Universidad Nacional Pedro Ruiz Gallo
Facultad de Ingeniería Civil, Sistemas y Arquitectura
Escuela Profesional de Ingeniería de Sistemas

Tesis

Comparativa de las metodologías Magerit y Octave, para determinar la más adecuada en la gestión de riesgos de tecnologías de información en la Unidad de Red Telemática de la Universidad Nacional Pedro Ruiz Gallo

Para el título Profesional de Ingeniero(a) de Sistemas

Presentado por:

Bach. Campos Cruz, Criceily Yasmin

Bach. León Tesen, Dany Dandy

Asesor

Dr. Ing. Celi Arévalo, Ernesto Karlo

Lambayeque – Perú – 2020

Universidad Nacional Pedro Ruiz Gallo

Facultad de Ingeniería Civil, Sistemas y Arquitectura

Escuela Profesional de Ingeniería de Sistemas

Tesis

Comparativa de las metodologías Magerit y Octave, para determinar la más adecuada en la gestión de riesgos de tecnologías de información en la Unidad de Red Telemática de la Universidad Nacional Pedro Ruiz Gallo

Miembros del jurado

Mg. Ing. Robert Edgar Puican Gutierrez
Presidente del jurado

Mg. Ing. Campos Rios Pilar Del Rosario
Miembro del jurado

Mg. Ing. Arteaga Lora Roberto Carlos
Miembro del jurado

Universidad Nacional Pedro Ruiz Gallo

Facultad de Ingeniería Civil, Sistemas y Arquitectura

Escuela Profesional de Ingeniería de Sistemas

Tesis

Comparativa de las metodologías Magerit y Octave, para determinar la más adecuada en la gestión de riesgos de tecnologías de información en la Unidad de Red Telemática de la Universidad Nacional Pedro Ruiz Gallo

---

Presentado por:

Dr. Ing. Ernesto Karlo Celi Arévalo
Asesor

Campos Cruz Criceily Yasmin
Responsable

León Tesén Dany Dandy
Responsable

DEDICATORIAS

Dedicada a Dios por darme la vida y estar siempre conmigo, guiándome en mí camino.

A mis padres, el esfuerzo y metas alcanzadas, refleja la dedicación y el amor que invirtieron mí. Gracias a ellos son quién soy, orgullosamente y con la cara en alto agradezco a Alfredo Campos Cruzado y Luz Marina Cruz Alvarado, mi mayor inspiración, gracias a ellos he concluido con mi mayor meta.

A mi hermana Sandra Campos Cruz por su cariño y apoyo incondicional, durante todo este proceso; a mi enamorado Brayan Montenegro por estar conmigo en todo momento y darme los ánimos cuando sentía que no podía continuar. A todos los mencionados muchas gracias.

Criceily Yasmin Campos Cruz

Dedicada a Dios, quien como guía estuvo presente en el caminar de mi vida, bendiciéndome y dándome las fuerzas para continuar con mis metas trazadas sin desfallecer.

A mi madre María Tesén quién con amor, paciencia y esfuerzo me han permitido llegar a cumplir hoy un sueño más, gracias por inculcar en mí el ejemplo de esfuerzo y valentía de no temer a las adversidades porque Dios está conmigo siempre.

A mis tíos Gladis Alicia y Juan Carlos por su cariño y apoyo incondicional, durante todo este proceso por estar conmigo en todo momento.

A toda mi familia porque con sus oraciones, consejos y palabras de aliento hicieron de mí una mejor persona y de una u otra forma me acompañan en todos mis sueño y metas.

Dany Dandy León Tesen

AGRADECIMIENTOS

Agradecemos a Dios por bendecirnos la vida, por guiarnos a lo largo de nuestra existencia, ser el apoyo y fortaleza en aquellos momentos de dificultad y de debilidad.

A nuestros padres por ser un pilar fundamental y habernos apoyado incondicionalmente, pese a las adversidades e inconvenientes que se presentaron.

Al ingeniero Vladimir Gonzales Mechan, jefe de la Unidad de Red Telemática por todo su apoyo y compromiso con la realización de la tesis.

Agradecemos a nuestro asesor de tesis Mg. Ernesto Celi quien con su experiencia, conocimiento y motivación nos orientó desde el inicio de la investigación.

RESUMEN

La presente tesis se desarrolló en la Unidad de Red Telemática de la Universidad Nacional Pedro Ruiz Gallo, específicamente en el sistema académico, servicio que proporciona la Unidad. Desarrollada en 5 capítulos descritos a continuación.

En el capítulo I se describe el porqué de la realización de la tesis, a través de la situación problema, formulación de la pregunta de investigación, los objetivos, delimitación de la investigación y justificación e importancia de la misma.

En el capítulo II, se plantea la hipótesis de la tesis y la operalización de las variables a utilizar en la presente investigación.

En el capítulo III se presenta el marco teórico de la investigación, se describe el marco metodológico de las metodologías a utilizar. Presentado en 5 Ítems: Descripción de la metodología, Desarrollo de la metodología, catálogo de elementos, guía de técnicas y herramientas de las mismas.

En el capítulo IV se describe el desarrollo del modelo de madurez para la evaluación del control interno, es decir la aplicación de las metodologías: MAGERIT y OCTAVE. La primera con el marco metodológico dividido en caracterización de los activos, caracterización de las amenazas , caracterización de las salvaguardas y el estado de riesgo y la segunda Mediante 3 fases: Construcción del perfil de amenaza basado en los activos, Identificación de vulnerabilidades de infraestructura tecnológica y Desarrollo de estrategias y planes de seguridad.

En el capítulo V se plasman los resultados y discusión de la aplicación. Así como también una comparativa del desarrollo de las metodologías.

Por último el capítulo VI, describimos las conclusiones y recomendaciones al finalizar la realización de la presente tesis.

Todo lo mencionado anteriormente con el propósito de proporcionar la metodología más adecuada para la gestión de riesgos de TI en la Unidad de Red Telemática de la Universidad Nacional Pedro Ruiz Gallo.

ABSTRAC

This thesis was developed in the Unidad de Red Telemática of the Pedro Ruiz Gallo National University, specifically in the academic system, a service provided by the Unidad. Developed in 5 chapters described below.

Chapter I describes the reason for the completion of the thesis, through the problem situation, formulation of the research question, the objectives, delimitation of the research and justification and importance of it.

In chapter II, the hypothesis of the thesis and the operalization of the variables to be used in the present investigation is presented.

Chapter III presents the theoretical framework of the research, describes the methodological framework of the methodologies to be used. Presented in 5 items: Description of the methodology, Development of the methodology, catalog of elements, guide of techniques and tools thereof.

Chapter IV describes the development of the maturity model for the evaluation of internal control, that is, the application of the methodologies: MAGERIT and OCTAVE. The first with the methodological framework divided into characterization of the assets, characterization of the threats, characterization of the safeguards and the risk status and the second Through 3 phases: Construction of the threat profile based on the assets, Identification of vulnerabilities of technological infrastructure and Development of security strategies and plans.

Chapter V shows the results and discussion of the application. As well as a comparison of the development of methodologies.

Finally, chapter VI, we describe the conclusions and recommendations at the end of this thesis.

Everything mentioned above with the purpose of providing the most appropriate methodology for IT risk management in the Unidad de Red Telemática of the National University Pedro Ruiz Gallo.

INDICE DE CONTENIDOS

INDICE DE TABLAS

INDICE DE FIGURAS

INTRODUCCIÓN

La presente tesis tiene como objetivo desarrollar una evaluación comparativa de las metodologías MAGERIT y OCTAVE, para determinar el nivel de adecuación de cada ellas al proceso de gestión de riesgos de TI en la Unidad de Red Telemática de la Universidad Nacional Pedro Ruiz Gallo.

La situación problema que conllevó a realizar el desarrollo de la presente tesis es la falta de atención a los requerimientos que se solicitan en el área de informática, no contar con un manual de políticas, procedimientos y normativa relacionada con la Seguridad de Información formalmente aprobados; así como, tampoco cuenta con ninguna normativa de gestión de riesgos, evidenciando la falta de procesos de evaluación y de tratamiento de riesgos de TI. Se cuenta con un Sistema de gestión de Incidencias, Problemas y Peticiones, pero que no es utilizado con eficacia, por no contar con una persona encargada de su manejo.

Por lo mencionado anteriormente se hace necesario, realizar un estudio de las metodologías de gestión de riesgos de TI más conocidas en nuestro medio, como son MAGERIT y OCTAVE, que permita determinar cuál es la más adecuada para ser tomada como referencia en la implementación de un sistema de gestión de riesgos de TI en la Unida de Red Telemática de la UNPRG.

CAPÍTULO I: PROBLEMÁTICA DE LA INVESTIGACIÓN

1.1. Descripción de la realidad problema

En la actualidad las grandes organizaciones en su mayoría dependen del uso de la tecnología donde la información es un activo vital para ser exitosas, competitivas y lograr su continuidad en el mercado. El aseguramiento de dicha información y de los sistemas que la procesan es, por tanto, un objetivo primordial para la organización; por ello, la evaluación y la gestión de riesgos surge como una prioridad para la mayoría de las organizaciones.

Según estudios de investigación realizados por la IBM Company (2012) han demostrado que las empresas que adoptan un criterio equilibrado ante la madurez de la gestión de riesgos de Tecnologías de la Información (TI), no sólo tienen menos incidentes en este ámbito, sino que obtienen mayor rentabilidad del negocio y de TI respecto de la competencia. La falta de acción con respecto a los riesgos se debe al temor de tomar decisiones equivocadas y como consecuencia señalar a un responsable ante la pérdida de un derivado. Esta es una de las medidas más importantes que una empresa puede implementar para reducir de forma potencial los riesgos de TI.

Si bien en los últimos cinco años las organizaciones globales y peruanas han mejorado el modo en que identifican, gestionan y responden a los riesgos, en la actualidad menos del 50% de las empresas peruanas identifican, evalúan y desarrollan planes para gestionar los riesgos, informó la consultora EY (EY, 2015).

En el momento en que se realiza una buena gestión de riesgos de TI se madura, pasando de una situación complicada de manejo de las actividades de cumplimiento y reducción de amenazas hasta llegar a servicios de TI ágiles que generen valor al negocio (Westerman, 2006).

1.2. Planteamiento del problema

La Unidad de Red Telemática de la Universidad Nacional Pedro Ruiz Gallo (UNPRG) es una unidad dependiente de la Oficina General de Sistemas Informáticos (OGSI) y es la encargada de prestar los servicios de comunicaciones de TI en toda la Universidad.

Los servicios más destacados que se brindan en la Red Telemática son: Hosting de servicios web en servidores, provisión de servicios de Internet y acceso a la intranet.

La infraestructura de comunicaciones de la Unidad de Red Telemática, permite integrar todas las dependencias de la universidad y compartir los recursos tecnológicos e incrementar la productividad. Estos recursos tecnológicos comprenden el servicio de Internet, sistema de base de datos, información y servicios de impresión, aplicaciones web y de escritorio, comunicaciones de voz, entre otros. La Unidad de Red Telemática soporta todos estos servicios en un esquema de seguridad distribuida con la finalidad de especializar o dedicar la protección según el servicio publicado.

En la recopilación de la información, aplicando la técnica de la entrevista al jefe de la Unidad de Red Telemática, se pudo obtener la siguiente información en relación a la gestión de riesgos de TI

- Falta de atención a los requerimientos que se solicitan en el área de informática, lo que ha conllevado al aumento del potencial de impacto negativo con la ocurrencia de incidencias relacionadas con la seguridad informática y la seguridad de la Información.
- No cuenta con un manual de políticas, procedimientos y normativa relacionada con la Seguridad de Información formalmente aprobados; así como, tampoco cuenta con ninguna normativa de gestión de riesgos. Asimismo, los documentos que detallan cada una de las actividades que se realizan en la Unidad de Red Telemática han sido enviados a jefatura de OGSI, sin continuar su gestión para la aprobación por rectorado de la Universidad. Por lo tanto, todos los usuarios de las tecnologías de información y de la información que se

gestiona dentro de la universidad, no tiene funciones ni responsabilidades definidas en relación a la seguridad de la información

- El personal con el que cuenta la Unidad de Red Telemática tiene un bajo nivel de conocimiento sobre gestión de riesgos de TI y tiene una alta rotación, dado que en su mayoría son practicantes que solo desempeñan sus labores por un periodo limitado. Como consecuencia, cualquier planificación de actividades y proyectos relacionados con la seguridad de la información y la gestión de riesgos de TI, no tiene continuidad.
- Se evidencia la falta de procesos de evaluación y de tratamiento de riesgos de TI, que analice adecuadamente las amenazas, vulnerabilidades, impactos asociados con cada activo. Ocasionando el aumento potencial de los impactos negativos sobre la seguridad de la información.
- El Área de Red Telemática no cuenta con un ambiente adecuado, ya que se encuentra rodeado de material combustible (equipos Eléctricos y Electrónicos), además de contener la sala de servidores donde se pueden generar accidentes u otros desastres, además de no contar con un debido control de acceso.
- La Unidad de Red Telemática esta soportada por una infraestructura y equipamiento 50% antiguo, entre los que se encuentran los equipos más críticos, como el SwitchCore y servidores. A raíz de ello, la continuidad de los servicios y procesos de TI que brinda la Unidad de Red Telemática, no están garantizados, pudiendo incidir en el incumplimiento de la disponibilidad de los mismos.
- La Unidad de Red Telemática cuenta con un Sistema de gestión de Incidencias, Problemas y Peticiones, pero que no es utilizado con eficacia, por no contar con una persona encargada de su manejo. Como consecuencia, la gestión de incidentes y problemas de TI no es eficiente, generando reclamaciones de los usuarios de TI y, sobre todo, potencialmente podría ocurrir caídas parciales o totales severas de algunos procesos o servicios de TI.

Se hace necesario, realizar un estudio de las metodologías de gestión de riesgos de TI más conocidas en nuestro medio, como son MAGERIT y OCTAVE, que permita determinar cuál es la más adecuada para ser tomada como referencia en la implementación de un sistema de gestión de riesgos de TI en la Unida de Red Telemática de la UNPRG.

1.3. Formulación de la pregunta de investigación

¿Qué metodología entre MAGERIT y OCTAVE es la más adecuada para la gestión de riesgos de TI en la Unidad Red Telemática de la Universidad Nacional Pedro Ruiz Gallo?

1.4. Objetivos de la investigación

1.4.1. Objetivo General

Desarrollar una evaluación comparativa de las metodologías MAGERIT y OCTAVE, para determinar el nivel de adecuación de cada una de ellas al proceso de gestión de riesgos de TI en la Unidad de Red Telemática de la Universidad Nacional Pedro Ruiz Gallo.

1.4.2. Objetivos Específicos

a. Describir las metodologías MAGERIT y OCTAVE en la gestión de riesgos de TI, desde la perspectiva de sus procedimientos, catálogos, técnicas y herramientas aplicadas.
b. Aplicar las metodologías MAGERIT y OCTAVE en la gestión de riesgos de TI con datos reales de los procesos y servicios brindados por la Unidad de Red Telemática
c. Identificar y definir indicadores y criterios de medición para la evaluación de los resultados obtenidos en la aplicación de las metodologías mencionadas en la gestión de riesgos de TI en la Unidad de Red Telemática.

1.5. Delimitación de la investigación

La realización de la presente tesis tiene como propósito proporcionar la metodología más adecuada para la gestión de riesgos de TI en los procesos y servicios que forman parte del sistema académico brindado en la Unidad de Red de la Universidad Nacional Pedro Ruiz Gallo pero esta no será aplicada. Por tal razón en la metodología MAGERIT solo se aplicó el Método de Análisis de riesgos, etapa que contiene tres tareas, las cuales son caracterización de los activos, caracterización de la amenaza y la caracterización de salvaguardas. Y en la metodología OCTAVE se utilizaron la Fase 1 y Fase 2 en su totalidad pero en la Fase 3 solo se utilizó hasta la actividad de selección de enfoques de mitigación.

1.6. Justificación e importancia

1.6.1. Justificación

1.6.1.1. Justificación Académica

Los activos de TI de la gestión académica de la Universidad Nacional Pedro Ruiz Gallo, cuentan con barreras y procedimientos de seguridad en base a conocimientos de seguridad de equipo tecnológicos pero no siguen algún plan de gestión y análisis de riesgos en sus activos de TI. Existen diversas metodologías que permiten realizar un estudio de nivel de confiabilidad y seguridad de sus activos de TI, entre ellas tenemos a la metodología MAGERIT y OCTAVE. Metodologías de análisis y gestión de riesgos de Tecnologías de información. Las cuales mediante una serie de pasos nos mostrarán el estado actual de seguridad en las que se encuentran sus activos de TI.

1.6.1.2. Justificación Tecnológica

En la actualidad la tecnología forma parte del día a día y con la automatización de procesos se va facilitando la vida del ser humano. La Universidad Nacional Pedro Ruiz Gallo no es ajena a las innovaciones tecnológicas, a través de sus sistemas como el de gestión académica han tomado un papel importante en la comunidad universitaria, para eso la comunidad universitaria debe confiar en que los activos de TI en los que la información sobre su formación académica se encuentra son seguros y confiables.

1.6.1.3. Justificación Institucional

En búsqueda de mantener una buena imagen institucional, conservando la confianza, eficiencia y eficacia en los principales procesos que brinda la Unidad de Red Telemática. La Universidad Nacional Pedro Ruiz Gallo debe considerar la mitigación de riesgos presente en los activos de TI de la Unidad, para así brindar un mejor servicio.

1.6.2. Importancia

La importancia de modernizar y normalizar las políticas del plan de mitigación de riesgos, significa obtener la información acerca de los riesgos que se presentan y las medidas que deben tomarse en la búsqueda de mejorar la seguridad de la información reduciendo los riegos a los que están expuestos los activos de TI que forman parte de la Unidad de Red Telemática de la Universidad Nacional Pedro Ruiz Gallo.

De esta manera ofrecer un plan de mitigación de riesgos que pueda ser desarrollado y llevar un correcto control de los mismos.

CAPÍTULO II METODOLOGÍA DE LA INVESTIGACIÓN

2.1. Hipótesis

La metodología más adecuada para la gestión de riesgos de TI en la Unidad de Red Telemática de la Universidad Nacional Pedro Ruiz Gallo es MAGERIT.

2.2. Operacionalización de las variables

Las variables de la investigación son:

Tabla 1: Operacionalización de las variables

VARIABLE INDEPENDIENTE	Metodologías MAGERIT y OCTAVE
VARIABLE DEPENDIENTE	Adecuación para la gestión de riesgos de TI en la Unidad de Red Telemática de la Universidad Nacional Pedro Ruiz Gallo.

En la siguiente tabla se muestran las dimensiones e indicadores a evaluar en el estudio:

Tabla 2: Operacionalización de variables

VARIABLE	DIMENSIÓN	INDICADOR	ESCALA DE MEDICIÓN
Metodologías MAGERIT y OCTAVE	Activos	Nivel de efectividad para identificar activos críticos.	Rango en 5 niveles
		Nivel de efectividad para priorizar activos.	Rango en 5 niveles.
	Escenario de riesgo	Número de amenazas identificadas y valoradas.	Rango en 5 niveles.
		Número de vulnerabilidades identificadas y valoradas.	Rango en 5 niveles.
	Nivel de riesgo	Efectividad para la valoración de impactos.	Rango en 5 niveles.
		Efectividad para la valoración de ocurrencia.	Rango en 5 niveles.
	Tratamiento del riesgo	Número de controles necesarios para la mitigación de riesgos no tolerables.	Rango en 5 niveles.
Adecuación para la gestión de riesgos de TI en la Unidad de Red Telemática de la Universidad Nacional Pedro Ruiz Gallo	Cumplimiento normativo	Nivel de adecuación a los procedimientos y normas institucionales.	Rango en 5 niveles.
		Nivel de cumplimiento de criterios de seguridad establecidos en el estándar ISO 27002.	Rango en 5 niveles.
	Adecuación funcional	Disminución de incidentes de seguridad.	Rango en 5 niveles.
		Nivel de oportunidad para el tratamiento de escenarios de riesgos.	Rango en 5 niveles.
	Usabilidad	Nivel de comprensión del uso del modelo propuesto.	Rango en 5 niveles.

CAPITULO III MARCO TEÓRICO CONCEPTUAL

3.1 Antecedentes de la investigación

3.1.1 Antecedente 1

En la tesis de (Guevara Chumán, 2015) titulada **"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",** se abordó el problema de la falta de un plan de contingencia y mitigación de riesgos sobre los servidores de los sistemas de gestión académica de la Universidad Nacional Pedro Ruiz Gallo. Por tanto, el estudio planteó el desarrollo de un modelo de gestión de riesgos de TI aplicando la MAGERIT para el Análisis y Gestión de Riesgos en los servidores de los Sistemas de Gestión Académica de la Universidad Nacional Pedro Ruiz Gallo, que detallara los riegos a los que estaban expuestos los servidores de los sistemas y las medidas que se puedan adoptarse para el control de riesgos. El propósito fue brindar un Plan de Mitigación de riesgos basado en las medidas de seguridad ya implementadas con la metodología MAGERIT y el aplicativo Pilar utilizado. Los resultados de la investigación concluyeron que los servidores están expuestos a un conjunto de riesgos debido a 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; evaluándose el nivel de exposición al riesgo de cada uno de ellos y finalmente, para aquellos niveles de riesgo críticos, se propuso un conjunto de controles que permitieran mitigarlos.

3.1.2 Antecedente 2

En la tesina (Peña Velázquez, 2011) titulada "**Aplicación de la metodología MAGERIT en el análisis de riesgo del flujo de información en el área de gestión de una empresa dedicada a la aplicación de exámenes de control de confianza**", se abordó el problema de la falta de políticas de seguridad de la información, la poca o nula capacitación del personal y la necesidad de contar con un sistema seguro de información por lo cual se propuso la aplicación de la Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información (MAGERIT) a un proceso del flujo de información que se llevaba a cabo en el área de gestión de resultados de una empresa dedicada a la aplicación de exámenes de control de confianza del personal para localizar los puntos vulnerables del flujo de información que se da entre las áreas de evaluación con el área de gestión y los datos generales de las personas. Lo cual permitió proteger los activos más importantes en el área de gestión de resultados y así poder seleccionar al personal adecuado que cumple con el perfil. Los resultados obtenidos con la aplicación de la metodología fueron la implementación de políticas de resguardo de la información, el uso de canales de comunicación seguros para el envío de los resultados de las áreas de gestión, un proceso adecuado para la generación de respaldo de la información y una base de datos que remplace el uso de archivos Excel.

3.1.3 Antecedente 3

En la tesis de (Reyes Bedoya, 2014) titulada: "**El Análisis de Riesgos Informáticos y su incidencia en la seguridad e integridad de la información en la Facultad de Ingeniería Civil y Mecánica de la Universidad Técnica de Ambato**." Cuya principal problemática abordada fue la ausencia de políticas de prevención de riesgos en los sistemas informáticos de la facultad cuyos sistemas informáticos sufrían de amenazas debido al desconocimiento y falta de aplicación de procedimientos de gestión de riesgos que permitan definir acciones más adecuadas para minimizar la inseguridad y vulnerabilidad de los recursos de la facultad ya mencionada. Se propuso la aplicación de una metodología de análisis informáticos las cuales fueron MAGERIT y OCTAVE, que les permitiera contar con una herramienta para la identificación de los recursos críticos, las amenazas a los que estaban expuestos los equipos. Los resultados de la investigación

concluyeron que la metodología que mejor se adecuaba a los sistemas informáticos de la facultad fue OCTAVE-S, ya que esta se enmarcaba en la estructura administrativa de la facultad, es auto dirigido ya que recurre al personal de la organización, quienes conocen los problemas que tiene la misma, y puede enfocar el análisis en los puntos más críticos.

