agua [N.*]Desastres naturales [I.5]Avería de origen físico o lógico [I.6]Corte del suministro eléctrico [I.7]Condiciones inadecuadas de temperatura o humedad [E.2]Errores del administrador del sistema/ seguridad [E.23]Errores de mantenimiento – hardware [E.24]Caída del sistema por agotamiento de recursos [E.25]Perdida de equipos [A.6]Abuso de privilegios de acceso [A.7]Uso no previsto [A.11]Acceso no autorizado [A.23]Manipulación del hardware [A.24]Denegación de servicios [A.25]Robo de equipos [A.26]Ataque destructivos
		[sanv] servidor Antivirus	[N.1]Fuego [N.2]Daños por agua [N.*]Desastres naturales [I.5]Avería de origen físico o lógico [I.6]Corte del suministro eléctrico [I.7]Condiciones inadecuadas de temperatura o humedad [E.2]Errores del administrador del sistema/ seguridad [E.23]Errores de mantenimiento – hardware [E.24]Caída del sistema por agotamiento de recursos [E.25]Perdida de equipos [A.6]Abuso de privilegios de acceso [A.7]Uso no previsto [A.11]Acceso no autorizado [A.23]Manipulación del hardware [A.24]Denegación de servicios [A.25]Robo de equipos [A.26]Ataque destructivos
		[spro] servidor Proxy	[N.1]Fuego [N.2]Daños por agua [N.*]Desastres naturales [I.5]Avería de origen físico o lógico [I.6]Corte del suministro eléctrico [I.7]Condiciones inadecuadas de temperatura o humedad [E.2]Errores del administrador del sistema/ seguridad [E.23]Errores de mantenimiento – hardware [E.24]Caída del sistema por agotamiento de recursos [E.25]Perdida de equipos [A.6]Abuso de privilegios de acceso [A.7]Uso no previsto [A.11]Acceso no autorizado [A.23]Manipulación del hardware [A.24]Denegación de servicios [A.25]Robo de equipos [A.26]Ataque destructivos

	[sred] soporte de la red		
		[conm] switch	[N.1]Fuego [N.2]Daños por agua [N.*]Desastres naturales [I.5]Avería de origen físico o lógico [I.6]Corte del suministro eléctrico [I.7]Condiciones inadecuadas de temperatura o humedad [E.2]Errores del administrador del sistema/ seguridad [E.23]Errores de mantenimiento – hardware [E.24]Caída del sistema por agotamiento de recursos [E.25]Perdida de equipos [A.6]Abuso de privilegios de acceso [A.7]Uso no previsto [A.11]Acceso no autorizado [A.23]Manipulación del hardware [A.24]Denegación de servicios [A.25]Robo de equipos [A.26]Ataque destructivos
		[cotf] firewall	[N.1]Fuego [N.2]Daños por agua [N.*]Desastres naturales [I.5]Avería de origen físico o lógico [I.6]Corte del suministro eléctrico [I.7]Condiciones inadecuadas de temperatura o humedad [E.2]Errores del administrador del sistema/ seguridad [E.23]Errores de mantenimiento – hardware [E.24]Caída del sistema por agotamiento de recursos [E.25]Perdida de equipos [A.6]Abuso de privilegios de acceso [A.7]Uso no previsto [A.11]Acceso no autorizado [A.23]Manipulación del hardware [A.24]Denegación de servicios [A.25]Robo de equipos [A.26]Ataque destructivos
		[rout] router	[N.1]Fuego [N.2]Daños por agua [N.*]Desastres naturales [I.5]Avería de origen físico o lógico [I.6]Corte del suministro eléctrico [I.7]Condiciones inadecuadas de temperatura o humedad [E.2]Errores del administrador del sistema/ seguridad [E.23]Errores de mantenimiento – hardware [E.24]Caída del sistema por agotamiento de recursos [E.25]Perdida de equipos [A.6]Abuso de privilegios de acceso [A.7]Uso no previsto [A.11]Acceso no autorizado [A.23]Manipulación del hardware [A.24]Denegación de servicios [A.25]Robo de equipos [A.26]Ataque destructivos