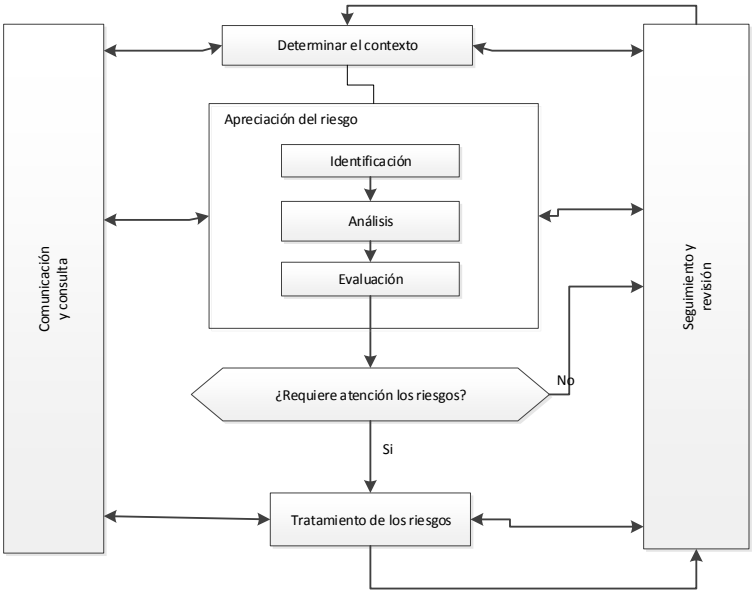
3.2 Metodología MAGERIT

3.2.1. Descripción de la metodología

El nombre de MAGERIT responde a "Metodología de Análisis y Gestión de Riesgos de TI", y es un método formal orientado a activos, cuya misión es descubrir los riesgos a los que se encuentran expuestos nuestros sistemas de información y recomendar las medidas apropiadas que deberían adoptarse para controlas estos riesgos. (Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica, 2012)

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 1: ISO 31000 - Marco de trabajo para la gestión de riesgos.

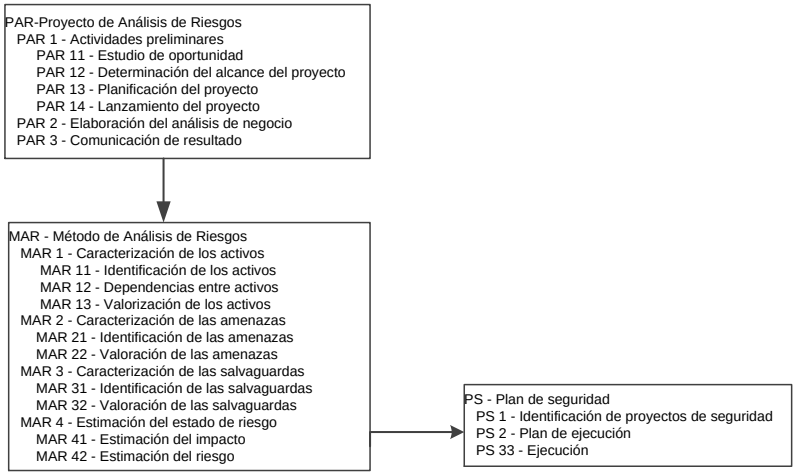


Fuente: Elaborado por los autores.

3.2.2. Método de Análisis de Riesgos y Proceso de Gestión de Riesgos propuestos por MAGERIT.

Dada la delimitación de la investigación soló se desarrolló la etapa de Método de Análisis de Riesgos, que abarca las tareas de Caracterización de activos, amenazas y salvaguardas. En la última tarea se desarrolló hasta la actividad tratamiento de riesgos.

Figura 2: Proceso de Gestión de Riesgos



Fuente: Elaborado por los autores

MAGERIT Fase 2: Método de análisis de riesgos.

El objetivo de estas tareas es reconocer los activos que componen el sistema, definir las dependencias entre ellos, y determinar que parte del valor del sistema se soporta en cada activo.

MAGERIT Fase 2 Proceso P1: Caracterización de los activos Proceso.

Tabla 3: Identificación de activos

MAR: Análisis de riesgos MAR 1: Características de los activos MAR 11: Identificación de los activos
Objetivos
Productos de entrada • Inventario de datos manejados por el sistema • Inventario de servicios prestados por el sistema • Procesos de negocio • Diagramas de uso • Diagramas fe flujo de datos • Inventarios de equipamiento lógico • Inventarios de equipamiento físico • Locales y sedes de la organización • Caracterización funcional de los puestos de trabajo.
Productos de salida: • Relación de activos a considerar. • Caracterización de los activos: valor propio y acumulado. • Relaciones entre activos.
Técnicas, prácticas y pauta - Diagrama de flujo de datos - Diagramas de procesos - Reuniones - Valoración Delphi.

Fuente: MAGERIT - V 3.0. Libro 1: Método. Gobierno de España-Ministerio de Hacienda y Relaciones Públicas. 2012.

Para cada activo hay que determinar una serie de características que lo definen:

- Código, típicamente procedente del inventario
- Nombre (corto)
- Descripción (larga)
- Tipo (o tipos) que caracterizan el activo.
- Unidad responsable.
- Persona responsable
- Ubicación, técnica o geografía
- Cantidad, si procede como puede ser en el caso de la informática personal.
- Otras características específicas del tipo de activo.

Tabla 4: Dependencia entre activos

MAR: Análisis de riesgos MAR 1: Características de los activos MAR 12: Dependencias entre activos
Objetivos - Identificar y 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.
Productos de entrada - Resultados de la tarea T 1.2.1. - Procesos de negocio. - Diagramas de flujo de datos. - Diagramas de uso.
Productos de salida - Diagrama de dependencia entre activos.
Técnicas, prácticas y pautas - Catálogos de amenazas - Arboles de ataques. - Entrevistas - Reuniones - Valoración Delphi.

Fuente: MAGERIT - V 3.0. Libro 1: Método. Gobierno de España-Ministerio de Hacienda y Relaciones Públicas. 2012.

Para cada dependencia conviene registrar la siguiente información:

- Estimación del grado de dependencia: hasta un 100%
- Explicación de la valoración de la dependencia
- Entrevistas realizadas de las que se ha deducido la anterior estimación.

Tabla 5: Valoración de los activos

MAR: Análisis de riesgos MAR 1: Características de los activos MAR 13: Valoración de los activos
Objetivos - Identificar en que dimensión es valioso el activo - Valorar el coste que para la organización supondría la destrucción del activo
Productos de entrada - Resultados de la tarea MAR 11 - Resultados de la tarea MAR 12
Productos de salida - Modelo de valor
Técnicas, prácticas y pautas - Catálogos de amenazas - Arboles de ataques. - Entrevistas - Reuniones - Valoración Delphi.

Fuente: MAGERIT - V 3.0. Libro 1: Método. Gobierno de España-Ministerio de Hacienda y Relaciones Públicas. 2012.

Para cada adquisición de este conocimiento puede ser necesario entrevistar a diferentes colectivos de la organización.

- Dirección o gerencia, que conocen las consecuencias para la misión de la organización.
- Responsables de los datos, que conocen las consecuencias de los fallos de seguridad.
- Responsables de los servicios, que conocen las consecuencias de la no prestación de los servicios o de su degradada.
- Responsables de sistemas de información y responsables de operación, que conocen las consecuencias de un incidente.

Para cada valoración conviene registrar la siguiente información:

- Dimensiones en las que el activo es relevante
- Estimación de la valoración en cada dimensión.
- Explicación de la valoración.
- Entrevistas realizadas de las que se han deducido las anteriores estimaciones.

- **MAGERIT Fase 2 Proceso P1 Actividad S1.1 Identificación de los activos.**

Entregables:

- Relación de activos a controlar
- Caracterización de los activos: valor propio y acumulado
- Relaciones entre activos

- **MAGERIT Fase 2 Proceso P1 Actividad s1.2 Dependencias de los activos.**

Entregables:

- Diagrama de dependencias entre activos

- **MAGERIT Fase 2 Proceso P1 Actividad S1.3 Valoración de los activos.**

Entregables:

- Informe de modelo de valor: informe de valor de los activos

MAGERIT Fase 2 Proceso P2: Caracterización de las amenazas.

- **MAGERIT Fase 2 Proceso P2 Actividad S2.1 Identificación de las amenazas.**

El objetivo de estas tareas es caracterizar el entorno al que se enfrenta el sistema, qué puede pasar, qué consecuencias se derivan y cómo de probable es que pase.

Tabla 6: Identificación de las amenazas

MAR: Análisis de riesgos MAR 1: Características de las amenazas MAR 21: Identificación de las amenazas
Objetivos - Identificar las amenazas relevantes cobre cada activo.
Productos de entrada - Resultados de la actividad MAR 1 - Informes relativos a defectos en los productos.
Productos de salida - Relación de amenazas posibles.
Técnicas, prácticas y pautas - Catálogos de amenazas - Arboles de ataques. - Entrevistas - Reuniones - Valoración Delphi.

Fuente: MAGERIT - V 3.0. Libro 1: Método. Gobierno de España-Ministerio de Hacienda y Relaciones Públicas. 2012.

En esta tarea se identifican las amenazas significativas sobre los activos identificados, tomando en consideración:

- El tipo de activo
- Las dimensiones en que el activo es valioso
- La experiencia de la Organización
- Los defectos reportados por los fabricantes y organismos de respuesta a incidentes de seguridad (CERTS)

Para cada amenaza sobre cada activo conviene registrar la siguiente información:

- Explicación del efecto de la amenaza
- Entrevistas realizadas de las que se ha deducido la anterior estimación.
- Antecedentes, si los hubiera, bien en la propia organización, bien en otras organizaciones que se haya considerado relevantes.

- **MAGERIT Fase 2 Proceso P2 Actividad S2.2 Valoración de las amenazas.**

Tabla 7: Valoración de las amenazas

MAR: Análisis de riesgos MAR 2: Características de las salvaguardas MAR 22: Valoración de las amenazas
Objetivos - Estimar la frecuencia de ocurrencia de cada amenaza sobre cada activo. - Estimar la degradación que causaría la amenaza del activo si legara a materializarse.
Productos de entrada - Resultados de la tarea MAR 21 - Series históricas de incidentes - Informes de defectos en los productos - Antecedentes: incidentes en la organización.
Productos de salida - Mapa de riesgos: informe de amenazas posibles, caracterizados por su frecuencia de ocurrencia y la degradación que causarían en los activos.
Técnicas, prácticas y pautas - Arboles de ataque - Entrevistas - Reuniones - Valoración Delphi.

Fuente: MAGERIT - V 3.0. Libro 1: Método. Gobierno de España-Ministerio de Hacienda y Relaciones Públicas. 2012.

En esta tarea se valoran las amenazas identificadas en la tarea anterior, tomando en consideración:

- La experiencia universal
- La experiencia del sector de actividad
- La experiencia del entorno en que se ubican los sistemas
- La experiencia de la propia organización
- Los informes anexos a los reportes de defectos proporcionados por los fabricantes y organismos de respuesta de seguridad (CERTS).

Para cada amenaza sobre cada activo conviene registrar la siguiente información:

- Estimación de la frecuencia de la amenaza
- Estimación del daño que causaría su materialización
- Entrevistas realizadas de las que se han deducido las anteriores estimaciones.

MAGERIT Fase 2 Proceso P3: Caracterización de las salvaguardas.

- **MAGERIT Fase 2 Proceso P3 Actividad S3.1 Identificación de las salvaguardas pertinentes.**

  Esta actividad consta de dos sub-tareas:

  MAR 31: Identificación de las salvaguardas pertinentes.

  MAR 32: Valoración de las salvaguardas.

Tabla 8: Identificación de salvaguardas pertinentes.

MAR: Análisis de riesgos MAR 1: Características de las salvaguardas MAR 31: Identificación de las salvaguardas pertinentes.
Objetivos - Identificar las salvaguardas convenientes para proteger el sistema.
Productos de entrada - Modelo de activos del sistema - Modelo de amenazas del sistema - Indicadores de impacto y riesgo residual - Informes de productos y servicios en el mercado.
Productos de salida - Declaración de aplicabilidad: relación justificada de las salvaguardas necesarias. - Relación de salvaguardas desplegadas.
Técnicas, prácticas y pautas - Catálogos de salvaguardas. - Arboles de ataque - Entrevistas - Reuniones.

Fuente: MAGERIT - V 3.0. Libro 1: Método. Gobierno de España-Ministerio de Hacienda y Relaciones Públicas. 2012.

Para cada salvaguarda conviene registrar la siguiente información:

- Descripción de la salvaguarda y su estado de implantación.
- Descripción de las amenazas a las que pretende hacer frente.
- Entrevistas realizadas de las que se ha deducido la anterior información.

En el proceso de descarte hay varias razones para eliminar una salvaguarda propuesta:

- Porque no es apropiada para el activo que necesitamos defender.
- Porque no es apropiada para la dimensión de seguridad que necesitamos defender.
- Porque no es efectiva oponiéndose a la amenaza que necesitamos defender.
- Porque es excesiva para el valor que tenemos que proteger.
- Porque disponemos de medidas alternativas.

- **MAGERIT Fase 2 Proceso P3 Actividad S3.2 Valoración de las salvaguardas.**

Tabla 9: Valoración de las salvaguardas.

MAR: Análisis de riesgos MAR 1: Características de las salvaguardas MAR 32: Valoración de las salvaguardas.
Objetivos - Determinar la eficacia de las salvaguardas pertinentes.
Productos de entrada - Evaluación de salvaguardas. Informe de salvaguardas desplegadas, caracterizados por su grado de efectividad. - Informe de insuficiencias: relación de salvaguardas que deberían estar, pero no están desplegadas en forma insuficiente.
Productos de salida - Declaración de aplicabilidad: relación justificada de las salvaguardas necesarias. - Relación de salvaguardas desplegadas.
Técnicas, prácticas y pautas - Catálogos de salvaguardas. - Arboles de ataque - Entrevistas - Reuniones.

Fuente: MAGERIT - V 3.0. Libro 1: Método. Gobierno de España-Ministerio de Hacienda y Relaciones Públicas. 2012.

En esta tarea se valora la efectividad de las salvaguardas identificadas en la tarea anterior, tomando en consideración:

- La idoneidad de la salvaguarda para el fin perseguido
- La calidad de la implantación
- La formación de los responsables de su configuración y operación.
- La formación de los usuarios, si tienen un papel activo.
- La existencia de controles de medida de su efectividad.
- La existencia de procedimientos de revisión regular.

Para cada salvaguarda conviene registrar la siguiente información:

- Estimación de su eficacia para afrontar aquella amenaza.
- Explicación de la estimación de eficacia.
- Entrevistas realizadas de las que se ha deducido la anterior estimación.

Proceso S7: Estimación del estado de riesgo En esta tarea se combinan los descubrimientos de las tareas anteriores (MAR 1, MAR 2 y MAR 3) para derivar estimaciones del estado de riesgo de la organización:

MAR 41: Estimación del impacto.

MAR 42: Estimación del riesgo

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

MAGERIT Fase 2 Proceso P4: Estimación del riesgo.

Tabla 10: Estimación del impacto

MAR: Análisis de riesgos MAR 4: Estimación del estado de riesgo MAR 41: Estimación del impacto
Objetivos - Determinar el impacto potencial al que está sometido el sistema - Determinar el impacto residual al que está sometido el sistema
Productos de entrada - Resultados de la actividad MAR 1: Caracterización de los activos. - Resultados de la actividad MAR 2: Caracterización de las amenazas. - Resultados de la actividad MAR 3: Caracterización de las salvaguardas.
Productos de salida - Informe de impacto (potencial) por activo - Informe de impacto residual por activo.
Técnicas, prácticas y pautas - Análisis mediante tablas. - Análisis algorítmico.

Fuente: MAGERIT - V 3.0. Libro 1: Método. Gobierno de España-Ministerio de Hacienda y Relaciones Públicas. 2012.

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

- 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.

MAGERIT Fase 2 Proceso P5: Estimación del impacto.

Tabla 11: Estimación del riesgo.

MAR: Análisis de riesgos MAR 4: Estimación del estado de riesgo MAR 41: Estimación del riesgo
Objetivos - Determinar el riesgo potencial al que está sometido el sistema. - Determinar el riesgo residual al que se está sometido el sistema.
Productos de entrada - Resultados de la actividad MAR 1: Caracterización de los activos. - Resultados de la actividad MAR 2: Caracterización de las amenazas. - Resultados de la actividad MAR 3: Caracterización de las salvaguardas. - Resultados de la actividad MAR 4: estimaciones de impacto.
Productos de salida - Informe de riesgo (potencial) por activo - Informe de riesgo residual por activo
Técnicas, prácticas y pautas - Análisis mediante tablas. - Análisis algorítmico.

Fuente: MAGERIT - V 3.0. Libro 1: Método. Gobierno de España-Ministerio de Hacienda y Relaciones Públicas. 2012.

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.

4. Catálogo de Elementos

Marca unas pautas en cuanto a:

a. 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.

a.1. Determinación de dependencias entre activos

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 o Información que se maneja o Servicios prestados.
- Servicios internos que estructuran ordenadamente el sistema de información.
- El equipamiento informático o Aplicaciones (software) o Equipos informáticos (hardware) o Comunicaciones o Soportes de información: discos, cintas, etc.

- El entorno: activos que se precisan para garantizar las siguientes capas o Equipamiento y suministros: energía, climatización, etc. o Mobiliario.
- Los servicios subcontratados a terceros.
- Las instalaciones físicas.
- El personal o Usuarios u Operadores y administradores o Desarrolladores

a.2. Valoración de los activos

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

No se está hablando de lo que cuestan las cosas. 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.

a.3. Dimensiones de los activos

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?

a.4. Valoración cualitativa de los activos

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

a.5. Valoración cuantitativa de los activos

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.

a.6. Criterios de valoración de los activos

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 O 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:

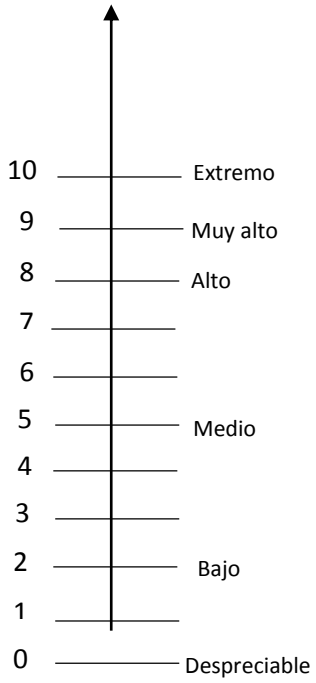


Tabla 12: Escala detallada de los criterios de valoración.

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 - V 3.0. Libro 1: Método. Gobierno de España-Ministerio de Hacienda y Relaciones Públicas. 2012.

b. Amenazas

Las amenazas son "cosas que ocurren". Y, de todo lo que puede ocurrir, interesa lo que puede pasarles a nuestros activos y causar un daño.

b.1. Identificación de las amenazas

- De origen natural.
- Del entorno (de origen industrial)

- Defectos de las aplicaciones
- Causadas por las personas de forma accidental
- Causadas por las personas de forma deliberada

b.2. 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.

Tabla 13: 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 - V 3.0. Libro 1: Método. Gobierno de España-Ministerio de Hacienda y Relaciones Públicas. 2012.

Tabla 14: 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 varios años
MB	1/100	Muy poco frecuente	Siglos

Fuente: MAGERIT - V 3.0. Libro 1: Método. Gobierno de España-Ministerio de Hacienda y Relaciones Públicas. 2012.

c. Salvaguardas

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.

c.1. 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:

- Tipo de activos a proteger, pues cada tipo se protege de una forma específica.
- Dimensión o dimensiones de seguridad que requieren protección.
- Amenazas de las que necesitamos protegernos.

Si existen salvaguardas alternativas

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

- El mayor o menor valor propio o acumulado sobre un activo, centrándonos en lo más valioso y obviando lo irrelevante.

- La mayor o menor probabilidad de que una amenaza ocurra, centrándonos en los riesgos más importantes.
- 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.

c.2. 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.
- **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. **Guía de Técnicas**

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.
- Árboles de ataque.
- Técnicas generales
- Técnicas gráficas

5. Herramientas: 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.

3.3 Metodología OCTAVE

3.3.1. Descripción de la metodología OCTAVE.

OCTAVE es una metodología para identificar y evaluar riesgos de seguridad de la información. Está destinado a ayudar a una organización a:

- Desarrollar criterios cualitativos de evaluación de riesgos que describan las tolerancias de riesgo operacional de la organización.
- Identificar activos que son importantes para la misión de la organización.
- Identificar vulnerabilidades y amenazas a esos activos.
- Determinar y evaluar las posibles consecuencias para la organización si se realizan amenazas.

Desde su lanzamiento en septiembre de 1999, ha habido una serie de actualizaciones y cambios en la metodología OCTAVE. La Tabla 15 proporciona una breve línea de tiempo de eventos significativos relacionados con OCTAVE.

Tabla 15: OCTAVE Timeline

FECHA	TÍTULO DE LA PUBLICACIÓN
Setiembre 1999	OCTAVE Framework, Version 1.0
Setiembre 2001	OCTAVE Framework, Version 2.0
Diciembre 2001	OCTAVE Criteria, Version 2.0
Setiembre 2003	OCTAVE-S v0.9
Marzo 2005	OCTAVE-S v1.0
Junio 2007	Introduction of OCTAVE Allegro v1.0

Guía de implementación de OCTAVE®-S, versión 1.0
Volumen 3: Pautas del método

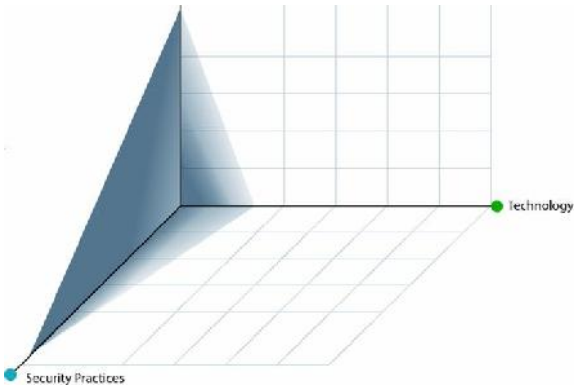
Ahora hay tres metodologías distintivas de OCTAVE disponibles para uso público: el método OCTAVE, OCTAVE-S y OCTAVE Allegro. La introducción de OCTAVE Allegro no pretende suplantar las metodologías anteriores de OCTAVE. OCTAVE Allegro es una variante que proporciona un proceso optimizado centrado en los activos de información. Sin embargo, cada método de OCTAVE tiene amplia aplicabilidad, y los

usuarios de estos métodos pueden seleccionar el enfoque que mejor se adapte a sus necesidades particulares de evaluación de riesgos de seguridad de la información.

De acuerdo a lo que se pretende en la tesis y a las características del lugar donde se ejecutará se utilizará OCTAVE-S.

OCTAVE-S es una variación del enfoque OCTAVE que se desarrolló para satisfacer las necesidades de organizaciones pequeñas y menos jerárquicas. Se adapta a los medios más limitados y las restricciones únicas que suelen encontrarse en organizaciones más pequeñas. Aunque el "aspecto y la sensación" de OCTAVE-S difiere del Método OCTAVE, la técnica produce los mismos tipos de resultados, incluida una estrategia de protección para toda la organización.

Figura 3: Riesgo Operacional y Prácticas de Seguridad



Fuente: Guía de implementación de OCTAVE®-S, versión 1.0
Volumen 3: Pautas del método

3.3.2. Método de gestión de riesgos de OCTAVE-S.

Dada la delimitación del trabajo del trabajo de investigación solo abarcaron la Fase 1 y Fase 2 en su totalidad pero en la Fase 3 solo se desarrolló hasta la actividad selección de enfoques de mitigación.

Fase 1: compilar perfiles de amenazas basados en activos.

La fase 1 es una evaluación de los aspectos organizacionales. Durante esta fase, el equipo de análisis define los criterios de evaluación de impacto que se utilizarán más adelante para evaluar los riesgos. También identifica los activos organizacionales importantes y evalúa la práctica de seguridad actual de la organización. El equipo completa todas las tareas por sí mismo, recolectando información adicional solo

cuando es necesario. Luego selecciona de tres a cinco activos críticos para analizar en profundidad en función de la importancia relativa para la organización.

Finalmente, el equipo define los requisitos de seguridad y un perfil de amenaza para cada activo crítico. La Tabla 16 ilustra los procesos y actividades de la Fase 1.

Tabla 16: Procesos y Actividades

FASE	PROCESO	ACTIVIDAD
Fase 1: compilar perfiles de amenazas basados en activos	Proceso S1: Identificar información de la organización	S1.1 Establecer criterios de evaluación de impacto
		S1.2 Identificar los activos de la organización
		S1.3 Evaluar las prácticas de seguridad organizacional
	Proceso S2: Crear perfiles de amenazas	S2.1 Seleccionar activos críticos
		S2.2 Identificar los requisitos de seguridad para los activos críticos
		S2.3 Identificar amenazas a los activos críticos

Fuente: Guía de implementación de OCTAVE®-S, versión 1.0
Volumen 3: Pautas del método

Proceso S1: Identificar información de la organización.

Este proceso se centra en desarrollar criterios para evaluar el impacto de los riesgos para la organización, identificar los activos de la organización y evaluar las prácticas de seguridad de la organización.

- **S1.1 Establecer criterios de evaluación de impacto.**

  Paso 1

  Defina un conjunto cualitativo de medidas (alto, medio, bajo) con respecto al cual evaluará el efecto de un riesgo en la misión y los objetivos comerciales de su organización.

- **S1.2 Identificar los activos de la organización.**

  Paso 2

  Identifique los activos relacionados con la información en su organización (información, sistemas, aplicaciones, personas).

- **S1.3 Evaluar las prácticas de seguridad organizacional.**

  Paso 3a

  Determine en qué medida cada práctica en la encuesta es utilizada por la organización.

  Paso 3b

  Al evaluar cada área de práctica de seguridad utilizando la encuesta del Paso 3a, documente ejemplos detallados de

  - Lo que su organización actualmente está haciendo bien en esta área (prácticas de seguridad)
  - Lo que su organización actualmente no está haciendo bien en esta área (vulnerabilidades organizacionales)

  Paso 4

  Después de completar los pasos 3a y 3b, asigne un estado de semáforo (rojo, amarillo o verde) a cada área de práctica de seguridad. El estado del semáforo debe reflejar qué tan bien cree que su organización se está desempeñando en cada área.

Proceso S2: Crear perfiles de amenazas.

Este proceso se enfoca en seleccionar activos críticos de aquellos previamente identificados, identificar los requisitos de seguridad para esos activos e identificar las amenazas a esos activos críticos.

- **S2.1 Seleccionar activos críticos.**

  Paso 5

  Revise los activos relacionados con la información que identificó durante el Paso 2 y seleccione hasta cinco (5) activos que sean más críticos para la organización.

Paso 6

Comience una Hoja de trabajo de información de activos críticos para cada activo crítico. Registre el nombre del activo crítico en la Hoja de trabajo de información de activos críticos apropiada.

Paso 7

Registre su razón de ser para seleccionar cada activo crítico en la Hoja de trabajo de información de activos críticos de ese activo.

Paso 8

Registre una descripción para cada activo crítico en la Hoja de trabajo de información de activos críticos de ese activo. Considere quién usa cada activo crítico y quién es el responsable de él.

Paso 9

Registre los activos que están relacionados con cada activo crítico en la Hoja de trabajo de información de activos críticos de ese activo. Consulte la Hoja de trabajo de identificación de activos para determinar qué activos están relacionados con el activo crítico.

- **S2.2 Identificar los requisitos de seguridad para los activos críticos.**

Paso 10

Registre los requisitos de seguridad para cada activo crítico en la Hoja de trabajo de información de activos críticos de ese activo.

Paso 11

Para cada activo crítico, registre el requisito de seguridad más importante en la Hoja de trabajo de información de activos críticos de ese activo.

- **S2.3 Identificar amenazas a los activos críticos.**

  Paso 12

  Complete todos los árboles de amenazas apropiados para cada activo crítico. Marque cada rama de cada árbol para la cual hay una posibilidad no despreciable de una amenaza para el activo.

  A medida que complete este paso, si tiene dificultades para interpretar una amenaza en cualquier árbol de amenazas, revise la descripción y ejemplos de esa amenaza en la Guía de traducción de amenazas.

  Paso 13

  Registre ejemplos específicos de actores amenazantes en la Hoja de trabajo del perfil de riesgos para cada combinación de actor-motivo aplicable.

  Paso 14

  Registre la fuerza del motivo de las amenazas deliberadas debidas a los actores humanos. También registre la confianza que tiene en su estimación de la fuerza del motivo del actor.

  Paso 15

  Registre con qué frecuencia ha ocurrido cada amenaza en el pasado. También registre qué tan preciso cree que son sus datos.

  Paso 16

  Registre las áreas de preocupación para cada fuente de amenaza donde sea apropiado. Un área de preocupación es un escenario que define cómo las amenazas específicas podrían afectar el activo crítico.

Fase 2: identificar vulnerabilidades de infraestructura.

Durante esta fase, el equipo de análisis lleva a cabo una revisión de alto nivel de la infraestructura informática de la organización, centrándose en la medida en que los responsables de mantenimiento de la infraestructura consideran la seguridad. El equipo de análisis primero analiza cómo las personas usan la infraestructura

informática para acceder a los activos críticos, generando clases clave de componentes y quién es responsable de configurar y mantener esos componentes.

El equipo luego examina hasta qué punto cada parte responsable incluye seguridad en sus prácticas y procesos de tecnología de la información. Los procesos y actividades de la Fase 2 se muestran en la Tabla 17.

Tabla 17: Procesos y Actividades Fase 2

FASE	PROCESO	ACTIVIDAD
Fase 2: identificar vulnerabilidades de infraestructura	Proceso S3: Examinar la infraestructura informática en relación con los activos críticos	S3.1 Examinar las rutas de acceso
		S3.2 Analizar procesos relacionados con la tecnología

Fuente: Guía de implementación de OCTAVE®-S, versión 1.0
Volumen 3: Pautas del método

Proceso S3: Examinar la infraestructura informática en relación con los activos críticos.

Este proceso se enfoca en examinar las rutas de acceso en la infraestructura para los activos críticos y luego analizar los procesos relacionados con la tecnología asociados con la infraestructura.

- **S3.1 Examinar las rutas de acceso.**

  Paso 17

  Seleccione el sistema (s) de interés para cada activo crítico (es decir, el sistema más estrechamente relacionado con el activo crítico).

  Paso 18a

  Revise las rutas utilizadas para acceder a cada activo crítico y seleccione las clases clave de componentes relacionados con cada activo crítico.

  Determine qué clases de componentes son parte del sistema de interés.

  Paso 18b

  Determine qué clases de componentes sirven como puntos de acceso intermedios (es decir, componentes que se utilizan para transmitir información y aplicaciones del sistema de interés para las personas).

Paso 18c

Determine qué clases de componentes, tanto internos como externos a las redes de la organización, son utilizados por personas (por ejemplo, usuarios, atacantes) para acceder al sistema.

Paso 18d

Determine dónde se almacena la información del sistema de interés para fines de respaldo.

Paso 18e

Determine qué otros sistemas acceden a la información o las aplicaciones del sistema de interés y qué otras clases de componentes se pueden usar para acceder a información o servicios críticos del sistema de interés.

- **S3.2 Analizar procesos relacionados con la tecnología.**

Paso 19a

Determine las clases de componentes que están relacionados con uno o más activos críticos y que pueden proporcionar acceso a esos activos. Marque el camino a cada clase seleccionada en los pasos 18a-18e. Tenga en cuenta cualquier subclase relevante o ejemplos específicos cuando corresponda.

Paso 19b

Para cada clase de componentes documentados en el Paso 19a, tenga en cuenta qué activos críticos están relacionados con esa clase.

Paso 20

Para cada clase de componentes documentados en el Paso 19a, anote la persona o grupo responsable de mantener y asegurar esa clase de componente.

Paso 21

Para cada clase de componentes documentada en el Paso 19a, observe en qué medida esa clase es resistente a los ataques de red. También registre cómo llegó a esa conclusión.

Finalmente, documente cualquier contexto adicional relevante para su análisis de infraestructura.

Fase 3: Desarrollar estrategias y planes de seguridad.

Durante la Fase 3, el equipo de análisis identifica los riesgos para los activos críticos de la organización y decide qué hacer con ellos. Con base en un análisis de la información recopilada, el equipo crea una estrategia de protección para la organización y planes de mitigación para abordar los riesgos para los activos críticos. Las hojas de trabajo de OCTAVE-S utilizadas durante la Fase 3 están altamente estructuradas y estrechamente vinculadas al catálogo de prácticas de OCTAVE, lo que permite que el equipo relacione sus recomendaciones de mejora con un punto de referencia aceptado de las prácticas de seguridad. La Tabla 18 muestra los procesos y actividades de la Fase 3.

Tabla 18: Procesos y Actividades de la Fase 3

FASE	PROCESO	ACTIVIDAD
Fase 3: Desarrollar estrategias y planes de seguridad	Proceso S4: identificar y analizar los riesgos	S4.1 Evaluar los impactos de las amenazas
		S4.2 Establecer criterios de evaluación de probabilidad
		S4.3 Evalúa Probabilidades de Amenazas
	Proceso S5: Desarrollar estrategias de protección y planes de mitigación	S5.1 Describir la estrategia de protección actual
		S5.2 Seleccionar enfoques de mitigación
		S5.3 Desarrollar planes de mitigación de riesgos
		S5.4 Identificar cambios en la estrategia de protección
		S5.5 Identifique los próximos pasos

Fuente: Guía de implementación de OCTAVE®-S, versión 1.0
Volumen 3: Pautas del método

Proceso S4: Identificar y analizar los riesgos.

Este proceso se centra en la evaluación del impacto y la probabilidad de amenazas a los activos críticos y el establecimiento de criterios de evaluación de probabilidad.

- **S4.1 Evaluar los impactos de las amenazas.**

  Paso 22

  Utilizando los criterios de evaluación de impacto como guía, asigne un valor de impacto (alto, medio o bajo) para cada amenaza activa a cada activo crítico.

- **S4.2 Establecer criterios de evaluación de probabilidad.**

  Paso 23 (opcional)

  Defina un conjunto cualitativo de medidas (alto, medio, bajo) con respecto al cual evaluará la probabilidad de que ocurra una amenaza.

- **S4.3 Evalúa Probabilidades de Amenazas.**
  Paso 24 (opcional)

  Utilizando los criterios de evaluación de probabilidad como guía, asigne un valor de probabilidad (alto, medio o bajo) para cada amenaza activa a cada activo crítico. Documente su nivel de confianza en su estimación de probabilidad.

Proceso S5: Desarrollar estrategias de protección y planes de mitigación.
Este proceso se enfoca en definir una estrategia de protección y planes de mitigación, así como los próximos pasos necesarios para implementar los resultados de la evaluación de OCTAVE-S.

- **S5.1 Describir la estrategia de protección actual.**
  Paso 25

  Transfiera el estado de semáforo de cada área de práctica de seguridad al área correspondiente en la hoja de trabajo de estrategia de protección.

  Para cada área de práctica de seguridad, identifique el enfoque actual de su organización para abordar esa área

- **S5.2 Seleccionar enfoques de mitigación.**
  Paso 26

  Transfiera el estado de semáforo de cada área de práctica de seguridad de la Hoja de trabajo de prácticas de seguridad a la sección "Áreas de práctica de

seguridad" (Paso 26) de la Hoja de trabajo de perfil de riesgo de cada activo crítico.

Paso 27

Seleccione un enfoque de mitigación (mitigar, aplazar, aceptar) para cada riesgo activo.

Para cada riesgo que haya decidido mitigar, circule una o más áreas de práctica de seguridad para las cuales tiene la intención de implementar actividades de mitigación.

4. Catálogos de OCTAVE-S.

En el volumen 3 de la guía de implementación de OCTAVE-S, en cada actividad se hace referencia a los catálogos de la metodología.

En la actividad S1.1 Establecer criterios de evaluación de impacto se muestra el siguiente catálogo.

- **Impacto**

  El efecto de una amenaza en la misión y los objetivos comerciales de una organización.

- **Valor de impacto**

  Una medida cualitativa del impacto de un riesgo específico para la organización (alto, medio o bajo).

- **Criterios de evaluación de impacto**

  Un conjunto de medidas cualitativas contra las cuales se evalúa el efecto de cada riesgo en la misión y los objetivos comerciales de una organización. Los criterios de evaluación de impacto definen rangos de impactos altos, medios y bajos para una organización.

En la actividad S1.2 Identificar los activos de la organización, se muestra el siguiente catálogo.

- **Activo**

  Algo de valor para la empresa. Los activos de tecnología de la información son la combinación de activos lógicos y físicos y se agrupan en clases específicas (información, sistemas, servicios y aplicaciones, personas).

- **Categorías de activos**
  - Información: datos documentados (en papel o electrónicos) o propiedad intelectual utilizados para cumplir con la misión de una organización.
  - Sistemas: una combinación de activos de información, software y hardware que procesa y almacena información. Cualquier host, cliente o servidor puede considerarse un sistema.
  - Servicios y aplicaciones: aplicaciones y servicios de software (sistemas operativos, aplicaciones de base de datos, software de red, aplicaciones de oficina, aplicaciones personalizadas, etc.) que procesan, almacenan o transmiten información.
  - Personas: las personas de una organización que poseen habilidades, conocimientos y experiencia únicos que son difíciles de reemplazar. En una evaluación de riesgos de seguridad de la información, los activos deben estar vinculados a la información de alguna manera.

    En una evaluación de riesgos de seguridad de la información, los activos deben estar vinculados a la información de alguna manera.

En la actividad 1.3 Evaluar las prácticas de seguridad organizacional, se muestra el siguiente catálogo.

- **Prácticas de seguridad**

  Acciones que ayudan a iniciar, implementar y mantener la seguridad dentro de una empresa.

- **Vulnerabilidades organizacionales**

  Debilidades en la política o práctica organizacional que pueden resultar en acciones no autorizadas.

- **Prácticas estratégicas**

  Prácticas de seguridad que se centran en cuestiones de organización a nivel de políticas. Incluyen asuntos relacionados con el negocio, así como también cuestiones que requieren planes y participación en toda la organización.

- **Prácticas operacionales**

  Prácticas de seguridad que se centran en cuestiones relacionadas con la tecnología. Incluyen cuestiones relacionadas con la forma en que las personas usan, interactúan y protegen la tecnología en el día a día.

- **Estado de semáforo**

  Qué tan bien se desempeña una organización en un área de práctica de seguridad. Los siguientes colores se asignan a un área según el rendimiento percibido en esa área:

  - Verde: la organización está realizando las prácticas de seguridad en el área muy bien; no hay una necesidad real de mejora.
  - Amarillo: la organización está realizando las prácticas de seguridad hasta cierto punto; Hay posibilidad de mejora.
  - Rojo: la organización no está realizando las prácticas de seguridad en el área; hay espacio significativo para la mejora.

  Las siguientes áreas de práctica de seguridad se evalúan en OCTAVE-S.

En la actividad 2.1 Seleccionar activos críticos, se muestra el siguiente catálogo.

- **Activos críticos**

  Los activos más importantes para una organización. La organización sufrirá un gran impacto adverso si

  - Un activo crítico se revela a personas no autorizadas
  - Un activo crítico se modifica sin autorización
  - Un activo crítico se pierde o se destruye
  - El acceso a un activo crítico se interrumpe

En la actividad 2.2 Identificar los requisitos de seguridad para los activos críticos, se muestra el siguiente catálogo.

- **Requisitos de seguridad**

  Declaraciones que describen las cualidades de los activos relacionados con la información que son importantes para una organización. Los requisitos de seguridad típicos son la confidencialidad, la integridad y la disponibilidad.

  - Confidencialidad

    La necesidad de mantener la información privada, confidencial o personal privado e inaccesible para cualquier persona que no esté autorizada para verla.

  - Integridad

    La autenticidad, precisión e integridad de un activo.

  - Disponibilidad

    Cuándo o con qué frecuencia debe estar presente o listo para usar un activo.

En la actividad 2.3 Identificar amenazas a los activos críticos, se muestra el siguiente catálogo.

- **Amenaza**

  Una indicación de un posible evento indeseable. Una amenaza se refiere a una situación en la que una persona puede hacer algo indeseable (un atacante que inicia un ataque de denegación de servicio contra el servidor de correo electrónico de una organización) o una ocurrencia natural puede provocar un resultado indeseable (un incendio que daña el hardware de tecnología de información de una organización).

- **Perfil de amenaza**

  Una forma estructurada de presentar una gama de amenazas a un activo crítico. Las amenazas en el perfil se agrupan según la fuente de la amenaza.

- **Perfil de amenaza genérico**

Un catálogo de amenazas que contiene un rango de todas las posibles amenazas bajo consideración. El perfil de amenaza genérico es un punto de partida para crear un perfil de amenaza único para cada activo crítico.

Las amenazas se representan utilizando las siguientes propiedades:

- Activo: algo de valor para la empresa
- Acceso: cómo un agente accede al activo (acceso a la red, acceso físico). El acceso se aplica solo a los actores humanos.
- Actor: quién o qué puede violar los requisitos de seguridad (confidencialidad, integridad, disponibilidad) de un activo
- Motivo: la intención de un actor (por ejemplo, deliberada o accidental). El motivo se aplica solo a los actores humanos.
- Resultado: el resultado inmediato (divulgación, modificación, destrucción, pérdida, interrupción) de la violación de los requisitos de seguridad de un activo En OCTAVE-S, las amenazas se representan visualmente en una estructura jerárquica, a menudo denominada árbol de amenazas.

Hay un árbol de amenazas para cada una de las siguientes categorías de fuente de amenaza:

Tabla 19: Categorías de Amenazas.

CATEGORÍA	DEFINICIÓN
Actores humanos que utilizan el acceso a la red	Las amenazas en esta categoría son amenazas basadas en la red a los activos críticos de una organización. Requieren una acción directa de una persona y pueden ser de naturaleza deliberada o accidental.
Actores humanos que usan acceso físico	Las amenazas en esta categoría son amenazas físicas a los activos críticos de una organización. Requieren una acción directa de una persona y pueden ser de naturaleza deliberada o accidental.
Problemas del Sistema	Las amenazas en esta categoría son problemas con los sistemas de tecnología de la información de una organización. Los ejemplos incluyen defectos de hardware, defectos de software, código malicioso (por ejemplo, virus) y otros problemas relacionados con el sistema.
Otros problemas	Las amenazas en esta categoría son problemas o situaciones que están fuera del control de una organización. Esta categoría de amenazas incluye los desastres naturales (por ejemplo, inundaciones, terremotos) y los riesgos de interdependencia. Los riesgos de interdependencia incluyen la falta de disponibilidad de infraestructuras críticas (por ejemplo, suministro de energía).

Fuente: Guía de implementación de OCTAVE®-S, versión 1.0
Volumen 3: Pautas del método

En la actividad 4.1 Evaluar los impactos de las amenazas, se muestra el siguiente catálogo.

- **Riesgo**

  La posibilidad de sufrir daño o pérdida. El riesgo se refiere a una situación en la que una persona puede hacer algo indeseable o una ocurrencia natural puede causar un resultado indeseable, lo que resulta en un impacto o consecuencia negativa.

  Un riesgo se compone de

  - Un evento
  - Incertidumbre
  - Una consecuencia

  En seguridad de la información, el evento básico es una amenaza.

  La incertidumbre está incorporada en gran parte de la información recopilada durante la evaluación de OCTAVE-S.

  Existe incertidumbre sobre si se producirá una amenaza y si la organización está suficientemente protegida contra el actor de la amenaza. La incertidumbre a menudo se representa utilizando la probabilidad de ocurrencia o probabilidad.

  La consecuencia que finalmente importa en el riesgo de seguridad de la información es el impacto resultante en la organización debido a una amenaza. Impacto describe cómo una organización puede verse afectada en función de los siguientes resultados de amenaza:

  - Divulgación de un activo crítico
  - Modificación de un activo crítico
  - Pérdida / destrucción de un activo crítico
  - Interrupción de un activo crítico

  Los resultados enumerados anteriormente están directamente relacionados con los activos; describen el efecto de las amenazas sobre los activos.

El impacto se centra en la organización; es el enlace directo a la misión de la organización y los objetivos comerciales.

En la Actividad S1.1, se crearon los criterios de evaluación de impacto para las siguientes áreas de impacto:

- reputación / confianza del cliente
- vida / salud de los clientes
- multas / sanciones legales
- financiero
- productividad
- otro

En la actividad 4.2 Establecer criterios de evaluación de probabilidad, se muestra el siguiente catálogo.

- **Probabilidad**

  La probabilidad de que ocurra un evento.

- **Valor de probabilidad**

  Una medida cualitativa de la probabilidad de una amenaza (alta, media o baja).

- **Criterios de evaluación de probabilidad**

  Un conjunto de medidas cualitativas utilizadas para estimar la probabilidad de que ocurra una amenaza. Los criterios de evaluación de probabilidad definen rangos de frecuencia para probabilidades altas, medias y bajas; indican con qué frecuencia se producen amenazas en un período de tiempo común.

- **Tiempo entre eventos**

  Una estimación de la frecuencia con que puede ocurrir un evento (por ejemplo, semanalmente, una vez cada dos años)

- **Frecuencia anualizada**

  La probabilidad proyectada de que ocurra una amenaza en un año determinado.

Las probabilidades de amenazas a la seguridad de la información se estiman utilizando una combinación de datos objetivos, experiencia subjetiva y experiencia. Si está utilizando OCTAVE-S por primera vez, es probable que carezca de datos objetivos relacionados con las amenazas. También puede carecer de experiencia y conocimientos en seguridad de la información y / o gestión de riesgos. Por esta razón, la probabilidad se considera opcional en OCTAVE-S. Cada equipo necesita decidir si usa la probabilidad y cómo usarla.

En OCTAVE-S, los valores de probabilidad se definen mediante un conjunto de criterios de evaluación que se categorizan según la frecuencia de ocurrencia. Los criterios de evaluación de probabilidad definen un conjunto estándar de definiciones para los valores de probabilidad. Estos criterios definen medidas altas, medias y bajas de probabilidades de amenaza.