[COM] Redes de Comunicaciones		
	[rlan] red local	[I.8]Fallo de servicios de comunicaciones [E.2]Errores del administrador del sistema/ seguridad [E.10]Errores de secuencia [E.15]Alteración de la información [E.19]Fugas de información [A.5]Suplantación de la identidad [A.6]Abuso de privilegios de acceso [A.7]Uso no previsto [A.10]Alteración de secuencia [A.11]Acceso no autorizado [A.12]Análisis de tráfico [A.14]Interceptación de información [A.15]Modificación de la información [A.18]Destrucción de la información [A.19]Revelación de información [A.24]Denegación de servicios
	[intr] internet	[I.8]Fallo de servicios de comunicaciones [E.2]Errores del administrador del sistema/ seguridad [E.10]Errores de secuencia [E.15]Alteración de la información [E.19]Fugas de información [E.24]Caída del sistema por agotamiento de recursos [A.5]Suplantación de la identidad [A.6]Abuso de privilegios de acceso [A.7]Uso no previsto [A.10]Alteración de secuencia [A.11]Acceso no autorizado [A.12]Análisis de tráfico [A.14]Interceptación de información [A.15]Modificación de la información [A.18]Destrucción de la información [A.19]Revelación de información [A.24]Denegación de servicios
[MEDIA] Soportes de Información		
	[disk] discos	[N.1]Fuego [N.2]Daños por agua [N.*]Desastres naturales [I.7]Condiciones inadecuadas de temperatura o humedad [I.10]Degradación de los soportes de almacenamiento de la información [E.1]Errores de los usuarios [E.15]Alteración de la información [E.18]Destrucción de la información [E.19]Fugas de información
	[prin] Documentación Impresa	[N.1]Fuego [N.2]Daños por agua [N.*]Desastres naturales [I.7]Condiciones inadecuadas de temperatura o humedad [I.10]Degradación de los soportes de almacenamiento de la información [E.1]Errores de los usuarios [E.15]Alteración de la información

		[E.18]Destrucción de la información [E.19]Fugas de información
[AUX] Equipamiento auxiliar		
	[upsi]sistemas de alimentación ininterrumpida	[N.1]Fuego [N.2]Daños por agua [N.*]Desastres naturales [E.23]Errores de mantenimiento – hardware [A.7]Uso no previsto [A.23]Manipulación del hardware [A.25]Robo de equipos [A.26]Ataque destructivos
	[grue] grupo electrógeno	[N.1]Fuego [N.2]Daños por agua [N.*]Desastres naturales [E.23]Errores de mantenimiento – hardware [A.7]Uso no previsto [A.23]Manipulación del hardware [A.25]Robo de equipos [A.26]Ataque destructivos
	[eqcs]equipo de aire acondicionado	[N.1]Fuego [N.2]Daños por agua [N.*]Desastres naturales [I.6]Corte del suministro eléctrico [E.23]Errores de mantenimiento – hardware [A.7]Uso no previsto [A.23]Manipulación del hardware [A.25]Robo de equipos [A.26]Ataque destructivos
	[cabl] cableado	
	[clec] cableado eléctrico	[N.1]Fuego [N.2]Daños por agua [N.*]Desastres naturales [E.23]Errores de mantenimiento – hardware [A.7]Uso no previsto [A.23]Manipulación del hardware (Manipulación del cableado eléctrico) [A.25]Robo de equipos (Robo del cableado eléctrico) [A.26]Ataque destructivos
	[cart] cableado de red	[N.1]Fuego [N.2]Daños por agua [N.*]Desastres naturales [E.23]Errores de mantenimiento – hardware [A.7]Uso no previsto [A.23]Manipulación del hardware (Manipulación del cableado de red) [A.25]Robo de equipos (Robo del cableado de red) [A.26]Ataque destructivos
[L] Instalaciones		
	[sase]Sala de Servidores	[N.1]Fuego [N.2]Daños por agua [N.*]Desastres naturales [I.1]Fuego [I.2]Daños por agua

		[A.5]Suplantación de la identidad [A.6]Abuso de privilegios de acceso [A.7]Uso no previsto [A.11]Acceso no autorizado [A.26]Ataque destructivos [A.27]Ocupación enemiga
[P] Personal		
	[user]Usuarios Finales	[E.15]Alteración de la información [E.18]Destrucción de la información [E.19]Fugas de información [A.15]Modificación de la información [A.18]Destrucción de la información [A.19]Revelación de información [A.30]Ingeniería social
	[admc] administrador de comunicaciones y seguridad	[E.15]Alteración de la información [E.18]Destrucción de la información [E.19]Fugas de información [E.28]Indisponibilidad del personal [A.15]Modificación de la información [A.18]Destrucción de la información [A.19]Revelación de información [A.28]Indisponibilidad del personal [A.29]Extorsión [A.30]Ingeniería social

Cuadro 19: Identificación de Salvaguardas - Activo
Fuente: Proyecto Pilar AGRSGA-UNPRG

10.9 Valoración de las amenazas

Tabla 29: Valoración de las Amenazas

ACTIVOS / AMENAZAS	N	[D]	[I]	[C]	[A]	[T]
[S] Servicios						
[gmat] Gestión de Matricula y notas de los alumnos – UNPRG		A	A	A	T	T
[E.1]Errores de los usuarios	M	M	M	M		
[E.2]Errores del administrador del sistema / de la seguridad	M	M	M	M		
[E.15]Alteración de la información	M		B			
[E.18]Destrucción de la información	M	M				
[E.19]Fugas de información	M			M		
[E.24]Caída del sistema por agotamiento de recursos	A	A				
[A.5]Suplantación de la identidad	M		A	A	T	
[A.6]Abuso de privilegios de acceso	M	B	M	M	T	
[A.7]Uso no previsto	M	B	M	M		
[A.11]Acceso no autorizado	M		M	A	T	
[A.13]Repudio	A					T
[A.15]Modificación de la información	A		A			
[A.18]Destrucción de la información	M	A				
[A.19]Revelación de la información	M			A		
[A.24]Denegación de servicio	A	A				
[SW] Software						
[sgap] Sistema de Gestión Académica para PreGrado		T	T	T	T	
[I.5]Avería de origen físico o lógico	M	A				
[E.1]Errores de los usuarios	M	B	M	M		
[E.2]Errores del administrador del sistema / de la seguridad	M	M	M	M		