Las medidas de probabilidad se definen considerando un rango de frecuencias (es decir, la probabilidad de que ocurra una amenaza en un año determinado):

- Diario
- Semanal
- Mensual
- 4 veces por año
- 2 veces por año
- Una vez al año
- Una vez cada 2 años
- Una vez cada 5 años
- Una vez cada 10 años
- Una vez cada 20 años
- Una vez cada 50 años

En la actividad 4.3 Evalúa Probabilidades de Amenazas, se muestra el siguiente catálogo.

Un riesgo se compone de

- Un evento
- Incertidumbre
- Una consecuencia

5. Técnicas de OCTAVE-S.

Esta versión no comienza con el conocimiento formal sino con la obtención de talleres para recopilar información sobre los elementos importantes, los requisitos de seguridad, las amenazas y las prácticas de seguridad. El supuesto es que el equipo de análisis de esta información ya se conoce.

Encontrará las hojas de cálculo de OCTAVE-S en los volúmenes 4-9 de la Guía de implementación de OCTAVE®-S, versión 1.0

- Volumen 4: Libro de trabajo de información organizacional

  Este volumen proporciona hojas de trabajo para toda la información de nivel organizacional recopilada y analizada durante OCTAVE-S.

- Volumen 5: libro de trabajo de activos críticos para información

  Este volumen proporciona hojas de trabajo para documentar datos relacionados con activos críticos que se clasifican como información.

- Volumen 6: libro de trabajo de activos críticos para sistemas

  Este volumen proporciona hojas de trabajo para documentar datos relacionados con activos críticos que se clasifican como sistemas.

- Volumen 7: libro de trabajo de activos críticos para aplicaciones

  Este volumen proporciona hojas de trabajo para documentar datos relacionados con activos críticos que se clasifican como aplicaciones.

- Volumen 8: Libro de trabajo de activos críticos para las personas

  Este volumen proporciona hojas de trabajo para documentar los datos relacionados con los activos críticos que se clasifican como personas.

- Volumen 9: Cuaderno de trabajo de estrategia y plan

  Este volumen proporciona hojas de trabajo para registrar la estrategia de protección actual y deseada y los planes de mitigación de riesgos.

6. Herramientas de OCTAVE-S.

Las actividades de preparación de SM (OCTAVE®) -S son importantes porque establecen el escenario para una evaluación exitosa. Durante la preparación, usted determina cómo su organización llevará a cabo OCTAVE-S. Además, abordará directamente los siguientes factores clave de éxito:

- Obtener patrocinio de la gerencia superior para la evaluación
- Seleccionar el equipo de análisis para dirigir la evaluación
- Establecer el alcance de la evaluación

El Volumen 2: Pautas de preparación, contiene antecedentes y orientación para prepararse para realizar una evaluación de OCTAVE-S

3.4 Apetito Y Tolerancia al riesgo.

2.3.1 Apetito al Riesgo.

El Apetito de Riesgo es una ponderación de alto nivel de cuánto riesgo la administración y la Junta están dispuestos a aceptar en el logro de sus metas. (Riesgos G. d., España: La Fábrica de Pensamiento del Instituto de Auditores Internos.)

Características principales:

La gerencia y la Junta deben formular el apetito al riesgo a nivel de entidad.

Las compañías pueden expresar su apetito al riesgo como el equilibrio aceptable del crecimiento, los riesgos y el retorno, o como una medida de valor agregado para los accionistas ajustada al riesgo.

El apetito se puede definir mediante el uso de un mapa de riesgos. Entidades, tales como organizaciones sin fines de lucro, expresan su apetito al riesgo como el nivel de riesgo que ellos aceptarían al proporcionar valor a sus partes relacionadas. (Riesgos, 2013)

2.3.2 Tolerancia al Riesgo.

Tolerancia al Riesgo es el nivel aceptable de variación en relación a la concesión de un objetivo. Algunos de los aspectos claves, que debemos tener presente:

La tolerancia al riesgo es medible, preferiblemente en las mismas unidades de los objetivos relacionados.

Al establecer la tolerancia al riesgo la gerencia considera la importancia relativa de los objetivos relacionados.

La tolerancia al riesgo se alinea con el apetito al riesgo. ¿Qué considera alto (qué exposición no está dispuesta a aceptar)?

¿En qué tipo de escenarios se sentiría la gerencia incomoda de manejar o enfrentar?

CAPÍTULO IV DESARROLLO DEL MODELO DE MADUREZ PARA LA EVALUACIÓN DEL CONTROL INTERNO

4.1. Análisis y gestión de Riesgos de los activos de TI de la Unidad de Red Telemática de la Universidad Nacional Pedro Ruiz Gallo aplicando la metodología MAGERIT v3.

Dada la delimitación del trabajo de investigación solo abarcará las actividades que están incluidas en las tareas de caracterización de los activos, amenazas y salvaguardas. En la última tarea solo hasta la actividad de tratamiento de riesgo.

Aplicando la etapa de Análisis de riesgos y catálogo de elementos que esta metodología plantea para comprobar si MAGERIT es la metodología más adecuada. Identificando dentro de la Unidad de Red Telemática de la Universidad Nacional Pedro Ruiz Gallo los activos, las dependencias entre estos, la amenazas así como la valorización de las mismas, la probabilidad de impacto, el riesgo y culminar con el tratamiento de riesgo.

4.1.1 Análisis de riesgos.

El objetivo del análisis de riesgos fue determinar y evaluar el riesgo de los activos de TI que forman parte de los procesos y servicios de la gestión académica pre-grado que brinda la Unidad de Red Telemática de la Universidad Nacional Pedro Ruiz Gallo, siguiendo los pasos establecidos por la metodología MAGERIT. Los datos de esta etapa fueron obtenidos mediante entrevistas, llenado de formularios realizados en colaboración con del jefe de la Unidad de Red Telemática.

1.1. Caracterización de los activos.

El objetivo de las actividades englobadas en esta actividad fue identificar los activos que componen los servicios y procesos que se desarrollan en la gestión académica pre – grado en la Unidad de Red Telemática de la Universidad Nacional Pedro Ruiz Gallo; así como también se definió las dependencias entre ellos. Paso siguiente se realizó la valoración según la importancia que tenga cada activo en el caso de estudio.

1.1.1. Identificación de los Activos.

Objetivo de la actividad

El objetivo de la actividad fue identificar los activos que forman parte de los servicios y procesos de la gestión académica que brinda la Unidad de Red Telemática de la Universidad Nacional Pedro Ruiz Gallo, determinando sus características y atributos del activo a tratar. Los cuales fueron código, nombre y una descripción.

Consideraciones previas

Para el desarrollo de esta tarea se tomó en cuenta lo siguiente.

- En el caso del código usado para cada activo se utilizó el código del grupos de activo al que pertenece (del catálogo que MAGERIT ofrece) seguido de dos letras más agregados por el autor, que en su mayor parte son primeras letras de las palabras que forman el nombre de cada activo.
- Para los nombres de cada activo se utilizó el que tiene asignado en la Unidad de Red Telemática.
- Se agregó una columna titulada Descripción del activo cuya información fue obtenida de la entrevista con el jefe encargado de la Unidad de Red Telemática.

Desarrollo de la actividad

La metodología MAGERIT nos plantea agrupar a los activos en 8 capas según su tipo, como son:

[S] Servicios

[SW] Aplicaciones
[HW] Equipos Informáticos
[COM] Redes de comunicaciones
[MEDIA] Soportes de información
[AUX] Equipamiento auxiliar
[L] Instalaciones
[P] Personal

Mencionados también en el Marco Teórico.
En esta tarea se identificaron los activos que intervienen con la gestión académica de la Universidad Nacional Pedro Ruiz Gallo. Se decidió delimitar el análisis y gestión de riesgos en los activos de TI, y aplicarlo solo en la gestión académica pre-grado de la Universidad Nacional Pedro Ruiz Gallo porque consideramos que dicha gestión es un elemento primordial en la institución, que si este servicio llegará a faltar o pueda verse afectado puede perjudicar tanto a la institución como a los usuarios ya sea internos o externos.

Los datos fueron obtenidos en una entrevista realizada con el Administrador de la Unidad de Red Telemática, cuyos resultados pueden ser vistos en el anexo Metodología MAGERIT.

A continuación describimos los 8 grupos en los cuales se dividen los activos de TI en la Unidad de Red Telemática.

[S] Servicios. Son servicios auxiliares que forman parte de la Unidad de Red Telemática.

[HW] Hardware (equipos informáticos). Los medios materiales, físicos, destinados a soportar directamente o indirectamente los servicios. Incluye tanto instalaciones dedicadas como servicios de comunicaciones contratadas.

[COM] Redes de Comunicaciones. Los dispositivos físicos que permiten almacenar la información de forma permanente de la Unidad de Red Telemática.

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

[AUX] Equipamiento auxiliar. Se consideran otros equipos que sirven de soporte, sin estar directamente relacionados con datos.

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

[P] Personal. Personas que trabajan en la unidad de Red Telemática.

Al culminar la tarea se obtuvo la lista de los 30 activos, tabla que podemos visualizar en el capítulo IV Resultados y Discusión.

1.1.2. Dependencias entre los activos.

Objetivo de la actividad

Identificar el grado de dependencia donde la seguridad de los activos que son superiores, depende de los activos inferiores de la Unidad de Red Telemática de la Universidad Nacional Pedro Ruiz Gallo.

Consideraciones previas

Para el desarrollo de la tarea se realizaron las siguientes actividades.

- Identificación de los activos superiores e inferiores con la colaboración del jefe de la Unidad del Red Telemática.
- Se utilizó la estructura que plantea MAGERIT para definir las dependencias agrupándolos en capas.

En la siguiente tabla, teniendo en cuenta las dependencias para operar, funcionalidad y almacenamiento de datos, se determina la siguiente matriz de dependencias entre activos (según el tipo de activo que corresponda). Podremos ver la lista completa de activos y dependencias en el Anexo Metodología MAGERIT.

Tabla 20: Matriz dependencia de activos según su la capa a la que pertenecen

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

Fuente: Elaborado por los autores.

Desarrollo de la actividad

Como resultado de la matriz de dependencia podemos observar que:

- Los activos que pertenecen al grupo de servicios [S] dependen de los activos que forman parte de [SW], [HW], [COM], [AUX], [L] y [P].
- Los activos que forman parte del grupo de Software [SW] dependen de los activos del grupo de [HW], [COM], [MEDIA], [AUX], [L] Y [P].
- Los activos que forman parte del grupo de Hardware [HW], dependen de los activos del grupo de [AUX], [L] y [P].
- Los activos de Redes de Comunicaciones [COM] dependen de los activos de [AUX], [L] y [P].
- Los activos de Soportes de Comunicación [MEDIA] dependen de los activos que forman parte de los activos del grupo [L] y [P].
- Los activos que forman parte del grupo de Equipamiento Auxiliar [AUX], dependen de los activos que forman parte de los activos de los grupos [L] y [P].
- Los activos del grupo de Instalaciones [L] dependen de los activos del grupo [P].
- A continuación observamos el árbol de dependencias con los activos de TI de la unidad de Red Telemática.

1.1.3. Valoración de los activos.

Objetivo de la tarea

El objetivo de la tarea fue identificar en qué dimensión es valioso el activo de TI perteneciente al sistema académico de la Unidad de Red Telemática de la Universidad Nacional Pedro Ruiz Gallo.

Consideraciones previas

Para el desarrollo de la actividad se hizo lo siguiente:

- Se entrevistó al jefe de la Unidad de Red telemática, para obtener los datos a valorar.
- Valorar los activos en las 5 dimensiones que MAGERIT plantea para valorar el activo.
- Se utilizaron los criterios de valoración que brinda MAGERIT. Pero algunos de ellos fueron excluidos, más adelante se detalla las razones de porque fueron excluidos.

Se consideraron datos importantes como dimensiones y criterios de valuación.

a. 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

b. Criterios de valoración

   MAGERIT nos plantea diferentes criterios de valoración. Para el presente proyecto solo se han elegido las que se acomodan a los procesos y servicios que ofrece la Unidad de Red Telemática de la Universidad Nacional Pedro Ruiz Gallo.

Se excluyeron los siguientes criterios:

- *Obligaciones legales*. Se excluyó porque no se evalúa el complimiento de contrato con terceros o con entidades supervisoras por que las tecnologías de la Universidad no brinda servicios de ese tipo solo ofrece de carácter interno.
- *Interese comerciales o económicos.* Este criterio se excluyó ya que los servicios y proceso de la Unidad de Red Telemática son de uso interno.
- *Orden Público.* Se excluyó porque los servicios que ofrece la Unidad de Red telemática es de uso interno.
- *Pérdida de confianza.* Este criterio se refiere a la publicidad negativa de la organización en caso se vea afectada por alguna amenaza. Se excluyó porque el Área de Red Telemática es una unidad que se encarga de administrar el uso correcto de los servicios dentro de la organización no fuera de ella.
- *Persecución de delitos.*
- Tiempo de recuperación del servicio. Se excluyó este servicio ya que el proyecto de investigación se está evaluando lo que sucedería si algún activo se ve afectado, sino solo plantea si la metodología utilizada ayuda a mejorar la gestión de riesgos en la unidad de Red Telemática.
- Información clasificada (nacional). La información que se maneja en la unidad de red telemática es solo de carácter interno y si se necesita información debe solicitarla con un oficio autorizado. Por eso se excluyó
- Información clasificada (europea)

Los criterios que se utilizaron son los que veremos a continuación:

Tabla 21: Criterios de evaluación de Activos

CRITERIOS DE VALORACIÓN PLANTEADOS POR MAGERIT					
NIVELES	[pi] Información de carácter personal	[si] Seguridad	[da] Interrupción del servicio	[olm] Operaciones	[adm] Administración y gestión
1 0		probablemente sea causa de un incidente excepcionalmente serio de seguridad o dificulte la investigación de incidentes excepcionalmente serios		Probablemente cause un daño excepcionalmente serio a la eficacia o seguridad de la misión operativa o logística	
8 Y 9		probablemente sea causa de un serio incidente de seguridad o dificulte la investigación de incidentes serios	9.da Probablemente cause una interrupción excepcionalmente seria de las actividades propias de la Organización con un serio impacto en otras organizaciones 9.da2 Probablemente tenga un serio impacto en otras organizaciones	Probablemente cause un daño serio a la eficacia o seguridad de la misión operativa o logística	9.adm probablemente impediría seriamente la operación efectiva de la Organización, pudiendo llegar a su cierre.
7		probablemente sea causa de un grave incidente de seguridad o dificulte la investigación de incidentes graves	7.da Probablemente cause una interrupción seria de las actividades propias de la Or-ganización con un impacto significativo en otras organizaciones 7.da2 Probablemente tenga un gran impacto en otras organizaciones	Probablemente perjudique la eficacia o seguridad de la misión operativa o logística	7.adm probablemente impediría la operación efectiva de la Organización
6	6.pi1 probablemente afecte gravemente a un grupo de individuos 6.pi2 probablemente quebrante seriamente la ley o algún reglamento de protección de información personal.				

5	5.pi1 probablemente afecte gravemente a un individuo 5.pi2 probablemente quebrante seriamente leyes o regulaciones		5.da Probablemente cause la interrupción de actividades propias de la Organización con impacto en otras organizaciones 5.da2 Probablemente cause un cierto impacto en otras organizaciones	Probablemente merme la eficacia o seguridad de la misión operativa o logística más allá del ámbito local	5.adm probablemente impediría la operación efectiva de más de una parte de la organización
4	4.pi1 probablemente afecte a un grupo de individuos 4.pi2 probablemente quebrante leyes o regulaciones				
3	3.pi1 probablemente afecte a un individuo 3.pi2 probablemente suponga el incumplimiento de una ley o regulación	Probablemente sea causa de una merma en la seguridad o dificulte la investigación de un incidente	3.da Probablemente cause la interrupción de actividades propias de la Organización	Probablemente merme la eficacia o seguridad de la misión operativa o logística (alcance local)	3.adm probablemente impediría la operación efectiva de una parte de la Organización
2	2.pi1 pudiera causar molestias a un individuo 2.pi2 pudiera quebrantar de forma leve leyes o regulaciones				
1	1.pi1 pudiera causar molestias a un individuo	pudiera causar una merma en la seguridad o dificultar la investigación de un incidente		Pudiera mermar la eficacia o seguridad de la misión operativa o logística (alcance local)	1.adm pudiera impedir la operación efectiva de una parte de la Organización

Fuente: Elaborada por los autores en base a los criterios de Valoración que plantea Magerit.

Los criterios que se utilizaron para valorar los activos tienen una escala del 0 a 10. En la siguiente tabla mostramos los niveles.

Tabla 22: Criterios de evaluación

ESCALA DE VALOR		
VALOR		CRITERIO
10	extremo	daño extremadamente grave
9	muy alto	daño muy grave
8-6	alto	daño grave
5-3	medio	daño importante
2-1	bajo	daño menor

Fuente: MAGERIT - V 3.0. Libro 1: Método. Gobierno de España-Ministerio de Hacienda y Relaciones Públicas. 2012.

Desarrollo de la actividad

Para el desarrollo de la actividad se elaboró una tabla con los activos identificados y en colaboración del Jefe encargado de la Unidad de Red telemática se fue valorando el activo de acuerdo a las 5 dimensiones que MAGERIT plantea teniendo en cuenta los criterios mencionados anteriormente para poder dar el valor de dicho activo en cada dimensión como resultado obtuvimos el valor del activo, el cual se obtuvo promediando cada valor de la dimensión en la que este se vio afectado. Tabla que podemos visualizar en el capítulo IV Resultados y Discusión.

1.2. Caracterización de las amenazas.

El objetivo de las actividades englobadas en esta tarea fue identificar las posibles amenazas que se pueden materializar sobre los activos, así como estimar la frecuencia de ocurrencia y degradación que causan en los activos.

1.2.1. Identificación de las Amenazas.

Objetivo de la tarea

El objetivo de la actividad fue identificar las amenazas relevantes sobre cada activo de la Unidad de Red Telemática de la Universidad Nacional Pedro Ruiz Gallo.

Consideraciones previas

Para realizar esta tarea se tuvo en consideración lo siguiente:

- Se utilizaron las amenazas que nos brinda MAGERIT en el libro II catálogo de Amenazas.
  Las amenazas según nos plantea la metodología MAGERIT los clasifica en 4 grupos:
  [N] Desastres Naturales
  [I] De origen Industrial
  [E] Errores y fallos no intencionados
  [A] Ataque intencionados
  Estas a su vez pueden atacar en más de una dimensión, para esto MAGERIT la dimensión atacada de la más a menos relevante.

- Se utilizó la lista de activos identificados en la Unidad de Red telemática.

Desarrollo de la actividad

Para el desarrollo de la actividad se realizó una entrevista con el jefe encargado de la Unidad de Red Telemática de la Universidad Nacional Pedro Ruiz Gallo. Se utilizó la lista completa de amenazas por cada activo y se fue marcando con una X la amenaza que podría afectar a al activo.

Podemos observar las amenazas identificadas en el capítulo IV Resultados Discusión.

1.2.2. Valoración de las amenazas.

Objetivo de la actividad

El objetivo de la actividad fue determinar cuan afectado se vería el activo en caso la amenaza se materializara.

Consideraciones previas

- Se utilizó la tabla de degradación de activos que brinda MAGERIT, la cual vemos a continuación.

Tabla 23: Degradación de activos

PORCENTAJE DE DEGRADACIÓN DEL ACTIVO SEGÚN MAGERIT	
PORCENTAJE	NIVEL
100%	MA
90%	MA
80%	A
70%	A
60%	A
50%	M
40%	M
30%	M
20%	B
10%	B
5%	MB
1%	MB
0	NA

Fuente: Elaborada por los autores en base a MAGERIT - V 3.0. Libro 1: Método. Gobierno de España-Ministerio de Hacienda y Relaciones Públicas. 2012.

Desarrollo de la actividad

Para calcular la degradación se tomó en cuenta los valores que se proporcionan en la tabla valoración de activos. Se valoró la degradación de cada activo teniendo en cuenta que para algunas amenazas afectan a hasta en 3 dimensiones como vemos en la siguiente tabla.

Tabla 24: Escala Cualitativa de degradación de activos

ESCALAS CUALITATIVAS DE DEGRADACIÓN DE ACTIVOS DEFINIDA POR LA ENTIDAD	
ROJO	MAYOR DESGASTE
AMARILLO	MEDIO DESGASTE
VERDE	BAJO DESGASTE

Fuente: Elaborada por los autores en base a MAGERIT - V 3.0. Libro 1: Método. Gobierno de España-Ministerio de Hacienda y Relaciones Públicas. 2012.

Para determinar el nivel de la amenaza se utilizó la tabla de escala cuantitativa de degradación definida por la entidad en un rango de 0.01 a 1 como vemos a continuación:

Tabla 25: Escalas cuantitativas de degradación

ESCALAS CUANTITATIVAS DE DEGRADACIÓN DEFINIDA POR LA ENTIDAD	
NIVEL	RANGO
MUY ALTO	0.81 a 1.00
ALTO	0.51 a 0.80
MEDIO	0.21 a 0.5
BAJO	0.06 a 0.2
MUY BAJO	0.01 a 0.05

Fuente: Elaborada por los autores en base a MAGERIT - V 3.0. Libro 1: Método. Gobierno de España-Ministerio de Hacienda y Relaciones Públicas. 2012.

1.2.3. Determinación del Impacto.

Objetivo de la Tarea

El objetivo fue determinar el impacto que las amenazas identificadas causan en el activo en caso estas se llegaran a materializar.

Consideraciones Previas

- Se obtuvo el valor de cada activo de la Unidad de Red Telemática de la Universidad Nacional Pedro Ruiz Gallo.
- Se obtuvo el nivel de desgaste de cada activo de acuerdo a las posibles amenazas a las cuales este se vea expuesto.

Desarrollo de la actividad

Para obtener el impacto se multiplicó el valor del activo y el desgaste del mismo obtenidos en las actividades anteriores.

Para determinar el nivel de impacto se elaboró una tabla de escalas cualitativas de impacto definidas por la entidad. El resultado final lo podemos observar en el capítulo IV Resultados y Discusión.

Tabla 26: Escala cualitativa de impacto

ESCALAS CUALITATIVA DE IMPACTO DEFINIDA POR LA ENTIDAD		
NIVEL	ESCALA CUALITATIVA	**RANGO**
5	MUY ALTO	7.01 a 10
4	ALTO	3.01 a 7
3	MEDIO	2.01 a 3
2	BAJO	0.06 a 2
1	MUY BAJO	0.01 a 0.05

Fuente: Elaborada por los autores en base a MAGERIT - V 3.0. Libro 1: Método. Gobierno de España-Ministerio de Hacienda y Relaciones Públicas. 2012.

1.2.4. Determinación de la Probabilidad de impacto.

Objetivo de la tarea

El objetivo de la tarea fue determinar cuan probable o improbable es que se materialice la amenaza.

Consideraciones previas

- Se utilizó la tabla de probabilidad de ataque que platea la metodología MAGERIT para determinar la probabilidad en que una amenaza se materialice. La Probabilidad se trabajó para cada 2 años.

Tabla 27: Probabilidad de Ocurrencia de una amenaza

NIVEL	ESCALA CUALITATIVA	SIGNIFICADO
5	Muy Frecuente	Se espera que la amenaza ocurra más de tres veces al año.
4	Frecuente	Se espera que la amenaza ocurra al menos dos veces en el último año
3	Normal	Se espera que la amenaza se presente al menos una vez en los último año.
2	Poco Frecuente	Se espera que la amenaza se presente al menos una vez en los últimos 2 años.
1	Muy Poco Frecuente	No se ha presentado en los últimos 2 años.

Fuente: Elaborada por los autores en base a MAGERIT - V 3.0. Libro 1: Método. Gobierno de España-Ministerio de Hacienda y Relaciones Públicas. 2012.

Desarrollo de la actividad

Se determinó la probabilidad de impacto en colaboración del jefe encargado de la Unidad de Red Telemática de la Universidad Nacional Pedro Ruiz Gallo, utilizando la escala cualitativa mencionada anteriormente. El resultado final lo podemos visualizar en el capítulo IV Resultados y Discusión.

1.2.5. Mapa de Riesgo.

Objetivo de la actividad

El objetivo de la tarea fue obtener el mapa de riesgo o de calor para determinar el estado de riesgo.

Consideraciones Previas

Se utilizó la tabla de escala de riesgos planteada por MAGERIT

Tabla 28: Escala de Riesgo

ESCALA DEL RIESGO		
NIVEL	ESCALA CUALITATIVA	NMÓNICO
5	Critico	MA
4	Importante	A
3	Apreciable	M
2	Bajo	B
1	Despreciable	MB

Fuente: Elaborada por los autores en base a MAGERIT - V 3.0. Libro 1: Método. Gobierno de España-Ministerio de Hacienda y Relaciones Públicas. 2012.

Desarrollo de la actividad

Con ayuda del jefe de la Unidad de Red Telemática se determinó cuáles fueron los niveles de riesgo para la Unidad.

Tabla 29: Mapa de Calor

MAPA DE CALOR DEL RIESGO DEFINIDA POR LA INSTITUCIÓN						
		IMPACTO				
		5	4	3	2	1
PROBABILIDAD	5	MA	MA	A	M	B
	4	MA	MA	A	M	B
	3	A	A	M	B	MB
	2	M	M	B	MB	MB
	1	B	B	MB	MB	MB

Fuente: Elaborada por los autores en base a MAGERIT - V 3.0. Libro 1: Método. Gobierno de España-Ministerio de Hacienda y Relaciones Públicas. 2012.

1.2.6. Determinación del Riesgo.

Objetivo de la tarea

El objetivo de la tarea fue determinar el riesgo de cada activo con sus respectivas amenazas.

Consideraciones Previas

Se estableció los niveles de riesgo con la colaboración del jefe de la Unidad de Red Telemática de la Universidad Nacional Pedro Ruiz Gallo.

Tabla 30: Nivel de Tolerancia

NIVELES DE TOLERANCIA DE RIESGO		
NIVEL	ESCALA	RANGO
5	Critico	16 a 25
4	Importante	13 a 15
3	Apreciable	7 a 12
2	Bajo	5 a 6
1	Despreciable	1 a 4

Fuente: Elaborada por los autores en base a MAGERIT - V 3.0. Libro 1: Método. Gobierno de España-Ministerio de Hacienda y Relaciones Públicas. 2012.

Desarrollo de la actividad

Para determinar el nivel de riesgo se multiplicó el impacto por la probabilidad de ocurrencia, de acuerdo a ese resultado se calificó en la escala de tolerancia cual era nivel que pertenecía. Resultado que podemos visualizar en el capítulo IV Resultados y Discusión.

1.2.7. Evaluación del Riesgo.

Objetivo de la actividad

Determinar cuáles de los riesgos obtenidos son los más críticos.

Consideraciones Previas

Se utilizó el mapa de calor para saber cuál de los riesgos obtenidos eran los más críticos.

Desarrollo de la actividad

Se evaluó cada riesgo con la probabilidad de impacto en escalas cualitativas y se fue completando hasta determinar cuál de ellos eran los más críticos. Resultado final que podemos observar en la tabla, en el capítulo IV Resultados y Discusión.

4.1.2 Tratamiento del riesgo.

Para mitigar el actuar de las amenazas representadas por el riesgo, planteamos una seria de salvaguardas que podrán controlar el imparto que estas tengan en los activos.

1.3. Caracterización de las salvaguardas.

1.3.1. Identificación de las salvaguardas.

Objetivo de la tarea

Identificar las salvaguardas que nos permitan prevenir, acotan o consolidad el efecto de la amenaza en caso esta se llegara a materializar.

Consideraciones previas

- Para el desarrollo de la tarea se utilizó el catálogo de Salvaguardas que brinda MAGERIT.

Tabla 31: Salvaguardas

SALVAGUARDAS SEGÚN MAGERIT	
CÓDIGO	**NOMBRE**
PROTECCION A SERVICIOS	
S	Protección de los Servicios
S.A	Aseguramiento de la disponibilidad
S.start	Aceptación y puesta en operación
S.SC	Se aplican perfiles de seguridad
S.op	Explotación
S.CM	Gestión de cambios (mejoras y sustituciones)
S.end	Terminación
S.www	Protección de servicios y aplicaciones web
S.email	Protección del correo electrónico
S.dir	Protección del directorio
S.dns	Protección del servidor de nombres de dominio (DNS)
S.TW	Teletrabajo
PROTECCIÓN DE LAS APLICACIONES	
SW	Protección de las Aplicaciones Informáticas
SW.A	Copias de seguridad (backup)
SW.start	Puesta en producción
SW.SC	Se aplican perfiles de seguridad
SW.op	Explotación / Producción
PROTECCIÓN DE LOS EQUIPOS	
HW	Protección de los Equipos Informáticos
HW.start	Puesta en producción
HW.SC	Se aplican perfiles de seguridad
HW.A	Aseguramiento de la disponibilidad
HW.op	Operación
HW.CM	Cambios (actualizaciones y mantenimiento)
HW.end	Terminación
HW.PCD	Informática móvil
HW.print	Reproducción de documentos

HW.pabx	Protección de la centralita telefónica (PABX)
PROTECCION DE LAS COMUNICACIONES	
COM	Protección de las Comunicaciones
COM.start	Entrada en servicio
COM.SC	Se aplican perfiles de seguridad
COM.A	Aseguramiento de la disponibilidad
COM.aut	Autenticación del canal
COM.I	Protección de la integridad de los datos intercambiados
COM.C	Protección criptográfica de la confidencialidad de los datos intercambiados
COM.op	Operación
COM.CM	Cambios (actualizaciones y mantenimiento)
COM.end	Terminación
COM.internet	Internet: uso de acceso a
COM.wifi	Seguridad Wireless (WiFi)
COM.mobile	Telefonía móvil
COM.DS	Segregación de las redes en dominios
PROTECCIÓN DE LOS SOPORTES DE INFORMACIÓN	
MP	Protección de los Soportes de Información
MP.A	Aseguramiento de la disponibilidad
MP.IC	Protección criptográfica del contenido
MP.clean	Limpieza de contenidos
MP.end	Destrucción de soportes
PROTECCIÓN DE ELEMENTOS AUXILIARES	
AUX	Elementos Auxiliares
AUX.A	Aseguramiento de la disponibilidad
AUX.start	Instalación
AUX.power	Suministro eléctrico
AUX.AC	Climatización
AUX.wires	Protección del cableado
SEGURIDAD FISICA-PROTECCIÓN DE LAS INSTALACIONES	
L	Protección de las Instalaciones
L.design	Diseño
L.depth	Defensa en profundidad
L.AC	Control de los accesos físicos
L.A	Aseguramiento de la disponibilidad
L.end	Terminación
SALVAGUARDAS RELATIVAS AL PERSONAL	
PS	Gestión del Personal
PS.AT	Formación y concienciación
PS.A	Aseguramiento de la disponibilidad

- También se utilizó la tabla de tipos de salvaguardas, la cual vemos a continuación.

Tabla 32: Tipos de Salvaguardas

TABLA TIPOS DE SALVAGUARDAS SEGÚN MAGERIT		
EFECTO	TIPO	
	CÓDIGO	NOMBRE
Preventivas	[PR]	Preventivas
	[DR]	Disuasorias
	[EL]	Eliminatorias
acotan la degradación	[IM]	Minimizadoras
	[CR]	Correctivas
	[RC]	recuperativas
consolidan el efecto de las demás	[MN]	De monotorización
	[DC]	de detección
	[AW]	de concienciación
	[AD]	administrativas

Desarrollo de la actividad

Para el desarrollo de la actividad se utilizaron los activos que tenían el nivel de riesgo MUY CRITICO e IMPORTANTE. Para cada riesgo se eligió la correspondiente salvaguarda, considerando el tipo y el efecto que estas tenían en el riesgo. El resultado final lo podemos observar en el capítulo IV Resultados y Discusión.

4.2. Análisis y gestión de Riesgos en los activos de TI del Área de Red Telemática de la Universidad Nacional Pedro Ruiz Gallo aplicando la metodología OCTAVE-S.

Dada la delimitación del trabajo del trabajo de investigación solo abarcaron la Fase 1 y Fase 2 en su totalidad pero en la Fase 3 solo se desarrolló hasta la actividad selección de enfoques de mitigación. Aplicando el marco metodológico que esta metodología plantea para comprobar si OCTAVE es la metodología más adecuada para realizar un correcto análisis de riesgos.

4.2.1 Fase 1: Construcción del perfil de amenaza basado en los activos.

En esta fase, se realizó una evaluación de los aspectos organizacionales donde definimos el impacto de los criterios de la evaluación que se utilizó para realizar una evaluación de riesgos. También se identificaron cuáles son los activos críticos y se evaluó las prácticas de seguridad que se practican actualmente en la Unidad de Red Telemática de la Universidad Nacional Pedro Ruiz Gallo.

En esta fase se realizaron dos procesos:

- Identificar la información organizacional
- Crear perfiles de amenaza

1. Identificar la información organizacional.

1.1. Establecer criterios de evaluación de impactos.

Objetivo de la tarea

El objetivo de la tarea fue definir la escala cualitativa de medidas con las cuales se evaluó el efecto del riesgo en los activos de TI de la Unidad de Red Telemática de la Universidad Nacional Pedro Ruiz Gallo.

Consideraciones previas

Se utilizaron los criterios de las áreas estándar que Octave plantea para evaluar el impacto.

Los criterios a evaluar fueron:

- *Reputación/ Confianza de cliente:* En este criterio se evaluó el grado de satisfacción de los alumnos y/o docentes en los servicios que ofrece la unidad de red telemática.
- *Multas/ Sanciones Legales:* Se midió el grado de cumplimiento de los procedimientos administrativos, las normas o políticas internas de la Unidad de Red Telemática de la Universidad Nacional Pedro Ruiz Gallo.
- *Operatividad:* Se midió el grado de cumplimiento de los controles internos: eficacia operativa, fiabilidad de la información y cumplimiento normativo.
- *Seguridad:* Se midió si los recursos humanos contaban con las debidas medidas de seguridad y salud en el Trabajo.
- *Finanzas:* Se midió el grado de cumplimiento del presupuesto asignado para dicha Unidad.

Desarrollo de la tarea

Mediante el uso de las Hojas de Trabajo: Impacto de los criterios de evaluación, se definió los rangos de posibles impactos que se pueden presentar en los activos de TI de la Unidad de Red Telemática de la Universidad Nacional Pedro Ruiz Gallo.

Se utilizó la información obtenida por la experiencia adquirida durante las prácticas profesionales de los tesistas para el establecimiento de medidas (muy bajo, bajo, medio, alto y muy alto), también fue establecida esa escala en niveles de 5 para uniformizar con la escala definida en la otra metodología con la cual se está comparando.

1.2. Identificar los activos organizacionales.

Objetivo de la tarea

El objetivo de la tarea fue identificar los activos relacionados con la información del sistema académico de la Unidad de Red Telemática de la Universidad Nacional Pedro Ruiz Gallo.

Consideraciones previas

Se limitó a identificar los activos de TI que forman parte del sistema académico, fundamentales en la Unidad de Red Telemática.

Desarrollo de la actividad

Para el desarrollo de la actividad se recolectó la información que forma parte de los activos de TI del sistema académico de la Unidad. Los datos recolectados como proceso de matrículas, historial académico, horarios, plan de estudios, notas, actas, cronogramas fueron información fundamental para el realizar la identificación de todos los activos organizacionales.

1.3. Evaluar las prácticas de seguridad organizacionales.

Objetivo de la Tarea

El objetivo de la tarea fue identificar en qué medida cada práctica de la encuesta planteada por OCTAVE-S es utilizada por la Unidad de Red Telemática.

Consideraciones Previas

Se utilizó la encuesta planteada por OCTAVE-S, donde se plantearon las prácticas de seguridad que la Unidad de Red Telemática debe utilizar.

Desarrollo de la actividad.

Con la experiencia de los tesistas, se fue respondiendo a cada pregunta de la encuesta, la cual valoraba el cumplimiento de la práctica en 4 niveles; si, algo, no y no se sabe.

También para la evaluación de cada área se tuvo en cuenta las prácticas que actualmente se estaban realizando en la Unidad de Red Telemática; así como las que la Unidad no ponía en práctica según la encuesta planteada por OCTAVE-S.

2. Crear perfiles de amenaza.

El objetivo de la tarea fue seleccionar los activos críticos de los ya identificados para la Unidad de Red Telemática, es decir se identificó los activos de los cuales el sistema académico de la Universidad Nacional Pedro Ruiz Gallo se vería afectado si alguno de ellos se vería amenazado.

2.1. Seleccionar activos críticos.

Objetivo de la tarea

El objetivo de la tarea fue identificar los 5 activos críticos de los activos identificados en la tarea anterior; para la Unidad de Red Telemática.

Consideraciones Previas

Utilizar la lista de activos que fueron identificados en el proceso anterior.

Desarrollo de la actividad

La primera de ellas fue identificar los activos críticos para la Unidad de Red Telemática, argumentando la razón del porque fueron elegidos, describiéndolos teniendo en cuenta quién los usaba y el encargado de los mismo y por ultimo identificar los activos relacionados con cada activo crítico.

2.2. Identificar los requisitos de seguridad para los activos críticos.

Objetivo de la tarea

El objetivo de la tarea fue identificar los requisitos de seguridad para cada activo.

Consideraciones Previas

Recolectar información sobre si se aplicaba algún requisito de seguridad a los activos críticos.

Desarrollo de la actividad

La segunda actividad fue identificar los requisitos de seguridad que se aplicaban a los activos críticos mencionados en la actividad anterior.

2.3. Identificar amenazas a los activos críticos.

Objetivo de la tarea

El objetivo de la tarea fue identificar las amenazas, utilizando los árboles de amenazas planteada por OCTAVE-s.

Consideraciones Previas

Árboles de amenazas planteados por OCTAVE-S.

Desarrollo de la actividad

La tercera actividad consistió en identificar las amenazas que afecten o podrían afectar a los activos críticos. Para eso se utilizó el árbol de amenazas, en el cual se identificó el acceso, el autor, el motivo y el resultado de dicha amenaza. Paso siguiente se registró con qué frecuencia ocurrió dicha amenaza.

Con ayuda del jefe de la Unidad de Red Telemática y la experiencia de los tesistas se utilizó la hoja de trabajo de perfil para Sistema académico actas virtuales UNPRG: Actores humanos que utilizan el acceso a la red, para identificar las amenazas que representan el personal que por red pueda acceder al activo crítico, ya sea que forme o no parte de la Unidad de Red Telemática.

Se utilizaron hojas de trabajo como actores humanos que utilizan el acceso físico para identificar las amenazas que representan las personas que tengan acceso al activo crítico mediante acceso físico. Problemas del sistema, para identificar las amenazas en caso el sistema fallara por motivos con defectos del sistema, caída del sistema, defectos de hardware o código malicioso. Otros problemas para identificar las amenazas en caso el activo critico se vea amenazado por problemas con el suministro de energía, problemas de telecomunicaciones, problemas con terceros o desastres naturales.

Luego de que las amenazas fueron identificadas, se determinó que tan fuerte fue el motivo del actor para amenazar al activo crítico y que tan confiables eran nuestros datos. También se determinó con qué frecuencia habían ocurrido dichas amenazas y que tan confiables eran nuestros datos. Para finalmente dar ejemplos de cómo ocurrieron las amenazas.

4.2.2 Fase 2: Identificar vulnerabilidades de infraestructura.

En esta fase se realizó el análisis de la infraestructura informática de la Unidad de Red Telemática. Se analizó como las personas usan la infraestructura informática para acceder a los activos críticos, verificando así los componentes y quien es el encargado del mismo.

Así mismo se examinó hasta qué punto el personal responsable incluida seguridad en los proceso de la Unidad de Red Telemática.

1. Examinar la infraestructura informática en relación con los activos críticos.

Para el desarrollo de la actividad se identificó las rutas mediante las cuales se podían acceder a cada activo crítico, con esto se determinó las clases de componentes que son parte del sistema académico de la Universidad Nacional Pedro Ruiz Gallo.

1.1. Examinar las rutas de acceso.

Objetivo de la tarea

El objetivo de la tarea fue identificar las rutas de acceso en la infraestructura para los activos críticos, así también se analizó los proceso relacionados con la tecnología asociados a dicha infraestructura.

Consideraciones Previas

Se identificaron los 5 activos críticos, pero se eligió al activo Sistema académico actas virtuales UNPRG, ya que es el activo del cual depende la parte académica en la cual se está aplicando la presente tesis.

Desarrollo de la actividad

Para el desarrollo de la actividad se identificó las rutas mediante las cuales se podían acceder a cada activo crítico, con esto se determinó las clases de componentes que son parte del sistema académico de la Universidad Nacional Pedro Ruiz Gallo.

De las rutas de acceso se determinó cuáles de los componentes sirven como puntos de acceso intermedios y cuáles de ellos fueron utilizados

por personas para acceder a los sistemas. Después de haber determinado las rutas, componentes y personas que los utilizan se determinó donde se almacenaba la información así como también si otros sistemas podían acceder a la información.

1.2. Analizar procesos relacionados con la tecnología.

Objetivo de la tarea

El objetivo de la actividad fu determinar cuál de los componentes estaban relacionados con uno o más activos críticos y dieran acceso a los mismos.

Consideraciones Previas

Elaborar una lista con las relaciones de los activos y como estos se conectaban.

Desarrollo de la actividad

Para el desarrollo de la actividad se realizaron los siguientes pasos:

- Se determinó las clases de componentes que están relacionados con dos o más activos críticos.
- Se determinó el o los responsables de los componentes.
- Se determinó en qué medida esa clase de componente esa resistente a los ataques de red.

4.2.3 Fase 3: Desarrollar estrategias y planes de seguridad.

Las tareas englobadas en esta fase tuvieron como objetivo identificar y analizar los riesgos a través de la evaluación de impactos de las amenazas, de haber establecido criterios para la avaluación de probabilidad, así como también evaluar dichos criterios en las amenazas.

Todo eso para poder establecer enfoques que permitan mitigar dichas amenazas.

1. Identificar y analizar los riesgos.

1.1. Evaluar los impactos de las amenazas.

Objetivo de la actividad

El objetivo de la actividad fue determinar el nivel de impacto que la amenaza activa produce en el activo crítico, utilizando los criterios de evaluación de impactos.

Consideraciones Previas

- Se estableció los niveles de impacto (muy bajo, bajo, medio, alto y muy alto) de los criterios de evaluación de impacto.
- Se identificaron y evaluaron las amenazas.

Desarrollo de la actividad

Para el desarrollo de la actividad se utilizaron las hojas de trabajo de perfil de riesgo para Sistema académico actas virtuales UNPRG- actores humanos que utilizan el acceso a la red, actores humanos que utilizan el acceso físico, problemas del sistema y otros problemas. Se evaluó el grado de impacto que las amenazas tenían en el activo crítico. Se utilizó una escala de 5 niveles: Muy bajo, bajo, medio, alto y muy alto, evaluando la amenaza en los 5 criterios de evaluación de impacto en colaboración con el jefe de la Unidad de Red Telemática.

1.2. Establecer criterios de evaluación de probabilidad.

Objetivo de la actividad

El objetivo de la actividad fue definir una escala cualitativa de medidas, con las cuales se evaluó la probabilidad de que ocurra una amenaza en el activo crítico.

Consideraciones Previas

Definir el tiempo en el que se iban a analizar las amenazas en este caso se tomó como referencia 2 años.

Desarrollo de la actividad

En colaboración con el encargado de la Unidad de Red Telemática se establecieron los criterios de evaluación de probabilidad. Se realizó en 5 niveles (Muy bajo, bajo, medio, alto y muy alto), tomando como referencia 2 años (tiempo entre eventos a analizar).

Tabla 33: Criterios de evaluación de probabilidad.

TIEMPO ENTRE EVENTOS ANALIZADA	MUY BAJO	BAJO	MEDIO	ALTO	MUY ALTO
	0 veces en 2 años	Al menos una vez en 2 años	Más de 2 veces al año	Al menos más de 2 veces al año	Más de 2 veces al año

Fuente: Elaborada por los autores

1.3. Evalúa Probabilidades de Amenazas.

Objetivo de la actividad

El objetivo de la actividad fue evaluar la probabilidad de impacto de la amenaza activa en el activo crítico: Sistema académico actas virtuales UNPRG.

Consideraciones Previas

Se establecieron los criterios de impacto de las amenazas en 5 niveles.

Desarrollo de la actividad

Para el desarrollo de la actividad en colaboración con el jefe de la Unidad de Red Telemática y la experiencia de los tesistas, se elaboró la hoja de trabajo de perfil de riesgo para Sistema académico actas virtuales UNPRG: Actores humanos que utilizan el acceso a la red, actores humanos que utilizan el acceso físico, problemas del sistema y otros problemas. En las cuales se evaluó el impacto que tendría las amenazas activas en el activo crítico y determinó que tan confiable era ese valor.

2. Desarrollar estrategias de protección y planes de mitigación.

2.1. Describir la estrategia de protección actual.

Objetivo de la tarea

El objetivo de la actividad fue describir el estado actual de las estrategias de protección en la Unidad de Red Telemática de la Universidad Nacional Pedro Ruiz Gallo, basado en 5 criterios de evaluación.

Consideraciones Previas

No hubo consideraciones previas para esta actividad.

Desarrollo de la actividad

Para el desarrollo de la actividad se utilizó el las estrategias de protección que proporciona OCTAVE. Mediante 5 criterios los cuales fueron: Conocimiento de seguridad y entrenamiento, estrategia de protección para el manejo colaborativo de la seguridad, estrategia de protección para monitorear y auditar seguridad física, estrategia de protección para autenticación y autorización, estrategia de protección para políticas de seguridad y regulaciones. En cada uno de los criterios se fue evaluando la situación actual de las estrategias de protección en colaboración con el jefe encargado de la Unidad de Red Telemática de la Universidad Nacional Pedro Ruiz Gallo.

2.2. Seleccionar enfoques de mitigación.

Objetivo de la actividad

El objetivo de la actividad fue decidir si aceptamos, aplazamos o mitigamos las amenazas.

Consideraciones Previas

Trasladar el estado semáforo de las prácticas de seguridad organizacional evaluadas en la primera fase.

Desarrollo de la actividad

Para el desarrollo de la actividad, se elaboró 4 hojas de trabajo en las que se trasladó el estado semáforo de las prácticas de seguridad que fueron evaluadas en dos áreas ya definidas por la metodología OCTAVE-S, el área Estratégica y Operacional. Donde se decidió mediante 3 enfoques si la amenaza se aceptaba, aplazaba o mitigaba.