	[E.8]Difusión de software dañino	M	M	M	M		
	[E.15]Alteración de la información	M		B			
	[E.18]Destrucción de la información	M	A				
	[E.19]Fugas de información	M			M		
	[E.20]Vulnerabilidades de los programas	M	B	M	M		
	[E.21]Errores de mantenimiento / actualización de programa	A	B	B			
	[A.5]Suplantación de la identidad	M		A	A	T	
	[A.6]Abuso de privilegios de acceso	M	B	M	M		
	[A.7]Uso no previsto	M	B	M	M		
	[A.8]Difusión de software dañino	M	T	T	T		
	[A.11]Acceso no autorizado	M		M	A		
	[A.15]Modificación de la información	M		A			
	[A.18]Destrucción de la información	M	A				
	[A.19]Revelación de la información	M			A		
	[A.22]Manipulación de programas	M	A	T	T		
	[sega] Sistema de Gestión Académica		T	T	T	T	
	[I.5]Avería de origen físico o lógico	M	A				
	[E.1]Errores de los usuarios	M	B	M	M		
	[E.2]Errores del administrador del sistema / de la seguridad	M	M	M	M		
	[E.8]Difusión de software dañino	M	M	M	M		
	[E.15]Alteración de la información	M		B			
	[E.18]Destrucción de la información	M	A				
	[E.19]Fugas de información	M			M		
	[E.20]Vulnerabilidades de los programas	M	B	M	M		
	[E.21]Errores de mantenimiento / actualización de programa	A	B	B			
	[A.5]Suplantación de la identidad	M		A	A	T	
	[A.6]Abuso de privilegios de acceso	M	B	M	M		
	[A.7]Uso no previsto	M	B	M	M		
	[A.8]Difusión de software dañino	M	T	T	T		
	[A.11]Acceso no autorizado	M		M	A		
	[A.15]Modificación de la información	M		A			
	[A.18]Destrucción de la información	M	A				
	[A.19]Revelación de la información	M			A		
	[A.22]Manipulación de programas	M	A	T	T		
[HW] Hardware							
	[serv]servidores						
	[seap] servidor de aplicaciones		T	M	A		
	[N.1]Fuego	B	T				
	[N.2]Daños por agua	B	A				
	[N.*]Desastres naturales	B	T				
	[I.1]Fuego	M	T				
	[I.2]Daños por agua	M	A				
	[I.*]Desastres industriales	M	T				
	[I.3]Contaminación ambiental	B	A				
	[I.4]Contaminación electromagnética	M	M				
	[I.5]Avería de origen físico o lógico	M	A				
	[I.6]Corte del suministro eléctrico	M	T				
	[I.7]Condiciones inadecuadas de temperatura o humedad	M	T				
	[I.11]Emanaciones Electromagnéticas	M			B		
	[E.2]Errores del administrador del sistema/ seguridad	M	M	M	M		

		[E.23]Errores de mantenimiento – hardware	M	M				
		[E.24]Caída del sistema por agotamiento de recursos	A	A				
		[E.25]Perdida de equipos	M	T		A		
		[A.6]Abuso de privilegios de acceso	M	M	M	A		
		[A.7]Uso no previsto	M	M	B	M		
		[A.11]Acceso no autorizado	M	M	M	A		
		[A.23]Manipulación del hardware	M	A		A		
		[A.24]Denegación de servicios	M	T				
		[A.25]Robo de equipos	M	T		A		
		[A.26]Ataque destructivos	M	T				
		[sapb] servidor de aplicaciones – backup		T	M	A		
		[N.1]Fuego	B	T				
		[N.2]Daños por agua	B	A				
		[N.*]Desastres naturales	B	T				
		[I.1]Fuego	M	T				
		[I.2]Daños por agua	M	A				
		[I.*]Desastres industriales	M	T				
		[I.3]Contaminación ambiental	B	A				
		[I.4]Contaminación electromagnética	M	M				
		[I.5]Avería de origen físico o lógico	M	A				
		[I.6]Corte del suministro eléctrico	M	T				
		[I.7]Condiciones inadecuadas de temperatura o humedad	M	T				
		[I.11]Emanaciones Electromagnéticas	M			B		
		[E.2]Errores del administrador del sistema/ seguridad	M	M	M	M		
		[E.23]Errores de mantenimiento – hardware	M	M				
		[E.24]Caída del sistema por agotamiento de recursos	A	A				
		[E.25]Perdida de equipos	M	T		A		
		[A.6]Abuso de privilegios de acceso	M	M	M	A		
		[A.7]Uso no previsto	M	M	B	M		
		[A.11]Acceso no autorizado	M	M	M	A		
		[A.23]Manipulación del hardware	M	A		A		
		[A.24]Denegación de servicios	M	T				
		[A.25]Robo de equipos	M	T		A		
		[A.26]Ataque destructivos	M	T				
		[sebd] servidor de base de datos		T	M	A		
		[N.1]Fuego	B	T				
		[N.2]Daños por agua	B	A				
		[N.*]Desastres naturales	B	T				
		[I.1]Fuego	M	T				
		[I.2]Daños por agua	M	A				
		[I.*]Desastres industriales	M	T				
		[I.3]Contaminación ambiental	B	A				
		[I.4]Contaminación electromagnética	M	M				
		[I.5]Avería de origen físico o lógico	M	A				
		[I.6]Corte del suministro eléctrico	M	T				
		[I.7]Condiciones inadecuadas de temperatura o humedad	M	T				
		[I.11]Emanaciones electromagnéticas	M			B		
		[E.2]Errores del administrador del sistema/ seguridad	M	M	M	M		
		[E.23]Errores de mantenimiento – hardware	M	M				
		[E.24]Caída del sistema por agotamiento de recursos	A	A				
		[E.25]Perdida de equipos	M	T		A		
		[A.6]Abuso de privilegios de acceso	M	M	M	A		