CAPÍTULO V RESULTADOS Y DISCUSIÓN

5.1. Metodología MAGERIT

5.1.1. Identificación de los Activos

Tabla 34: Activos de la Unidad de Red Telemática de la Universidad Nacional Pedro Ruiz Gallo

ACTIVOS DE LA UNIDAD DE RED TELEMÁTICA DE LA UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO			
ACTIVO		DESCRIPCIÓN	ENCARGADO
CÓDIGO	NOMBRE		
[S] SERVICIOS			
[sges]	Gestión de Actas virtuales y matricula online	Este servicio tiene cuatro plataformas, uno para alumnos (matricula, historial, horario, plan de estudios, notas), registros académicos (registrar actas de docentes e ingresarlos al sistema), para el docente (carga horaria, horarios e ingreso de notas) y el administrador de aplicaciones y base de datos (generar actas, cambio de notas, bloqueos de actas, conteo de actas , proceso de matrícula, activar actas, cronograma de matrículas, programación de semestres, programación de cursos, grupos).	[adm1] Administrador del data center
[sgeo]	Gestión de Actas virtuales OCCA	Sistema para ver notas antiguas, podemos ver las guías de matrícula, mensajes adicionales de la parte académica, Se ingresa como el administrador o por el estudiante. El estudiante puede ver datos como estudiante, constancia de matrícula de cualquier semestre académico y su historial académico con respecto a su carrera profesional.	[adm1] Administrador del data center
[SW] APLICACIONES			
[swsc]	Sistema académico actas virtuales UNPRG	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.	[adm1] Administrador del data center
[swoc]	Sistema académico 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.	[adm1] Administrador del data center
[HW] EQUIPOS INFORMÁTICOS			
[serv]	Servidores		
[ser1]	Servidor de dominio	Servidor en donde se encuentrarn las aplicaciones de sistemas operativos Windows Server, servicios de active directory, a la cual se conectan todas las computadoras de la Universidad Nacional Pedro Ruiz Gallo.	[adm1] Administrador del data center
[ser2]	Servidor de proxy	Es el servidor encargado de la validad de los acceso y permisos a la red de computadoras.	[adm1] Administrador del data center
[ser3]	Servidor de base de datos	Es el servidor que almacena la base de datos del sistema académico para pregrado.	[adm1] Administrador del data center
[ser4]	Servidor de base de datos - backup	Es el servidor donde se almacenan los Backup de las bases de datos del sistema de pre grado de la Universidad Nacional Pedro Ruiz Gallo	[adm1] Administrador del data center

[ser5]	Servidor web	Es el servidor encargado de almacenar las aplicaciones entre ellas al sistema de gestión académica para pregrado.	[adm1] Administrador del data center
[ser6]	Servidor de archivos	Es el servidor que almacena la base de datos del sistema de gestión académica para pregrado.	[adm1] Administrador del data center
[ser7]	Servidor de datos - OCCA	Es el servidor que almacena la base de datos del sistema de gestión académica.	[adm1] Administrador del data center
[ser8]	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.	[adm1] Administrador del data center
[netw]	Soporte de red		
[swit]	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.	[adm1] Administrador del data center
[rout]	Router	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.	[adm1] Administrador del data center
[fire]	Firewall	Router principal de la red - UNPRG, realiza el enrutamiento de la red y permite acceso al servicio de internet.	[adm1] Administrador del data center
[COM] REDES DE COMUNICACIONES			
[cint]	Internet	Servicio brindado por terceros, a través de líneas dedicadas que son distribuidas para los diferentes servicios que se tiene en la universidad.	
[cwfi]	Red Inalámbrica	Servicio de wifi que sirve para conectar a los dispositivos como laptop para los diferentes servicios que brinda la Unidad de Red Telemática.	
[MEDIA] SOPORTE DE INFORMACIÓN			
[elect]	Electrónicos		
[ele1]	Cintas Magnéticas	Se utilizan para el soporte de almacenamiento de datos.	[adm1] Administrador del data center
[ele2]	Disco externo USB	Se utilizan para el soporte de almacenamiento de datos.	[adm1] Administrador del data center
[store]	Storage de respaldo de BD	Se almacenan las bases de datos de las diferentes aplicaciones y servicios que ofrece la Unidad de Red Telemática.	[adm1] Administrador del data center
[noel]	No electrónico		
[mimp]	Material impreso	Material impreso como inventario de la Unidad de Red Telemática, resoluciones, ingresos y salidas de dispositivos, notas de servicio.	[adm1] Administrador del data center
[AUX] EQUIPAMIENTO AUXILIAR			
[powr]	Acumulador de energía UPS	Sistema de alimentación ininterrumpida (UPS), encargados de brindar energía por un tiempo determinado a los servidores en caso que la energía eléctrica se pierda.	[adm1] Administrador del data center
[psis]	Sistema de aire acondicionado	Es un equipo de aire acondicionado encargado de mantener a una temperatura adecuada el data center.	[adm1] Administrador del data center
[gelc]	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.	[adm1] Administrador del data center
[cable]	Cableado		
[cab1]	Cableado de red	Cable por el cual se conectan los dispositivos de la Unidad de Red Telemática.	[adm1] Administrador del data center [uex1]Personal de TI
[cab2]	Fibra óptica	Filamento por donde se transmite los servicios que ofrece la Unidad de Red Telemática a los diferentes departamentos académicos de la Universidad Nacional Pedro Ruiz Gallo.	[adm1] Administrador del data center
[L] INSTALACIONES			
[site]	Data Center	Es el local de la UNPRG, Unida de Red Telemática, donde se encuentran los equipos que brindan los servicios y el personal encargado de tener en funcionamiento óptimo para los equipos.	[adm1] Administrador del data center

[P] PERSONAL			
[ueex]	Usuario externo	Estudiantes, docentes y Trabajadores Administrativos. Los estudiantes que ingresan al portal web para matricularse, ver sus notas, etc.; el personal administrativo principalmente de las oficinas de OAP y dirección de escuelas.	
[uex1]	Personal de TI	Practicantes que ayudan con el correcto funcionamiento de la Unidad de Red Telemática. También se encargan de brindar soporte técnico a las diferentes áreas de la universidad Nacional Pedro Ruiz Gallo.	
[adm1]	Administrador del data center	El encargado de dirigir y autorizar todas las actividades y procesos de la Unidad de Red Telemática el Ingeniero Vladimir Gonzales Menchán.	

Fuente: Elaborada por los autores en base a MAGERIT- V 3.0 - Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro II

Se utilizó la tabla Activos de la Unidad de Red telemática de la Universidad Nacional Pedro Ruiz Gallo, para identificar los activos. Como se mencionó anteriormente estos los divide en 8 capas. En la primera capa se identificaron los servicios de Gestión de Actas virtuales y matricula online y Gestión de Actas virtuales OCCA, en la capa de aplicaciones se identificaron las aplicaciones Sistema académico actas virtuales UNPRG y Sistema académico OCCA. La tercera capa está compuesta por los servidores como Servidor de dominio, proxy, base de datos, base de datos - backup, web, de archivos, de datos - OCCA, base de datos - backup-OCCA y soportes de red como Switch, Router y Firewall. Redes de comunicaciones cuarta capa está compuesta por Internet y Red Inalámbrica; Cintas Magnética, Disco externo USB, Storage de respaldo de BD, No electrónico, Material impreso conforman la capa número cinco. La capa de Equipamiento auxiliar la conforman Acumulador de energía UPS, Sistema de aire acondicionado, Grupo electrógeno y el cableado. El data center en la capa de instalaciones y por último el personal conformado por usuario externo, personal de TI y administrador del data center.

5.1.2. Dependencia entre activos

Tabla 35: Tabla dependencia entre activos.

ACTIVOS Y SUS DEPENDENCIAS DE LA UNIDAD DE RED TELEMÁTICA DE LA UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO		
ACTIVO		DEPENDENCIA
CÓDIGO	NOMBRE	
[S] SERVICIOS		
[sges]	Gestión de Actas virtuales y matricula online	[ser1] Servidor de dominio [ser2] Servidor de proxy [ser3] Servidor de base de datos [ser4] Servidor de base de datos - backup [ser5] Servidor web [ser6] Servidor de archivos [ser7] Servidor de datos - OCCA [ser8] Servidor de base de datos - backup-OCCA [swit]Switch [rout] Router [fire] Firewall [cint] Internet [cwfi] Red Inalámbrica [store] Storage de respaldo de BD [powr] Acumulador de energía UPS [psis] Sistema de aire acondicionado [gelc] Grupo electróngeno [cab1] Cableado de red [cab2] Fibra óptica [site] Data Center [ueex] Usuario externo [uex1] Personal de TI
[sgeo]	Gestión de Actas virtuales OCCA	[ser1] Servidor de dominio [ser2] Servidor de proxy [ser3] Servidor de base de datos [ser4] Servidor de base de datos - backup [ser5] Servidor web [ser6] Servidor de archivos [ser7] Servidor de datos - OCCA [ser8] Servidor de base de datos - backup-OCCA [swit]Switch [rout] Router [fire] Firewall [cint] Internet [cwfi] Red Inalámbrica [store] Storage de respaldo de BD [powr] Acumulador de energía UPS [psis] Sistema de aire acondicionado [gelc] Grupo electróngeno [cab1] Cableado de red [cab2] Fibra óptica [site] Data Center [ueex] Usuario externo [uex1] Personal de TI
[SW] APLICACIONES		
[swsc]	Sistema académico actas virtuales UNPRG	[sges] Gestión de Actas virtuales y matricula online [ser3] Servidor de base de datos [ser4] Servidor de base de datos - backup [swit]Switch [rout] Router [fire] Firewall [cint] Internet [site] Data Center [uex1] Personal de TI [adm1] Administrador del data center
[swoc]	Gestión de Actas virtuales OCCA	[sgeo] Gestión de Actas virtuales OCCA [ser3] Servidor de base de datos [swit]Switch [rout] Router [cint] Internet [powr] Acumulador de energía UPS [psis] Sistema de aire acondicionado [gelc] Grupo electróngeno [site] Data Center
[HW] EQUIPOS INFORMÁTICOS		
[serv]	Servidores	
[ser1]	Servidor de dominio	[cint] Internet [powr] Acumulador de energía UPS [psis] Sistema de aire acondicionado [gelc] Grupo electróngeno [cab1] Cableado de red

		[cab2] Fibra óptica [site] Data Center [uex1] Personal de TI [adm1] Administrador del data center
[ser2]	Servidor de proxy	[cint] Internet [powr] Acumulador de energía UPS [psis] Sistema de aire acondicionado [gelc] Grupo electróngeno [cab1] Cableado de red [cab2] Fibra óptica [site] Data Center [uex1] Personal de TI [adm1] Administrador del data center
[ser3]	Servidor de base de datos	[cint] Internet [powr] Acumulador de energía UPS [psis] Sistema de aire acondicionado [gelc] Grupo electróngeno [cab1] Cableado de red [cab2] Fibra óptica [site] Data Center [uex1] Personal de TI [adm1] Administrador del data center
[ser4]	Servidor de base de datos - backup	[cint] Internet [powr] Acumulador de energía UPS [psis] Sistema de aire acondicionado [gelc] Grupo electróngeno [cab1] Cableado de red [cab2] Fibra óptica [site] Data Center [uex1] Personal de TI [adm1] Administrador del data center
[ser5]	Servidor web	[cint] Internet [powr] Acumulador de energía UPS [psis] Sistema de aire acondicionado [gelc] Grupo electróngeno [cab1] Cableado de red [cab2] Fibra óptica [site] Data Center [uex1] Personal de TI [adm1] Administrador del data center
[ser6]	Servidor de archivos	[cint] Internet [powr] Acumulador de energía UPS [psis] Sistema de aire acondicionado [gelc] Grupo electróngeno [cab1] Cableado de red [cab2] Fibra óptica [site] Data Center [uex1] Personal de TI [adm1] Administrador del data center
[ser7]	Servidor de datos - OCCA	[cint] Internet [powr] Acumulador de energía UPS [psis] Sistema de aire acondicionado [gelc] Grupo electróngeno [cab1] Cableado de red [cab2] Fibra óptica [site] Data Center [uex1] Personal de TI [adm1] Administrador del data center
[ser8]	Servidor de base de datos - backup-OCCA	[cint] Internet [powr] Acumulador de energía UPS [psis] Sistema de aire acondicionado [gelc] Grupo electróngeno [cab1] Cableado de red [cab2] Fibra óptica [site] Data Center [uex1] Personal de TI [adm1] Administrador del data center
[netw]	Soporte de red	
[swit]	Switch	[site] Data Center [uex1] Personal de TI [adm1] Administrador del data center
[rout]	Router	[site] Data Center [uex1] Personal de TI [adm1] Administrador del data center
[fire]	Firewall	[site] Data Center [uex1] Personal de TI [adm1] Administrador del data center
[COM] REDES DE COMUNICACIONES		
[cint]	Internet	[swit]Switch [rout] Router [fire] Firewall [powr] Acumulador de energía UPS

		[psis] Sistema de aire acondicionado [gelc] Grupo electróngeno [cab1] Cableado de red [cab2] Fibra óptica [site] Data Center [uex1] Personal de TI [adm1] Administrador del data center
[cwfi]	Red Inalámbrica	[swit]Switch [rout] Router [fire] Firewall [powr] Acumulador de energía UPS [psis] Sistema de aire acondicionado [gelc] Grupo electróngeno [cab1] Cableado de red [cab2] Fibra óptica [site] Data Center [uex1] Personal de TI [adm1] Administrador del data center
[MEDIA] SOPORTE DE INFORMACIÓN		
[elect]	Electrónicos	
[ele1]	Cintas Magnéticas	[site] Data Center [uex1] Personal de TI [adm1] Administrador del data center
[ele2]	Disco externo USB	[site] Data Center [uex1] Personal de TI [adm1] Administrador del data center
[store]	Storage de respaldo de BD	[site] Data Center [uex1] Personal de TI [adm1] Administrador del data center
[noel]	No electrónico	
[mimp]	Material impreso	[site] Data Center [uex1] Personal de TI [adm1] Administrador del data center
[AUX] EQUIPAMIENTO AUXILIAR		
[powr]	Acumulador de energía UPS	[site] Data Center [uex1] Personal de TI
[psis]	Sistema de aire acondicionado	[site] Data Center [uex1] Personal de TI
[gelc]	Grupo electrógeno	[site] Data Center [uex1] Personal de TI
[cable]	Cableado	
[cab1]	Cableado de red	[uex1] Personal de TI
[cab2]	Fibra óptica	[site] Data Center [uex1] Personal de TI [adm1] Administrador del data center
[L] INSTALACIONES		
[site]	Data Center	[uex1] Personal de TI [adm1] Administrador del data center
[P] PERSONAL		
[ueex]	Usuario externo	
[uex1]	Personal de TI	
[adm1]	Administrador del data center	

5.1.3. Valorización de Activos

Para la valoración de los activos se utilizó la tabla Valoración de Activos de la Unidad de Red Telemática – UNPRG. En ella valoramos a los activos identificados en las 5 dimensiones de los cuales el Sistema académico actas virtuales UNPRG, Servidor de base de datos - backup, Cintas Magnéticas, Material impreso, Cableado de red, Fibra óptica, Data Center y Administrador del data center, fueron los activos más valiosos para la Unidad de Red Telemática.

Tabla 36: Valoración de Activos de la Unidad de Red Telemática - UNPRG

VALORACIÓN DE ACTIVOS DE LA UNIDAD DE RED TELEMÁTICA DE LA UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO							
ACTIVO	DIMENSIÓN	TOTAL					
CÓDIGO	NOMBRE	DISPONIBILIDAD	INTEGRIDAD	CONFIDENCIALIDAD	AUTENTICIDAD	TRAZABILIDAD	TOTAL
[S] SERVICIOS							
[sges]	Gestión de Actas virtuales y matricula online	3					3
[sgeo]	Gestión de Actas virtuales OCCA	3	3	1	3	2	2.4
[SW] APLICACIONES							
[swsc]	Sistema académico actas virtuales UNPRG	4	7		7	2	5
[swoc]	Sistema académico OCCA	3	5		4	1	3.3
[HW] EQUIPOS INFORMÁTICOS							
[serv]	Servidores						
[ser1]	Servidor de dominio	3	4		4	4	3.8
[ser2]	Servidor de proxy	2					2
[ser3]	Servidor de base de datos	6	7	1	6	5	5
[ser4]	Servidor de base de datos - backup	2	7		6	3	4.5
[ser5]	Servidor web	3	3	1	3	1	2.2
[ser6]	Servidor de archivos	2	2		2		2
[ser7]	Servidor de datos - OCCA	3	3	1	3	1	2.2
[ser8]	Servidor de base de datos - backup-OCCA	3	4		3	1	2.8
[netw]	Soporte de red						
[swit]	Switch	3				1	2
[rout]	Router	3				1	2
[fire]	Firewall		5		4	2	3.7
[COM] REDES DE COMUNICACIONES							
[cint]	Internet	4				2	3
[cwfi]	Red Inalámbrica	4				2	3
[MEDIA] SOPORTE DE INFORMACIÓN							
[elect]	Electrónicos						
[ele1]	Cintas Magnéticas	3	6		5	4	4.5
[ele2]	Disco externo USB	3	5		4	3	3.8
[store]	Storage de respaldo de BD	3	6		5	4	4.5
[noel]	No electrónico						
[mimp]	Material impreso	4	6	6			5.3
[AUX] EQUIPAMIENTO AUXILIAR							
[powr]	Acumulador de energía UPS	4				6	5
[psis]	Sistema de aire acondicionado	4				6	5
[gelc]	Grupo electrógeno	4				6	5
[cable]	Cableado						
[cab1]	Cableado de red	4				7	5.5
[cab2]	Fibra óptica	4				7	5.5
[L] INSTALACIONES							
[site]	Data Center	4			7		5.5
[P] PERSONAL							
[ueex]	Usuario externo	3				2	2.5
[uex1]	Personal de TI	3				2	2.5
[adm1]	Administrador del data center	8				3	5.5

Fuente: Elaborada por los autores en base a MAGERIT- V 3.0 - Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro II

5.1.4. Valorización de Amenazas

Se utilizó la tabla Valoración de las amenazas en los activos de TI de la Unidad de Red Telemática – UNPRG, Se valoró la amenaza identificada en las 5 dimensiones. Y de acuerdo a la valoración dada por el feje de la Unidad de la Red Telemática algunas de las amenazas identificadas en los activos arrojaron que algunos tenían un nivel de criticidad de muy alto y alto. Como por ejemplo el Sistema académico actas virtuales UNPRG tuvo un nivel de criticidad de muy alto y alto en las amenazas como fuego, fallo de servicios de comunicaciones e Interrupción de otros servicios y suministros esenciales, caída del sistema por agotamiento de recursos y Denegación del servicio.

5.1.5. Identificación de Amenazas

Tabla 37: Identificación de Amenazas de activos de TI de la Unidad de Red Telemática - UNPRG

IDENTIFICACIÓN DE AMENAZAS EN LOS ACTIVOS DE LA UNIDAD DE RED TELEMÁTICA				
ACTIVO		AMENAZA		
CÓDIGO	NOMBRE	CÓDIGO	NOMBRE	DIMENSIÓN AFECTADA
[S] SERVICIOS				
[sges]	Gestión de Actas virtuales y matricula online	[I.6]	Corte de suministro	Disponibilidad
		[I.8]	Fallo de servicios de comunicaciones	Disponibilidad
		[I.9]	Interrupción de otros servicios y suministros esenciales	Disponibilidad
		[E.1]	Errores de los usuarios	Integridad
				Confidencialidad
				Disponibilidad
		[E.20]	Vulnerabilidades de los programas (software)	Integridad
				Disponibilidad
				Confidencialidad
		[E.24]	Caída del sistema por agotamiento de recursos	Disponibilidad
		[A.24]	Denegación del servicio	Disponibilidad
[sgeo]	Gestión de Actas virtuales OCCA	[I.8]	Fallo de servicios de comunicaciones	Disponibilidad
		[I.9]	Interrupción de otros servicios y suministros esenciales	Disponibilidad
		[E.1]	Errores de los usuarios	Integridad
				Confidencialidad
				Disponibilidad
		[E.20]	Vulnerabilidades de los programas (software)	Integridad
				Disponibilidad
				Confidencialidad
		[A.5]	Suplantación de la identidad del usuario	Confidencialidad
				Autenticidad
				Integridad
		[A.24]	Denegación del servicio	Disponibilidad
[SW] APLICACIONES				
[swsc]	Sistema académico actas virtuales UNPRG	[N.1]	Fuego	Disponibilidad
		[I.8]	Fallo de servicios de comunicaciones	Disponibilidad

		[I.9]	Interrupción de otros servicios y suministros esenciales	Disponibilidad
		[E.2]	Errores del administrador	Disponibilidad
				Integridad
				Confidencialidad
		[E.21]	Errores de mantenimiento / actualización de programas (software)	Integridad
				Disponibilidad
		[E.23]	Errores de mantenimiento / actualización de equipos (hardware)	Disponibilidad
		[E.24]	Caída del sistema por agotamiento de recursos	Disponibilidad
		[A.24]	Denegación del servicio	Disponibilidad
[swoc]	Sistema académico OCCA	[I.1]	Fuego	Disponibilidad
		[I.5]	Avería de origen físico o lógico	Disponibilidad
		[I.6]	Corte de suministro	Disponibilidad
		[I.7]	Condiciones inadecuadas de temperatura o humedad	Disponibilidad
		[I.8]	Fallo de servicios de comunicaciones	Disponibilidad
		[I.9]	Interrupción de otros servicios y suministros esenciales	Disponibilidad
		[I.10]	Degradación de los soportes de almacenamiento de la información	Disponibilidad
		[E.2]	Errores del administrador	Disponibilidad
				Autenticidad
				Integridad
		[E.20]	Vulnerabilidades de los programas (software)	Integridad
				Disponibilidad
				Confidencialidad
		[E.21]	Errores de mantenimiento / actualización de programas (software)	Integridad
				Disponibilidad
		[E.24]	Caída del sistema por agotamiento de recursos	Disponibilidad
		[A.24]	Denegación del servicio	Disponibilidad
[HW] EQUIPOS INFORMÁTICOS				
[serv]	Servidores			
[ser1]	Servidor de dominio	[N.1]	Fuego	Disponibilidad
		[I.5]	Avería de origen físico o lógico	Disponibilidad
		[I.6]	Corte de suministro	Disponibilidad
		[I.7]	Condiciones inadecuadas de temperatura o humedad	Disponibilidad
		[I.8]	Fallo de servicios de comunicaciones	Disponibilidad
		[I.9]	Interrupción de otros servicios y suministros esenciales	Disponibilidad
		[I.10]	Degradación de los soportes de almacenamiento de la información	Disponibilidad
		[E.9]	Errores de re-encaminamiento	Confidencialidad
		[E.20]	Vulnerabilidades de los programas (software)	Integridad
				Disponibilidad
				Confidencialidad
		[E.21]	Errores de mantenimiento / actualización de programas (software)	Integridad
				Disponibilidad
		[E.23]	Errores de mantenimiento / actualización de equipos (hardware)	Disponibilidad
		[E.24]	Caída del sistema por agotamiento de recursos	Disponibilidad
		[A.4]	Manipulación de la configuración	Integridad
				Confidencialidad
				Disponibilidad
		[A.24]	Denegación del servicio	Disponibilidad
[ser2]	Servidor de proxy	[I.1]	Fuego	Disponibilidad
		[I.5]	Avería de origen físico o lógico	Disponibilidad
		[I.6]	Corte de suministro	Disponibilidad
		[I.7]	Condiciones inadecuadas de temperatura o humedad	Disponibilidad
		[I.8]	Fallo de servicios de comunicaciones	Disponibilidad
		[I.9]	Interrupción de otros servicios y suministros esenciales	Disponibilidad
		[I.10]	Degradación de los soportes de almacenamiento de la información	Disponibilidad

		[E.2]	Errores del administrador	Disponibilidad
				Integridad
				Confidencialidad
		[E.4]	Errores de configuración	Integridad
				Confidencialidad
		[E.20]	Vulnerabilidades de los programas (software)	Integridad
				Disponibilidad
				Confidencialidad
		[E.21]	Errores de mantenimiento / actualización de programas (software)	Integridad
				Disponibilidad
		[E.23]	Errores de mantenimiento / actualización de equipos (hardware)	Disponibilidad
		[E.24]	Caída del sistema por agotamiento de recursos	Disponibilidad
		[E.28]	Indisponibilidad del personal	Disponibilidad
		[A.24]	Denegación del servicio	Disponibilidad
[ser3]	Servidor de base de datos	[I.1]	Fuego	Disponibilidad
		[I.5]	Avería de origen físico o lógico	Disponibilidad
		[I.6]	Corte de suministro	Disponibilidad
		[I.7]	Condiciones inadecuadas de temperatura o humedad	Disponibilidad
		[I.8]	Fallo de servicios de comunicaciones	Disponibilidad
		[I.9]	Interrupción de otros servicios y suministros esenciales	Disponibilidad
		[I.10]	Degradación de los soportes de almacenamiento de la información	Disponibilidad
		[E.2]	Errores del administrador	Disponibilidad
				Integridad
				Confidencialidad
		[E.14]	Escapes de información	Confidencialidad
		[E.15]	Alteración accidental de la información	Integridad
		[E.20]	Vulnerabilidades de los programas (software)	Integridad
				Disponibilidad
				Autenticidad
		[E.21]	Errores de mantenimiento / actualización de programas (software)	Integridad
				Disponibilidad
		[E.23]	Errores de mantenimiento / actualización de equipos (hardware)	Disponibilidad
		[E.24]	Caída del sistema por agotamiento de recursos	Disponibilidad
		[A.15]	Modificación deliberada de la información	Integridad
		[A.24]	Denegación del servicio	Disponibilidad
		[A.28]	Indisponibilidad del personal	Disponibilidad
[ser4]	Servidor de base de datos - backup	[I.1]	Fuego	Disponibilidad
		[I.6]	Corte de suministro	Disponibilidad
		[I.7]	Condiciones inadecuadas de temperatura o humedad	Disponibilidad
		[I.8]	Fallo de servicios de comunicaciones	Disponibilidad
		[I.9]	Interrupción de otros servicios y suministros esenciales	Disponibilidad
		[I.10]	Degradación de los soportes de almacenamiento de la información	Disponibilidad
		[E.2]	Errores del administrador	Disponibilidad
				Integridad
				Confidencialidad
		[E.14]	Escapes de información	Confidencialidad
		[E.15]	Alteración accidental de la información	Integridad
		[E.18]	Destrucción de la información	Disponibilidad
		[E.20]	Vulnerabilidades de los programas (software)	Integridad
				Disponibilidad
				Confidencialidad
		[E.21]	Errores de mantenimiento / actualización de programas (software)	Integridad
				Disponibilidad
		[E.23]	Errores de mantenimiento / actualización de equipos (hardware)	Disponibilidad

		[E.24]	Caída del sistema por agotamiento de recursos	Disponibilidad
		[E.28]	Indisponibilidad del personal	Disponibilidad
		[A.15]	Modificación deliberada de la información	Integridad
		[A.18]	Destrucción de información	Disponibilidad
		[A.24]	Denegación del servicio	Disponibilidad
		[A.28]	Indisponibilidad del personal	Disponibilidad
[ser5]	Servidor web	[I.1]	Fuego	Disponibilidad
		[I.5]	Avería de origen físico o lógico	Disponibilidad
		[I.6]	Corte de suministro	Disponibilidad
		[I.7]	Condiciones inadecuadas de temperatura o humedad	Disponibilidad
		[I.8]	Fallo de servicios de comunicaciones	Disponibilidad
		[I.9]	Interrupción de otros servicios y suministros esenciales	Disponibilidad
		[I.10]	Degradación de los soportes de almacenamiento de la información	Disponibilidad
		[E.14]	Escapes de información	Confidencialidad
		[E.15]	Alteración accidental de la información	Integridad
		[E.20]	Vulnerabilidades de los programas (software)	Integridad
				Disponibilidad
				Confidencialidad
		[E.21]	Errores de mantenimiento / actualización de programas (software)	Integridad
				Disponibilidad
		[E.23]	Errores de mantenimiento / actualización de equipos (hardware)	Disponibilidad
		[E.24]	Caída del sistema por agotamiento de recursos	Disponibilidad
		[A.24]	Denegación del servicio	Disponibilidad
[ser6]	Servidor de archivos	[I.1]	Fuego	Disponibilidad
		[I.5]	Avería de origen físico o lógico	Disponibilidad
		[I.6]	Corte de suministro	Disponibilidad
		[I.7]	Condiciones inadecuadas de temperatura o humedad	Disponibilidad
		[I.8]	Fallo de servicios de comunicaciones	Disponibilidad
		[I.9]	Interrupción de otros servicios y suministros esenciales	Disponibilidad
		[I.10]	Degradación de los soportes de almacenamiento de la información	Disponibilidad
		[E.1]	Errores de los usuarios	Integridad
				Confidencialidad
				Disponibilidad
		[E.14]	Escapes de información	Confidencialidad
		[E.20]	Vulnerabilidades de los programas (software)	Integridad
				Disponibilidad
				Confidencialidad
		[E.21]	Errores de mantenimiento / actualización de programas (software)	Integridad
				Disponibilidad
		[E.23]	Errores de mantenimiento / actualización de equipos (hardware)	Disponibilidad
		[E.24]	Caída del sistema por agotamiento de recursos	Disponibilidad
		[A.5]	Suplantación de la identidad del usuario	Confidencialidad
				Integridad
				Autenticidad
		[A.24]	Denegación del servicio	Disponibilidad
[ser7]	Servidor de datos - OCCA	[I.1]	Fuego	Disponibilidad
		[I.5]	Avería de origen físico o lógico	Disponibilidad
		[I.6]	Corte de suministro	Disponibilidad
		[I.7]	Condiciones inadecuadas de temperatura o humedad	Disponibilidad
		[I.8]	Fallo de servicios de comunicaciones	Disponibilidad
		[I.9]	Interrupción de otros servicios y suministros esenciales	Disponibilidad
		[I.10]	Degradación de los soportes de almacenamiento de la información	Disponibilidad
		[E.20]	Vulnerabilidades de los programas (software)	Integridad
				Disponibilidad

				Confidencialidad
		[E.21]	Errores de mantenimiento / actualización de programas (software)	Integridad
				Disponibilidad
		[E.23]	Errores de mantenimiento / actualización de equipos (hardware)	Disponibilidad
		[E.24]	Caída del sistema por agotamiento de recursos	Disponibilidad
		[A.24]	Denegación del servicio	Disponibilidad
[ser8]	Servidor de base de datos - backup-OCCA	[I.1]	Fuego	Disponibilidad
		[I.5]	Avería de origen físico o lógico	Disponibilidad
		[I.6]	Corte de suministro	Disponibilidad
		[I.7]	Condiciones inadecuadas de temperatura o humedad	Disponibilidad
		[I.8]	Fallo de servicios de comunicaciones	Disponibilidad
		[I.9]	Interrupción de otros servicios y suministros esenciales	Disponibilidad
		[I.10]	Degradación de los soportes de almacenamiento de la información	Disponibilidad
		[E.2]	Errores del administrador	Disponibilidad
				Integridad
				Confidencialidad
		[E.20]	Vulnerabilidades de los programas (software)	Integridad
				Disponibilidad
				Confidencialidad
		[E.21]	Errores de mantenimiento / actualización de programas (software)	Integridad
				Disponibilidad
		[E.23]	Errores de mantenimiento / actualización de equipos (hardware)	Disponibilidad
		[E.24]	Caída del sistema por agotamiento de recursos	Disponibilidad
		[A.6]	Abuso de privilegios de acceso	Confidencialidad
				Integridad
				Disponibilidad
		[A.24]	Denegación del servicio	Disponibilidad
[netw]	Soporte de red			
[swit]	Switch	[I.1]	Fuego	Disponibilidad
		[I.5]	Avería de origen físico o lógico	Disponibilidad
		[I.6]	Corte de suministro	Disponibilidad
		[I.7]	Condiciones inadecuadas de temperatura o humedad	Disponibilidad
		[I.8]	Fallo de servicios de comunicaciones	Disponibilidad
		[I.9]	Interrupción de otros servicios y suministros esenciales	Disponibilidad
		[E.1]	Errores de los usuarios	Integridad
				Confidencialidad
				Disponibilidad
		[E.2]	Errores del administrador	Integridad
				Disponibilidad
				Confidencialidad
		[E.9]	Errores de re-encaminamiento	Confidencialidad
		[E.23]	Errores de mantenimiento / actualización de equipos (hardware)	Disponibilidad
		[E.24]	Caída del sistema por agotamiento de recursos	Disponibilidad
		[A.24]	Denegación del servicio	Disponibilidad
[rout]	Router	[I.1]	Fuego	Disponibilidad
		[I.5]	Avería de origen físico o lógico	Disponibilidad
		[I.6]	Corte de suministro	Disponibilidad
		[I.7]	Condiciones inadecuadas de temperatura o humedad	Disponibilidad
		[I.8]	Fallo de servicios de comunicaciones	Disponibilidad
		[I.9]	Interrupción de otros servicios y suministros esenciales	Disponibilidad
		[E.2]	Errores del administrador	Disponibilidad
				Integridad
				Confidencialidad
		[E.9]	Errores de re-encaminamiento	Confidencialidad

		[E.23]	Errores de mantenimiento / actualización de equipos (hardware)	Disponibilidad
		[E.24]	Caída del sistema por agotamiento de recursos	Disponibilidad
		[A.24]	Denegación del servicio	Disponibilidad
[fire]	Firewall	[I.1]	Fuego	Disponibilidad
		[I.5]	Avería de origen físico o lógico	Disponibilidad
		[I.6]	Corte de suministro	Disponibilidad
		[I.7]	Condiciones inadecuadas de temperatura o humedad	Disponibilidad
		[I.8]	Fallo de servicios de comunicaciones	Disponibilidad
		[I.9]	Interrupción de otros servicios y suministros esenciales	Disponibilidad
		[I.10]	Degradación de los soportes de almacenamiento de la información	Disponibilidad
		[E.20]	Vulnerabilidades de los programas (software)	Integridad
				Disponibilidad
				Confidencialidad
		[E.21]	Errores de mantenimiento / actualización de programas (software)	Integridad
				Disponibilidad
		[E.23]	Errores de mantenimiento / actualización de equipos (hardware)	Disponibilidad
		[E.24]	Caída del sistema por agotamiento de recursos	Disponibilidad
		[A.4]	Manipulación de la configuración	Integridad
				Confidencialidad
				Disponibilidad
		[A.24]	Denegación del servicio	Disponibilidad
[COM] REDES DE COMUNICACIONES				
[cint]	Internet	[I.1]	Fuego	Disponibilidad
		[I.5]	Avería de origen físico o lógico	Disponibilidad
		[I.6]	Corte de suministro	Disponibilidad
		[I.7]	Condiciones inadecuadas de temperatura o humedad	Disponibilidad
		[I.8]	Fallo de servicios de comunicaciones	Disponibilidad
		[I.9]	Interrupción de otros servicios y suministros esenciales	Disponibilidad
		[E.4]	Errores de configuración	Integridad
		[E.9]	Errores de re-encaminamiento	Confidencialidad
		[E.24]	Caída del sistema por agotamiento de recursos	Disponibilidad
		[A.24]	Denegación del servicio	Disponibilidad
[cwfi]	Red Inalámbrica	[I.6]	Corte de suministro	Disponibilidad
		[I.7]	Condiciones inadecuadas de temperatura o humedad	Disponibilidad
		[I.8]	Fallo de servicios de comunicaciones	Disponibilidad
		[I.9]	Interrupción de otros servicios y suministros esenciales	Disponibilidad
		[E.23]	Errores de mantenimiento / actualización de equipos (hardware)	Disponibilidad
		[E.25]	Pérdida de equipos	Disponibilidad
				Confidencialidad
		[A.24]	Denegación del servicio	Disponibilidad
[MEDIA] SOPORTE DE INFORMACIÓN				
[elect]	Electrónicos			
[ele1]	Cintas Magnéticas	[I.1]	Fuego	Disponibilidad
		[I.5]	Avería de origen físico o lógico	Disponibilidad
		[I.10]	Degradación de los soportes de almacenamiento de la información	Disponibilidad
		[A.25]	Robo	Disponibilidad
				Confidencialidad
[ele2]	Disco externo USB	[I.1]	Fuego	Disponibilidad
		[I.5]	Avería de origen físico o lógico	Disponibilidad
		[I.10]	Degradación de los soportes de almacenamiento de la información	Disponibilidad
		[E.1]	Errores de los usuarios	Integridad
				Confidencialidad
				Disponibilidad
		[E.25]	Pérdida de equipos	Disponibilidad

				Confidencialidad
[store]	Storage de respaldo de BD	[I.1]	Fuego	Disponibilidad
		[I.5]	Avería de origen físico o lógico	Disponibilidad
		[I.9]	Interrupción de otros servicios y suministros esenciales	Disponibilidad
		[I.10]	Degradación de los soportes de almacenamiento de la información	Disponibilidad
		[E.23]	Errores de mantenimiento / actualización de equipos (hardware)	Disponibilidad
		[A.24]	Denegación del servicio	Disponibilidad
[noel]	No electrónico			
[mimp]	Material impreso	[I.1]	Fuego	Disponibilidad
		[E.7]	Deficiencias en la organización	Disponibilidad
		[E.14]	Escapes de información	Confidencialidad
		[E.19]	Fugas de información	Confidencialidad
		[A.19]	Divulgación de información	Confidencialidad
		[A.25]	Robo	Disponibilidad
				Confidencialidad
[AUX] EQUIPAMIENTO AUXILIAR				
[powr]	Acumulador de energía UPS	[I.1]	Fuego	Disponibilidad
		[I.5]	Avería de origen físico o lógico	Disponibilidad
		[I.6]	Corte de suministro	Disponibilidad
		[I.7]	Condiciones inadecuadas de temperatura o humedad	Disponibilidad
		[I.8]	Fallo de servicios de comunicaciones	Disponibilidad
		[I.9]	Interrupción de otros servicios y suministros esenciales	Disponibilidad
		[E.1]	Errores de los usuarios	Integridad
				Confidencialidad
				Disponibilidad
		[E.23]	Errores de mantenimiento / actualización de equipos (hardware)	Disponibilidad
		[E.24]	Caída del sistema por agotamiento de recursos	Disponibilidad
[psis]	Sistema de aire acondicionado	[I.1]	Fuego	Disponibilidad
		[I.2]	Daños por agua	Disponibilidad
		[I.*]	Desastres industriales	Disponibilidad
		[I.3]	Contaminación mecánica	Disponibilidad
		[I.4]	Contaminación electromagnética	Disponibilidad
		[I.5]	Avería de origen físico o lógico	Disponibilidad
		[I.6]	Corte de suministro	Disponibilidad
		[I.7]	Condiciones inadecuadas de temperatura o humedad	Disponibilidad
		[I.9]	Interrupción de otros servicios y suministros esenciales	Disponibilidad
		[E.1]	Errores de los usuarios	Integridad
				Confidencialidad
				Disponibilidad
		[E.23]	Errores de mantenimiento / actualización de equipos (hardware)	Disponibilidad
		[E.24]	Caída del sistema por agotamiento de recursos	Disponibilidad
		[A.11]	Acceso no autorizado	Confidencialidad
				Integridad
		[A.23]	Manipulación de los equipos	Confidencialidad
				Disponibilidad
		[A.25]	Robo	Disponibilidad
[gelc]	Grupo electrógeno	[I.1]	Fuego	Disponibilidad
		[I.2]	Daños por agua	Disponibilidad
		[I.4]	Contaminación electromagnética	Disponibilidad
		[I.5]	Avería de origen físico o lógico	Disponibilidad
		[I.6]	Corte de suministro	Disponibilidad
		[I.9]	Interrupción de otros servicios y suministros esenciales	Disponibilidad
		[E.1]	Errores de los usuarios	Integridad
				Confidencialidad
				Disponibilidad

		[E.23]	Errores de mantenimiento / actualización de equipos (hardware)	Disponibilidad
		[E.24]	Caída del sistema por agotamiento de recursos	Disponibilidad
		[A.25]	Robo	Disponibilidad
				Confidencialidad
		[A.28]	Indisponibilidad del personal	Disponibilidad
[cable]	Cableado			
[cab1]	Cableado de red	[I.1]	Fuego	Disponibilidad
		[I.2]	Daños por agua	Disponibilidad
		[I.4]	Contaminación electromagnética	Disponibilidad
		[I.5]	Avería de origen físico o lógico	Disponibilidad
		[E.23]	Errores de mantenimiento / actualización de equipos (hardware)	Disponibilidad
		[A.7]	Uso no previsto	Disponibilidad
				Confidencialidad
				Integridad
		[A.23]	Manipulación de los equipos	Integridad
				Disponibilidad
		[A.25]	Robo	Disponibilidad
				Confidencialidad
		[A.28]	Indisponibilidad del personal	Disponibilidad
[cab2]	Fibra óptica	[I.1]	Fuego	Disponibilidad
		[I.5]	Avería de origen físico o lógico	Disponibilidad
		[E.7]	Deficiencias en la organización	Disponibilidad
		[E.23]	Errores de mantenimiento / actualización de equipos (hardware)	Disponibilidad
		[E.28]	Indisponibilidad del personal	Disponibilidad
		[A.23]	Manipulación de los equipos	Confidencialidad
				Disponibilidad
[L] INSTALACIONES				
[site]	Data Center	[N.*]	Desastres naturales	Disponibilidad
		[I.1]	Fuego	Disponibilidad
		[I.2]	Daños por agua	Disponibilidad
		[I.7]	Condiciones inadecuadas de temperatura o humedad	Disponibilidad
		[I.9]	Interrupción de otros servicios y suministros esenciales	Disponibilidad
		[E.25]	Pérdida de equipos	Disponibilidad
				Confidencialidad
		[A.11]	Acceso no autorizado	Confidencialidad
				Integridad
		[A.26]	Ataque destructivo	Disponibilidad
		[A.27]	Ocupación enemiga	Disponibilidad
				Confidencialidad
		[A.28]	Indisponibilidad del personal	Disponibilidad
[P] PERSONAL				
[ueex]	Usuario externo	[I.8]	Fallo de servicios de comunicaciones	Disponibilidad
		[E.1]	Errores de los usuarios	Integridad
				Confidencialidad
				Disponibilidad
		[E.18]	Destrucción de la información	Disponibilidad
		[E.19]	Fugas de información	Confidencialidad
		[E.20]	Vulnerabilidades de los programas (software)	Integridad
				Disponibilidad
				Confidencialidad
		[E.24]	Caída del sistema por agotamiento de recursos	Disponibilidad
		[E.25]	Pérdida de equipos	Disponibilidad
		[A.6]	Abuso de privilegios de acceso	Confidencialidad
				Integridad
		[A.7]	Uso no previsto	Disponibilidad

				Confidencialidad
				Integridad
		[A.15]	Modificación deliberada de la información	Integridad
		[A.18]	Destrucción de información	Disponibilidad
		[A.25]	Robo	Disponibilidad
				Confidencialidad
		[A.29]	Extorsión	Confidencialidad
				Integridad
				Disponibilidad
[uex1]	Personal de TI	[I.4]	Contaminación electromagnética	Disponibilidad
		[I.7]	Condiciones inadecuadas de temperatura o humedad	Disponibilidad
		[E.1]	Errores de los usuarios	Integridad
				Confidencialidad
				Disponibilidad
		[E.7]	Deficiencias en la organización	Disponibilidad
		[A.19]	Divulgación de información	Confidencialidad
		[A.29]	Extorsión	Confidencialidad
				Integridad
				Disponibilidad
		[A.30]	Ingeniería social	Confidencialidad
				Integridad
				Disponibilidad
[adm1]	Administrador del data center	[I.4]	Contaminación electromagnética	Disponibilidad
		[I.7]	Condiciones inadecuadas de temperatura o humedad	Disponibilidad
		[I.11]	Emanaciones electromagnética	Confidencialidad
		[E.28]	Indisponibilidad del personal	Disponibilidad
		[A.28]	Indisponibilidad del personal	Disponibilidad

Fuente: Elaborada por los autores en base a MAGERIT- V 3.0 - Metodología de Análisis y Gestión de Riesgos de los Sistemas

Se utilizó la tabla Identificación de Amenazas de activos de TI de la Unidad de Red Telemática – UNPRG. En la que se colocaron las amenazas identificadas por el feje de la Unidad de Red Telemática. Es total fueron identificadas 312 amenazas, la mayoría pertenecientes a las del grupo de Origen físico como y Errores no intencionados.