		[A.7]Uso no previsto	M	M	B	M		
		[A.11]Acceso no autorizado	M	M	M	A		
		[A.23]Manipulación del hardware	M	A		A		
		[A.24]Denegación de servicios	M	T				
		[A.25]Robo de equipos	M	T		A		
		[A.26]Ataque destructivos	M	T				
		[sapd] servidor de aplicaciones 2		T	M	A		
		[N.1]Fuego	B	T				
		[N.2]Daños por agua	B	A				
		[N.*]Desastres naturales	B	T				
		[I.1]Fuego	M	T				
		[I.2]Daños por agua	M	A				
		[I.*]Desastres industriales	M	T				
		[I.3]Contaminación ambiental	B	A				
		[I.4]Contaminación electromagnética	M	M				
		[I.5]Avería de origen físico o lógico	M	A				
		[I.6]Corte del suministro eléctrico	M	T				
		[I.7]Condiciones inadecuadas de temperatura o humedad	M	T				
		[I.11]Emanaciones electromagnéticas	M			B		
		[E.2]Errores del administrador del sistema/ seguridad	M	M	M	M		
		[E.23]Errores de mantenimiento – hardware	M	M				
		[E.24]Caída del sistema por agotamiento de recursos	A	A				
		[E.25]Perdida de equipos	M	T		A		
		[A.6]Abuso de privilegios de acceso	M	M	M	A		
		[A.7]Uso no previsto	M	M	B	M		
		[A.11]Acceso no autorizado	M	M	M	A		
		[A.23]Manipulación del hardware	M	A		A		
		[A.24]Denegación de servicios	M	T				
		[A.25]Robo de equipos	M	T		A		
		[A.26]Ataque destructivos	M	T				
		[sbdo] servidor de base de datos – OCCA		T	M	A		
		[N.1]Fuego	B	T				
		[N.2]Daños por agua	B	A				
		[N.*]Desastres naturales	B	T				
		[I.1]Fuego	M	T				
		[I.2]Daños por agua	M	A				
		[I.*]Desastres industriales	M	T				
		[I.3]Contaminación ambiental	B	A				
		[I.4]Contaminación electromagnética	M	M				
		[I.5]Avería de origen físico o lógico	M	A				
		[I.6]Corte del suministro eléctrico	M	T				
		[I.7]Condiciones inadecuadas de temperatura o humedad	M	T				
		[I.11]Emanaciones electromagnéticas	M			B		
		[E.2]Errores del administrador del sistema/ seguridad	M	M	M	M		
		[E.23]Errores de mantenimiento – hardware	M	M				
		[E.24]Caída del sistema por agotamiento de recursos	A	A				
		[E.25]Perdida de equipos	M	T		A		
		[A.6]Abuso de privilegios de acceso	M	M	M	A		
		[A.7]Uso no previsto	M	M	B	M		
		[A.11]Acceso no autorizado	M	M	M	A		
		[A.23]Manipulación del hardware	M	A		A		
		[A.24]Denegación de servicios	M	T				

		[A.25]Robo de equipos	M	T		A		
		[A.26]Ataque destructivos	M	T				
		[srbo] servidor de base de datos- backup -OCCA		T	M	A		
		[N.1]Fuego	B	T				
		[N.2]Daños por agua	B	A				
		[N.*]Desastres naturales	B	T				
		[I.1]Fuego	M	T				
		[I.2]Daños por agua	M	A				
		[I.*]Desastres industriales	M	T				
		[I.3]Contaminación ambiental	B	A				
		[I.4]Contaminación electromagnética	M	M				
		[I.5]Avería de origen físico o lógico	M	A				
		[I.6]Corte del suministro eléctrico	M	T				
		[I.7]Condiciones inadecuadas de temperatura o humedad	M	T				
		[I.11]Emanaciones electromagnéticas	M			B		
		[E.2]Errores del administrador del sistema/ seguridad	M	M	M	M		
		[E.23]Errores de mantenimiento – hardware	M	M				
		[E.24]Caída del sistema por agotamiento de recursos	A	A				
		[E.25]Perdida de equipos	M	T		A		
		[A.6]Abuso de privilegios de acceso	M	M	M	A		
		[A.7]Uso no previsto	M	M	B	M		
		[A.11]Acceso no autorizado	M	M	M	A		
		[A.23]Manipulación del hardware	M	A		A		
		[A.24]Denegación de servicios	M	T				
		[A.25]Robo de equipos	M	T		A		
		[A.26]Ataque destructivos	M	T				
		[sacd] servidor Directorio de Usuarios		T	M	A		
		[N.1]Fuego	B	T				
		[N.2]Daños por agua	B	A				
		[N.*]Desastres naturales	B	T				
		[I.1]Fuego	M	T				
		[I.2]Daños por agua	M	A				
		[I.*]Desastres industriales	M	T				
		[I.3]Contaminación ambiental	B	A				
		[I.4]Contaminación electromagnética	M	M				
		[I.5]Avería de origen físico o lógico	M	A				
		[I.6]Corte del suministro eléctrico	M	T				
		[I.7]Condiciones inadecuadas de temperatura o humedad	M	T				
		[I.11]Emanaciones electromagnéticas	M			B		
		[E.2]Errores del administrador del sistema/ seguridad	M	M	M	M		
		[E.23]Errores de mantenimiento – hardware	M	M				
		[E.24]Caída del sistema por agotamiento de recursos	A	A				
		[E.25]Perdida de equipos	M	T		A		
		[A.6]Abuso de privilegios de acceso	M	M	M	A		
		[A.7]Uso no previsto	M	M	B	M		
		[A.11]Acceso no autorizado	M	M	M	A		
		[A.23]Manipulación del hardware	M	A		A		
		[A.24]Denegación de servicios	M	T				
		[A.25]Robo de equipos	M	T		A		
		[A.26]Ataque destructivos	M	T				
		[sanv] servidor Antivirus		T	M	A		
		[N.1]Fuego	B	T				

		[N.2]Daños por agua	B	A				
		[N.*]Desastres naturales	B	T				
		[I.1]Fuego	M	T				
		[I.2]Daños por agua	M	A				
		[I.*]Desastres industriales	M	T				
		[I.3]Contaminación ambiental	B	A				
		[I.4]Contaminación electromagnética	M	M				
		[I.5]Avería de origen físico o lógico	M	A				
		[I.6]Corte del suministro eléctrico	M	T				
		[I.7]Condiciones inadecuadas de temperatura o humedad	M	T				
		[I.11]Emanaciones electromagnéticas	M			B		
		[E.2]Errores del administrador del sistema/ seguridad	M	M	M	M		
		[E.23]Errores de mantenimiento – hardware	M	M				
		[E.24]Caída del sistema por agotamiento de recursos	A	A				
		[E.25]Perdida de equipos	M	T		A		
		[A.6]Abuso de privilegios de acceso	M	M	M	A		
		[A.7]Uso no previsto	M	M	N	M		
		[A.11]Acceso no autorizado	M	M	M	A		
		[A.23]Manipulación del hardware	M	A		A		
		[A.24]Denegación de servicios	M	T				
		[A.25]Robo de equipos	M	T		A		
		[A.26]Ataque destructivos	M	T				
		[spro] servidor Proxy		T	M	A		
		[N.1]Fuego	B	T				
		[N.2]Daños por agua	B	A				
		[N.*]Desastres naturales	B	T				
		[I.1]Fuego	M	T				
		[I.2]Daños por agua	M	A				
		[I.*]Desastres industriales	M	T				
		[I.3]Contaminación ambiental	B	A				
		[I.4]Contaminación electromagnética	M	M				
		[I.5]Avería de origen físico o lógico	M	A				
		[I.6]Corte del suministro eléctrico	M	T				
		[I.7]Condiciones inadecuadas de temperatura o humedad	M	T				
		[I.11]Emanaciones electromagnéticas	M			B		
		[E.2]Errores del administrador del sistema/ seguridad	M	M	M	M		
		[E.23]Errores de mantenimiento – hardware	M	M				
		[E.24]Caída del sistema por agotamiento de recursos	A	A				
		[E.25]Perdida de equipos	M	T		A		
		[A.6]Abuso de privilegios de acceso	M	M	M	A		
		[A.7]Uso no previsto	M	M	B	M		
		[A.11]Acceso no autorizado	M	M	M	A		
		[A.23]Manipulación del hardware	M	A		A		
		[A.24]Denegación de servicios	M	T				
		[A.25]Robo de equipos	M	T		A		
		[A.26]Ataque destructivos	M	T				
	[sred] soporte de la red							
		[conm] switch		T	M	A		
		[N.1]Fuego	B	T				
		[N.2]Daños por agua	B	A				
		[N.*]Desastres naturales	B	T				
		[I.1]Fuego	M	T				

		[I.2]Daños por agua	M	A				
		[I.*]Desastres industriales	M	T				
		[I.3]Contaminación ambiental	B	A				
		[I.4]Contaminación electromagnética	M	M				
		[I.5]Avería de origen físico o lógico	M	A				
		[I.6]Corte del suministro eléctrico	M	T				
		[I.7]Condiciones inadecuadas de temperatura o humedad	M	T				
		[I.11]Emanaciones electromagnéticas	M			B		
		[E.2]Errores del administrador del sistema/ seguridad	M	M	M	M		
		[E.23]Errores de mantenimiento – hardware	M	M				
		[E.24]Caída del sistema por agotamiento de recursos	A	A				
		[E.25]Perdida de equipos	M	T		A		
		[A.6]Abuso de privilegios de acceso	M	M	M	A		
		[A.7]Uso no previsto	M	M	B	M		
		[A.11]Acceso no autorizado	M	M	M	A		
		[A.23]Manipulación del hardware	M	A		A		
		[A.24]Denegación de servicios	M	T				
		[A.25]Robo de equipos	M	T		A		
		[A.26]Ataque destructivos	M	T				
		[cotf] firewall		T	M	A		
		[N.1]Fuego	B	T				
		[N.2]Daños por agua	B	A				
		[N.*]Desastres naturales	B	T				
		[I.1]Fuego	M	T				
		[I.2]Daños por agua	M	A				
		[I.*]Desastres industriales	M	T				
		[I.3]Contaminación ambiental	B	A				
		[I.4]Contaminación electromagnética	M	M				
		[I.5]Avería de origen físico o lógico	M	A				
		[I.6]Corte del suministro eléctrico	M	T				
		[I.7]Condiciones inadecuadas de temperatura o humedad	M	T				
		[I.11]Emanaciones electromagnéticas	M			B		
		[E.2]Errores del administrador del sistema/ seguridad	M	M	M	M		
		[E.23]Errores de mantenimiento – hardware	M	M				
		[E.24]Caída del sistema por agotamiento de recursos	A	A				
		[E.25]Perdida de equipos	M	T		A		
		[A.6]Abuso de privilegios de acceso	M	M	M	A		
		[A.7]Uso no previsto	M	M	B	M		
		[A.11]Acceso no autorizado	M	M	M	A		
		[A.23]Manipulación del hardware	M	A		A		
		[A.24]Denegación de servicios	M	T				
		[A.25]Robo de equipos	M	T		A		
		[A.26]Ataque destructivos	M	T				
		[rout] router		T	M	A		
		[N.1]Fuego	B	T				
		[N.2]Daños por agua	B	A				
		[N.*]Desastres naturales	B	T				
		[I.1]Fuego	M	T				
		[I.2]Daños por agua	M	A				
		[I.*]Desastres industriales	M	T				
		[I.3]Contaminación ambiental	B	A				
		[I.4]Contaminación electromagnética	M	M				

		[I.5]Avería de origen físico o lógico	M	A				
		[I.6]Corte del suministro eléctrico	M	T				
		[I.7]Condiciones inadecuadas de temperatura o humedad	M	T				
		[I.11]Emanaciones electromagnéticas	M			B		
		[E.2]Errores del administrador del sistema/ seguridad	M	M	M	M		
		[E.23]Errores de mantenimiento – hardware	M	M				
		[E.24]Caída del sistema por agotamiento de recursos	A	A				
		[E.25]Perdida de equipos	M	T		A		
		[A.6]Abuso de privilegios de acceso	M	M	M	A		
		[A.7]Uso no previsto	M	M	B	M		
		[A.11]Acceso no autorizado	M	M	M	A		
		[A.23]Manipulación del hardware	M	A		A		
		[A.24]Denegación de servicios	M	T				
		[A.25]Robo de equipos	M	T		A		
		[A.26]Ataque destructivos	M	T				
[COM] Redes de Comunicaciones								
		[rlan] red local		A	M	A	T	
		[I.8]Fallo de servicios de comunicaciones	M	A				
		[E.2]Errores del administrador del sistema/ seguridad	M	M	M	M		
		[E.9]Errores de re-encaminamiento	M			M		
		[E.10]Errores de secuencia	M		M			
		[E.15]Alteración de la información	M		B			
		[E.19]Fugas de información	M			M		
		[E.24]Caída del sistema por agotamiento de recursos	M	A				
		[A.5]Suplantación de la identidad	M		M	A	T	
		[A.6]Abuso de privilegios de acceso	M		M	A	T	
		[A.7]Uso no previsto	M	M	M	M		
		[A.9]Encaminamiento de mensajes	M			M		
		[A.10]Alteración de secuencia	M		M			
		[A.11]Acceso no autorizado	M		M	A	T	
		[A.12]Análisis de tráfico	M			B		
		[A.14]Interceptación de información	M			B		
		[A.15]Modificación de la información	M		M			
		[A.18]Destrucción de la información	M	A				
		[A.19]Revelación de información	M			A		
		[A.24]Denegación de servicios	A	A				
		[intr] internet		A	M	A	T	
		[I.8]Fallo de servicios de comunicaciones	M	A				
		[E.2]Errores del administrador del sistema/ seguridad	M	M	M	M		
		[E.9]Errores de re-encaminamiento	M			M		
		[E.10]Errores de secuencia	M		M			
		[E.15]Alteración de la información	M		B			
		[E.19]Fugas de información	M			M		
		[E.24]Caída del sistema por agotamiento de recursos	M	A				
		[A.5]Suplantación de la identidad	M		M	A	T	
		[A.6]Abuso de privilegios de acceso	M		M	A	T	
		[A.7]Uso no previsto	M	M	M	M		
		[A.9]Encaminamiento de mensajes	M			M		
		[A.10]Alteración de secuencia	M		M			
		[A.11]Acceso no autorizado	M		M	A	T	
		[A.12]Análisis de tráfico	M			B		
		[A.14]Interceptación de información	M			M		

	[A.15]Modificación de la información	M		M			
	[A.18]Destrucción de la información	M	A				
	[A.19]Revelación de información	M			A		
	[A.24]Denegación de servicios	A	A				
[MEDIA] Soportes de Información							
	[disk] discos		T	T	T		
	[N.1]Fuego	B	T				
	[N.2]Daños por agua	B	A				
	[N.*]Desastres naturales	B	T				
	[I.1]Fuego	M	T				
	[I.2]Daños por agua	M	A				
	[I.*]Desastres industriales	M	T				
	[I.3]Contaminación ambiental	M	A				
	[I.4]Contaminación electromagnética	M	M				
	[I.5]Avería de origen físico o lógico	M	A				
	[I.6]Corte del suministro eléctrico	M	T				
	[I.7]Condiciones inadecuadas de temperatura o humedad	M	T				
	[I.10]Degradación de los soportes de almacenamiento de la información	M	T				
	[I.11]Emanaciones electromagnéticas	M			B		
	[E.1]Errores de los usuarios	M	B	M	M		
	[E.15]Alteración de la información	M		B			
	[E.18] Destrucción de la información	M	T				
	[E.19]Fugas de información	M			M		
	[E.23]Errores de mantenimiento – hardware	M	T				
	[E.25]Perdida de equipos	M	M		A		
	[A.7]Uso no previsto	M	B		B		
	[A.11]Acceso no autorizado	M		B	A		
	[A.15] Modificación de la información	A		T			
	[A.18]Destrucción de la información	M	T				
	[A.19]Revelación de la información	M			M		
	[A.23]Manipulación del hardware	B	A		A		
	[A.25]Robo de equipos	M	M		T		
	[A.26]Ataque destructivos	M	M				
	[prin] Documentación Impresa		T	T	T		
	[N.1]Fuego	B	T				
	[N.2]Daños por agua	B	A				
	[N.*]Desastres naturales	B	T				
	[I.1]Fuego	M	T				
	[I.2]Daños por agua	M	A				
	[I.*]Desastres industriales	M	T				
	[I.3]Contaminación ambiental	M	A				
	[I.7]Condiciones inadecuadas de temperatura o humedad	M	T				
	[I.10]Degradación de los soportes de almacenamiento de la información	M	T				
	[E.1]Errores de los usuarios	M	B	M	M		
	[E.15]Alteración de la información	M		B			
	[E.18] Destrucción de la información	M	T				
	[E.19]Fugas de información	M			M		
	[E.25]Perdida de equipos	M	M		A		
	[A.7]Uso no previsto	M	B		B		
	[A.11]Acceso no autorizado	M		B	A		
	[A.15] Modificación de la información	A		T			
	[A.18]Destrucción de la información	M	T				

	[A.19]Revelación de la información	M			M		
	[A.25]Robo de equipos	M	M		T		
	[A.26]Ataque destructivos	M	M				
[AUX] Equipamiento auxiliar							
	[upsi] Sistema de alimentación ininterrumpida		B				
	[N.1]Fuego	B	B				
	[N.2]Daños por agua	B	B				
	[N.*]Desastres naturales	B	B				
	[I.1]Fuego	M	B				
	[I.2]Daños por agua	M	B				
	[I.*]Desastres industriales	M	B				
	[I.3]Contaminación ambiental	B	B				
	[E.23]Errores de mantenimiento – hardware	M	B				
	[A.7]Uso no previsto	M	B				
	[A.23]Manipulación del hardware	M	B				
	[A.25]Robo de equipos	M	B				
	[A.26]Ataque destructivos	M	B				
	[grue] grupo electrógeno		B				
	[N.1]Fuego	B	B				
	[N.2]Daños por agua	B	B				
	[N.*]Desastres naturales	B	B				
	[I.1]Fuego	M	B				
	[I.2]Daños por agua	M	B				
	[I.*]Desastres industriales	M	B				
	[I.3]Contaminación ambiental	B	B				
	[I.9] interrupción de otros servicios o suministros esenciales	M	B				
	[E.23]Errores de mantenimiento – hardware	M	B				
	[A.7]Uso no previsto	M	B				
	[A.23]Manipulación del hardware	M	B				
	[A.25]Robo de equipos	M	B				
	[A.26]Ataque destructivos	M	B				
	[eqcs]equipo de aire acondicionado		M				
	[N.1]Fuego	B	M				
	[N.2]Daños por agua	B	M				
	[N.*]Desastres naturales	B	M				
	[I.1]Fuego	M	M				
	[I.2]Daños por agua	M	M				
	[I.*]Desastres industriales	M	M				
	[I.3]Contaminación ambiental	B	M				
	[I.6]Corte del suministro eléctrico	M	M				
	[I.9] interrupción de otros servicios o suministros esenciales	M	M				
	[E.23]Errores de mantenimiento – hardware	M	M				
	[A.7]Uso no previsto	M	M				
	[A.23]Manipulación del hardware	M	M				
	[A.25]Robo de equipos	M	M				
	[A.26]Ataque destructivos	M	M				
	[cabl] cableado						
	[clec] cableado eléctrico		T	M	A		
	[N.1]Fuego	B	T				
	[N.2]Daños por agua	B	A				
	[N.*]Desastres naturales	B	T				
	[I.1]Fuego	M	T				

		[I.2]Daños por agua	M	A				
		[I.*]Desastres industriales	M	T				
		[I.3]Contaminación ambiental	B	A				
		[I.4]Contaminación electromagnética	M	M				
		[I.11]Emanaciones electromagnéticas	M			B		
		[E.23]Errores de mantenimiento – hardware	M	M				
		[A.7]Uso no previsto	M	A	B	B		
		[A.11]Acceso no autorizado	M		M	A		
		[A.23]Manipulación del hardware	M	A		A		
		[A.25]Robo de equipos	M	T		0		
		[A.26]Ataque destructivos	M	T				
		[cart] cableado de red		T	M	A		
		[N.1]Fuego	B	T				
		[N.2]Daños por agua	B	A				
		[N.*]Desastres naturales	B	T				
		[I.1]Fuego	M	T				
		[I.2]Daños por agua	M	A				
		[I.*]Desastres industriales	M	T				
		[I.3]Contaminación ambiental	B	A				
		[I.4]Contaminación electromagnética	M	M				
		[I.11]Emanaciones electromagnéticas	M			B		
		[E.23]Errores de mantenimiento – hardware	M	M				
		[A.7]Uso no previsto	M	A	B	B		
		[A.11]Acceso no autorizado	M		M	A		
		[A.23]Manipulación del hardware	M	A		A		
		[A.25]Robo de equipos	M	T		0		
		[A.26]Ataque destructivos	M	T				
[L] Instalaciones								
		[sase]Sala de Servidores		T	M	A		
		[N.1]Fuego	M	T				
		[N.2]Daños por agua	M	T				
		[N.*]Desastres naturales	M	T				
		[I.1]Fuego	M	T				
		[I.2]Daños por agua	M	T				
		[I.*]Desastres industriales	M	T				
		[I.3]Contaminación ambiental	M	M				
		[I.4]Contaminación electromagnética	B	M				
		[I.11]Emanaciones electromagnéticas	B			B		
		[A.5]Suplantación de la identidad	M		M	A		
		[A.6]Abuso de privilegios de acceso	M	M	M	A		
		[A.7]Uso no previsto	M	M	M	A		
		[A.11]Acceso no autorizado	A		M	A		
		[A.26]Ataque destructivos	B	T				
		[A.27]Ocupación enemiga	M	T		A		
[P] Personal								
		[user]Usuarios Finales		A	A	M		
		[E.15]Alteración de la información	M		M			
		[E.18]Destrucción de la información	M	B				
		[E.19]Fugas de información	M			M		
		[E.28]Indisponibilidad del personal	M	M				
		[A.15]Modificación de la información	M		A			
		[A.18]Destrucción de la información	M	M				
		[A.19]Revelación de información	A			M		

	[A.28]Indisponibilidad del personal	M	A				
	[A.29]Extorsión	M	M	M	M		
	[A.30]Ingeniería social	M	M	M	M		
	[admc] administrador de comunicaciones y seguridad		A	T	T		
	[E.15]Alteración de la información	M		M			
	[E.18]Destrucción de la información	M	B				
	[E.19]Fugas de información	M			M		
	[E.28]Indisponibilidad del personal	M	M				
	[A.15]Modificación de la información	M		A			
	[A.18]Destrucción de la información	M	M				
	[A.19]Revelación de información	A			A		
	[A.28]Indisponibilidad del personal	M	M				
	[A.29]Extorsión	M	A	T	T		
	[A.30]Ingeniería social	M	A	T	T		

Fuente: Proyecto Pilar AGRSGA-UNPRG

10.10 Anexos en CD

- *Anexo CD 01: Libro I Método MAGERIT*
- *Anexo CD 01: Libro II Catalogo MAGERIT*
- *Anexo CD 01: Libro III Técnicas MAGERIT*
- *Anexo CD 02: Manual de Pilar*
- *Anexo CD 03: AGRSGA-UNPRG*
- *Anexo CD 04: Estado de Riesgo e Impacto*
- *Anexo CD 05: Diapositivas de Sustentación*