Tabla 38: Valoración de las amenazas en los activos de TI de la Unidad de Red Telemática - UNPRG

VALORACIÓN DE ACTIVOS DE LA UNIDAD DE RED TELEMÁTICA											
ACTIVO		AMENAZA		DIMENSIÓN					TOTAL	NIVEL
CÓDIGO	NOMBRE	CÓDIGO	NOMBRE	DISPONIBILIDAD	INTEGRIDAD	CONFIDENCIALIDAD	AUTENTICIDAD	TRAZABILIDAD		
[S] SERVICIOS										
[sges]	Gestión de Actas virtuales y matricula online	[I.6]	Corte de suministro	0.9					0.9	MUY ALTO
		[I.8]	Fallo de servicios de comunicaciones	0.5					0.5	MEDIO
		[I.9]	Interrupción de otros servicios y suministros esenciales	0.8					0.8	ALTO
		[E.1]	Errores de los usuarios	0.1	0.1	0.1			0.1	BAJO
		[E.20]	Vulnerabilidades de los programas (software)	0.1	0.1	0.1			0.1	BAJO
		[E.24]	Caída del sistema por agotamiento de recursos	0.5					0.5	MEDIO
		[A.24]	Denegación del servicio	0.6					0.6	ALTO
[sgeo]	Gestión de Actas virtuales OCCA	[I.8]	Fallo de servicios de comunicaciones	0.5					0.5	MEDIO
		[I.9]	Interrupción de otros servicios y suministros esenciales	0.6					0.6	ALTO
		[E.1]	Errores de los usuarios	0.01	0.1	0.1			0.1	BAJO
		[E.20]	Vulnerabilidades de los programas (software)	0.1	0.1	0.1			0.1	BAJO
		[A.5]	Suplantación de la identidad del usuario		0.7	0.8	0.8		0.8	ALTO
		[A.24]	Denegación del servicio	0.6					0.6	ALTO
[SW] APLICACIONES										
[swsc]	Sistema académico actas virtuales UNPRG	[N.1]	Fuego	1					1	MUY ALTO
		[I.8]	Fallo de servicios de comunicaciones	1					1	MUY ALTO
		[I.9]	Interrupción de otros servicios y suministros esenciales	0.6					0.6	ALTO
		[E.2]	Errores del administrador	0.7	0.1	0.1			0.3	MEDIO
		[E.21]	Errores de mantenimiento / actualización de programas (software)	0.5	0.1				0.3	MEDIO
		[E.23]	Errores de mantenimiento / actualización de equipos (hardware)	0.5					0.5	MEDIO
		[E.24]	Caída del sistema por agotamiento de recursos	1					1	MUY ALTO
		[A.24]	Denegación del servicio	1					1	MUY ALTO
[swoc]	Sistema académico OCCA	[I.1]	Fuego	1					1	MUY ALTO

		[I.5]	Avería de origen físico o lógico	0.5					0.5	MEDIO
		[I.6]	Corte de suministro	0.8					0.8	ALTO
		[I.7]	Condiciones inadecuadas de temperatura o humedad	0.5					0.5	MEDIO
		[I.8]	Fallo de servicios de comunicaciones	0.7					0.7	ALTO
		[I.9]	Interrupción de otros servicios y suministros esenciales	0.5					0.5	MEDIO
		[I.10]	Degradación de los soportes de almacenamiento de la información	0.7					0.7	ALTO
		[E.2]	Errores del administrador	0.1	0.1	0.1			0.1	BAJO
		[E.20]	Vulnerabilidades de los programas (software)	0.3	0.6	0.5			0.5	MEDIO
		[E.21]	Errores de mantenimiento / actualización de programas (software)	0.9	0.5				0.7	ALTO
		[E.24]	Caída del sistema por agotamiento de recursos	1					1	MUY ALTO
		[A.24]	Denegación del servicio	1					1	MUY ALTO
[HW] EQUIPOS INFORMÁTICOS										
[serv]	Servidores									
[ser1]	Servidor de dominio	[N.1]	Fuego	1					1	MUY ALTO
		[I.5]	Avería de origen físico o lógico	0.5					0.5	MEDIO
		[I.6]	Corte de suministro	0.5					0.5	MEDIO
		[I.7]	Condiciones inadecuadas de temperatura o humedad	0.5					0.5	MEDIO
		[I.8]	Fallo de servicios de comunicaciones	0.5					0.5	MEDIO
		[I.9]	Interrupción de otros servicios y suministros esenciales	0.2					0.2	BAJO
		[I.10]	Degradación de los soportes de almacenamiento de la información	0.1					0.1	BAJO
		[E.9]	Errores de re-encaminamiento			0.2			0.2	BAJO
		[E.20]	Vulnerabilidades de los programas (software)	0.9	0.9	0.7			0.8	MUY ALTO
		[E.21]	Errores de mantenimiento / actualización de programas (software)	0.3	0.1				0.2	BAJO
		[E.23]	Errores de mantenimiento / actualización de equipos (hardware)	0.2					0.2	BAJO
		[E.24]	Caída del sistema por agotamiento de recursos	0.6					0.6	ALTO
		[A.4]	Manipulación de la configuración	0.1	0.1	0.1			0.1	BAJO
		[A.24]	Denegación del servicio	0.9					0.9	MUY ALTO
[ser2]	Servidor de proxy	[I.1]	Fuego	1					1	MUY ALTO
		[I.5]	Avería de origen físico o lógico	0.5					0.5	MEDIO
		[I.6]	Corte de suministro	0.5					0.5	MEDIO
		[I.7]	Condiciones inadecuadas de temperatura o humedad	0.5					0.5	MEDIO
		[I.8]	Fallo de servicios de comunicaciones	0.5					0.5	MEDIO
		[I.9]	Interrupción de otros servicios y suministros esenciales	0.2					0.2	BAJO
		[I.10]	Degradación de los soportes de almacenamiento de la información	0.1					0.1	BAJO
		[E.2]	Errores del administrador	0.1	0.05	0.05			0.1	BAJO
		[E.4]	Errores de configuración		0.2	0.2			0.2	BAJO
		[E.20]	Vulnerabilidades de los programas (software)	0.2	0.3	0.5			0.3	MEDIO
		[E.21]	Errores de mantenimiento / actualización de programas (software)	0.1	0.1				0.1	BAJO

		[E.23]	Errores de mantenimiento / actualización de equipos (hardware)	0.7					0.7	ALTO
		[E.24]	Caída del sistema por agotamiento de recursos	0.5					0.5	MEDIO
		[E.28]	Indisponibilidad del personal	0.2					0.2	BAJO
		[A.24]	Denegación del servicio	0.9					0.9	MUY ALTO
[ser3]	Servidor de base de datos	[I.1]	Fuego	1					1	MUY ALTO
		[I.5]	Avería de origen físico o lógico	0.5					0.5	MEDIO
		[I.6]	Corte de suministro	0.5					0.5	MEDIO
		[I.7]	Condiciones inadecuadas de temperatura o humedad	0.5					0.5	MEDIO
		[I.8]	Fallo de servicios de comunicaciones	0.5					0.5	MEDIO
		[I.9]	Interrupción de otros servicios y suministros esenciales	0.3					0.3	MEDIO
		[I.10]	Degradación de los soportes de almacenamiento de la información	0.1					0.1	BAJO
		[E.2]	Errores del administrador	0.1	0.2	0.2			0.2	BAJO
		[E.14]	Escapes de información			0.7			0.7	ALTO
		[E.15]	Alteración accidental de la información		0.5				0.5	MEDIO
		[E.20]	Vulnerabilidades de los programas (software)	0.1	0.2	0.4			0.2	MEDIO
		[E.21]	Errores de mantenimiento / actualización de programas (software)	0.1	0.1				0.1	BAJO
		[E.23]	Errores de mantenimiento / actualización de equipos (hardware)	0.1					0.1	BAJO
		[E.24]	Caída del sistema por agotamiento de recursos	0.5					0.5	MEDIO
		[A.15]	Modificación deliberada de la información		0.4				0.4	MEDIO
		[A.24]	Denegación del servicio	0.5					0.5	MEDIO
		[A.28]	Indisponibilidad del personal	0.8					0.8	ALTO
[ser4]	Servidor de base de datos - backup	[I.1]	Fuego	0.1					0.1	BAJO
		[I.6]	Corte de suministro	0.5					0.5	MEDIO
		[I.7]	Condiciones inadecuadas de temperatura o humedad	0.5					0.5	MEDIO
		[I.8]	Fallo de servicios de comunicaciones	0.5					0.5	MEDIO
		[I.9]	Interrupción de otros servicios y suministros esenciales	0.5					0.5	MEDIO
		[I.10]	Degradación de los soportes de almacenamiento de la información	0.5					0.5	MEDIO
		[E.2]	Errores del administrador	0.5	0.1	0.1			0.2	MEDIO
		[E.14]	Escapes de información			0.9			0.9	MUY ALTO
		[E.15]	Alteración accidental de la información		0.5				0.5	MEDIO
		[E.18]	Destrucción de la información	0.5					0.5	MEDIO
		[E.20]	Vulnerabilidades de los programas (software)	0.5	0.2	0.1			0.3	MEDIO
		[E.21]	Errores de mantenimiento / actualización de programas (software)	0.5	0.2				0.4	MEDIO
		[E.23]	Errores de mantenimiento / actualización de equipos (hardware)	0.5					0.5	MEDIO
		[E.24]	Caída del sistema por agotamiento de recursos	0.5					0.5	MEDIO
		[E.28]	Indisponibilidad del personal	0.2					0.2	BAJO
		[A.15]	Modificación deliberada de la información		0.5				0.5	MEDIO
		[A.18]	Destrucción de información	0.6					0.6	ALTO

		[A.24]	Denegación del servicio	0.5					0.5	MEDIO
		[A.28]	Indisponibilidad del personal	0.1					0.1	BAJO
[ser5]	Servidor web	[I.1]	Fuego	0.9					0.9	MUY ALTO
		[I.5]	Avería de origen físico o lógico	0.9					0.9	MUY ALTO
		[I.6]	Corte de suministro	0.05					0.1	MUY BAJO
		[I.7]	Condiciones inadecuadas de temperatura o humedad	1					1	MUY ALTO
		[I.8]	Fallo de servicios de comunicaciones	1					1	MUY ALTO
		[I.9]	Interrupción de otros servicios y suministros esenciales	0.5					0.5	MEDIO
		[I.10]	Degradación de los soportes de almacenamiento de la información	0.5					0.5	MEDIO
		[E.14]	Escapes de información			0.05			0.1	MUY BAJO
		[E.15]	Alteración accidental de la información		0.2				0.2	BAJO
		[E.20]	Vulnerabilidades de los programas (software)	0.1	0.2	0.3			0.2	BAJO
		[E.21]	Errores de mantenimiento / actualización de programas (software)	0.1	0.05				0.1	BAJO
		[E.23]	Errores de mantenimiento / actualización de equipos (hardware)	0.1					0.1	BAJO
		[E.24]	Caída del sistema por agotamiento de recursos	1					1	MUY ALTO
		[A.24]	Denegación del servicio	1					1	MUY ALTO
[ser6]	Servidor de archivos	[I.1]	Fuego	0.9					0.9	MUY ALTO
		[I.5]	Avería de origen físico o lógico	0.9					0.9	MUY ALTO
		[I.6]	Corte de suministro	0.05					0.1	MUY BAJO
		[I.7]	Condiciones inadecuadas de temperatura o humedad	1					1	MUY ALTO
		[I.8]	Fallo de servicios de comunicaciones	1					1	MUY ALTO
		[I.9]	Interrupción de otros servicios y suministros esenciales	0.8					0.8	ALTO
		[I.10]	Degradación de los soportes de almacenamiento de la información	0.1					0.1	BAJO
		[E.1]	Errores de los usuarios	0.05	0.1	0.1			0.1	BAJO
		[E.14]	Escapes de información			0.2			0.2	BAJO
		[E.20]	Vulnerabilidades de los programas (software)	0.05	0.1	0.1			0.1	BAJO
		[E.21]	Errores de mantenimiento / actualización de programas (software)	0.1	0.2				0.15	BAJO
		[E.23]	Errores de mantenimiento / actualización de equipos (hardware)	0.1					0.1	BAJO
		[E.24]	Caída del sistema por agotamiento de recursos	1					1	MUY ALTO
		[A.5]	Suplantación de la identidad del usuario		0.1	0.2	0.4		0.2	MEDIO
		[A.24]	Denegación del servicio	1					1	MUY ALTO
[ser7]	Servidor de datos - OCCA	[I.1]	Fuego	0.9					0.9	MUY ALTO
		[I.5]	Avería de origen físico o lógico	0.9					0.9	MUY ALTO
		[I.6]	Corte de suministro	0.05					0.1	MUY BAJO
		[I.7]	Condiciones inadecuadas de temperatura o humedad	1					1	MUY ALTO
		[I.8]	Fallo de servicios de comunicaciones	1					1	MUY ALTO
		[I.9]	Interrupción de otros servicios y suministros esenciales	0.8					0.8	ALTO
		[I.10]	Degradación de los soportes de almacenamiento de la información	0.8					0.8	ALTO

		[E.20]	Vulnerabilidades de los programas (software)	0.1	0.3	0.4			0.3	MEDIO
		[E.21]	Errores de mantenimiento / actualización de programas (software)	0.2	0.05				0.1	BAJO
		[E.23]	Errores de mantenimiento / actualización de equipos (hardware)	0.6					0.6	ALTO
		[E.24]	Caída del sistema por agotamiento de recursos	1					1	MUY ALTO
		[A.24]	Denegación del servicio	1					1	MUY ALTO
[ser8]	Servidor de base de datos - backup-OCCA	[I.1]	Fuego	0.9					0.9	MUY ALTO
		[I.5]	Avería de origen físico o lógico	0.9					0.9	MUY ALTO
		[I.6]	Corte de suministro	0.05					0.05	MUY BAJO
		[I.7]	Condiciones inadecuadas de temperatura o humedad	1					1	MUY ALTO
		[I.8]	Fallo de servicios de comunicaciones	1					1	MUY ALTO
		[I.9]	Interrupción de otros servicios y suministros esenciales	0.9					0.9	MUY ALTO
		[I.10]	Degradación de los soportes de almacenamiento de la información	0.8					0.8	ALTO
		[E.2]	Errores del administrador	0.1	0.05	0.05			0.1	BAJO
		[E.20]	Vulnerabilidades de los programas (software)	0.05	0.1	0.2			0.1	BAJO
		[E.21]	Errores de mantenimiento / actualización de programas (software)	0.05	0.1				0.1	BAJO
		[E.23]	Errores de mantenimiento / actualización de equipos (hardware)	0.1					0.1	BAJO
		[E.24]	Caída del sistema por agotamiento de recursos	1					1	MUY ALTO
		[A.6]	Abuso de privilegios de acceso	0.05	0.1	0.2			0.1	BAJO
		[A.24]	Denegación del servicio	1					1	MUY ALTO
[netw]	Soporte de red									
[swit]	Switch	[I.1]	Fuego	1					1	MUY ALTO
		[I.5]	Avería de origen físico o lógico	1					1	MUY ALTO
		[I.6]	Corte de suministro	1					1	MUY ALTO
		[I.7]	Condiciones inadecuadas de temperatura o humedad	1					1	MUY ALTO
		[I.8]	Fallo de servicios de comunicaciones	1					1	MUY ALTO
		[I.9]	Interrupción de otros servicios y suministros esenciales	1					1	MUY ALTO
		[E.1]	Errores de los usuarios	0.05	0.1	0.05			0.1	BAJO
		[E.2]	Errores del administrador	0.1	0.05	0			0.1	MUY BAJO
		[E.9]	Errores de re-encaminamiento			0.05			0.1	MUY BAJO
		[E.23]	Errores de mantenimiento / actualización de equipos (hardware)	0.9					0.9	MUY ALTO
		[E.24]	Caída del sistema por agotamiento de recursos	0.9					0.9	MUY ALTO
		[A.24]	Denegación del servicio	1					1	MUY ALTO
[rout]	Router	[I.1]	Fuego	1					1	MUY ALTO
		[I.5]	Avería de origen físico o lógico	0.5					0.5	MEDIO
		[I.6]	Corte de suministro	0.05					0.1	MUY BAJO
		[I.7]	Condiciones inadecuadas de temperatura o humedad	1					1	MUY ALTO
		[I.8]	Fallo de servicios de comunicaciones	1					1	MUY ALTO
		[I.9]	Interrupción de otros servicios y suministros esenciales	1					1	MUY ALTO

		[E.2]	Errores del administrador	0.1	0.05	0.01			0.1	
		[E.9]	Errores de re-encaminamiento			0.9			0.9	MUY ALTO
		[E.23]	Errores de mantenimiento / actualización de equipos (hardware)	0.5					0.5	MEDIO
		[E.24]	Caída del sistema por agotamiento de recursos	0.5					0.5	MEDIO
		[A.24]	Denegación del servicio	0.5					0.5	MEDIO
[fire]	Firewall	[I.1]	Fuego	1					1	MUY ALTO
		[I.5]	Avería de origen físico o lógico	0.5					0.5	MEDIO
		[I.6]	Corte de suministro	0.05					0.1	MUY BAJO
		[I.7]	Condiciones inadecuadas de temperatura o humedad	0.4					0.4	MEDIO
		[I.8]	Fallo de servicios de comunicaciones	0.5					0.5	MEDIO
		[I.9]	Interrupción de otros servicios y suministros esenciales	0.5					0.5	MEDIO
		[I.10]	Degradación de los soportes de almacenamiento de la información	0.5					0.5	MEDIO
		[E.20]	Vulnerabilidades de los programas (software)	0.8	0.9	0.6			0.8	ALTO
		[E.21]	Errores de mantenimiento / actualización de programas (software)	0.1	0.1				0.1	BAJO
		[E.23]	Errores de mantenimiento / actualización de equipos (hardware)	0.5					0.5	MEDIO
		[E.24]	Caída del sistema por agotamiento de recursos	0.5					0.5	MEDIO
		[A.4]	Manipulación de la configuración	0.05	0.2	0.1			0.1	BAJO
		[A.24]	Denegación del servicio	0.5					0.5	MEDIO
[COM] REDES DE COMUNICACIONES										
[cint]	Internet	[I.1]	Fuego	0.6					0.6	ALTO
		[I.5]	Avería de origen físico o lógico	0.8					0.8	ALTO
		[I.6]	Corte de suministro	0.5					0.5	MEDIO
		[I.7]	Condiciones inadecuadas de temperatura o humedad	0.8					0.8	ALTO
		[I.8]	Fallo de servicios de comunicaciones	1					1	MUY ALTO
		[I.9]	Interrupción de otros servicios y suministros esenciales	0.2					0.2	BAJO
		[E.4]	Errores de configuración		0.01				0.0	MUY BAJO
		[E.9]	Errores de re-encaminamiento			0.05			0.1	MUY BAJO
		[E.24]	Caída del sistema por agotamiento de recursos	0.5					0.5	MEDIO
		[A.24]	Denegación del servicio	0.5					0.5	MEDIO
[cwfi]	Red Inalámbrica	[I.6]	Corte de suministro	0.5					0.5	MEDIO
		[I.7]	Condiciones inadecuadas de temperatura o humedad	0.3					0.3	MEDIO
		[I.8]	Fallo de servicios de comunicaciones	0.9					0.9	MUY ALTO
		[I.9]	Interrupción de otros servicios y suministros esenciales	0.6					0.6	ALTO
		[E.23]	Errores de mantenimiento / actualización de equipos (hardware)	0.5					0.5	MEDIO
		[E.25]	Pérdida de equipos	0.9		0.1			0.5	MEDIO
		[A.24]	Denegación del servicio	0.8					0.8	ALTO
[MEDIA] SOPORTE DE INFORMACIÓN										
[elect]	Electrónicos									

[ele1]	Cintas Magnéticas	[I.1]	Fuego	1					1	MUY ALTO
		[I.5]	Avería de origen físico o lógico	1					1	MUY ALTO
		[I.10]	Degradación de los soportes de almacenamiento de la información	1					1	MUY ALTO
		[A.25]	Robo	1		0.9			0.95	MUY ALTO
[ele2]	Disco externo USB	[I.1]	Fuego	1					1	MUY ALTO
		[I.5]	Avería de origen físico o lógico	0.5					0.5	MEDIO
		[I.10]	Degradación de los soportes de almacenamiento de la información	0.5					0.5	MEDIO
		[E.1]	Errores de los usuarios	0.05	0.8	0.1			0.3	MEDIO
		[E.25]	Pérdida de equipos	0.9		0.5			0.7	ALTO
[store]	Storage de respaldo de BD	[I.1]	Fuego	1					1	MUY ALTO
		[I.5]	Avería de origen físico o lógico	0.5					0.5	MEDIO
		[I.9]	Interrupción de otros servicios y suministros esenciales	0.8					0.8	ALTO
		[I.10]	Degradación de los soportes de almacenamiento de la información	0.5					0.5	MEDIO
		[E.23]	Errores de mantenimiento / actualización de equipos (hardware)	0.5					0.5	MEDIO
		[A.24]	Denegación del servicio	0.05					0.1	MUY BAJO
[noel]	No electrónico									
[mimp]	Material impreso	[I.1]	Fuego	1					1	MUY ALTO
		[E.7]	Deficiencias en la organización	0.4					0.4	MEDIO
		[E.14]	Escapes de información			0.1			0.1	BAJO
		[E.19]	Fugas de información			0.2			0.2	BAJO
		[A.19]	Divulgación de información			0.1			0.1	BAJO
		[A.25]	Robo	0.5		0.2			0.4	MEDIO
[AUX] EQUIPAMIENTO AUXILIAR										
[powr]	Acumulador de energía UPS	[I.1]	Fuego	1					1	MUY ALTO
		[I.5]	Avería de origen físico o lógico	1					1	MUY ALTO
		[I.6]	Corte de suministro	0.05					0.1	MUY BAJO
		[I.7]	Condiciones inadecuadas de temperatura o humedad	0.1					0.1	BAJO
		[I.8]	Fallo de servicios de comunicaciones	0.01					0.0	MUY BAJO
		[I.9]	Interrupción de otros servicios y suministros esenciales	0.05					0.1	MUY BAJO
		[E.1]	Errores de los usuarios	0.3	0.5	0			0.3	MEDIO
		[E.23]	Errores de mantenimiento / actualización de equipos (hardware)	0.7					0.7	ALTO
		[E.24]	Caída del sistema por agotamiento de recursos	1					1	MUY ALTO
[psis]	Sistema de aire acondicionado	[I.1]	Fuego	1					1	MUY ALTO
		[I.2]	Daños por agua	0.5					0.5	MEDIO
		[I.*]	Desastres industriales	0.5					0.5	MEDIO
		[I.3]	Contaminación mecánica	0.05					0.1	MUY BAJO
		[I.4]	Contaminación electromagnética	0.05					0.1	MUY BAJO
		[I.5]	Avería de origen físico o lógico	0.5					0.5	MEDIO

		[I.6]	Corte de suministro	0.1					0.1	BAJO
		[I.7]	Condiciones inadecuadas de temperatura o humedad	0.5					0.5	MEDIO
		[I.9]	Interrupción de otros servicios y suministros esenciales	0.9					0.9	MUY ALTO
		[E.1]	Errores de los usuarios	0.7	0.5	0			0.4	MEDIO
		[E.23]	Errores de mantenimiento / actualización de equipos (hardware)	0.5					0.5	MEDIO
		[E.24]	Caída del sistema por agotamiento de recursos	1					1	MUY ALTO
		[A.11]	Acceso no autorizado		0.05	0			0.03	MUY BAJO
		[A.23]	Manipulación de los equipos		0.5	0			0.3	MEDIO
		[A.25]	Robo	1		0			0.5	MEDIO
[gelc]	Grupo electrógeno	[I.1]	Fuego	1					1	MUY ALTO
		[I.2]	Daños por agua	1					1	MUY ALTO
		[I.4]	Contaminación electromagnética	0.05					0.1	MUY BAJO
		[I.5]	Avería de origen físico o lógico	1					1	MUY ALTO
		[I.6]	Corte de suministro	0.05					0.1	MUY BAJO
		[I.9]	Interrupción de otros servicios y suministros esenciales	0.2					0.2	BAJO
		[E.1]	Errores de los usuarios	0.3	0.4	0			0.2	MEDIO
		[E.23]	Errores de mantenimiento / actualización de equipos (hardware)	0.6					0.6	ALTO
		[E.24]	Caída del sistema por agotamiento de recursos	1					1	MUY ALTO
		[A.25]	Robo	1		0			0.5	MEDIO
		[A.28]	Indisponibilidad del personal	0.3					0.3	MEDIO
[cable]	Cableado									
[cab1]	Cableado de red	[I.1]	Fuego	0.7					0.7	ALTO
		[I.2]	Daños por agua	0.7					0.7	ALTO
		[I.4]	Contaminación electromagnética	0.1					0.1	BAJO
		[I.5]	Avería de origen físico o lógico	0.7					0.7	ALTO
		[E.23]	Errores de mantenimiento / actualización de equipos (hardware)	0.2					0.2	BAJO
		[A.7]	Uso no previsto	0.2	0.01	0.5			0.2	MEDIO
		[A.23]	Manipulación de los equipos	0.2	0.05				0.1	BAJO
		[A.25]	Robo	0.1		0			0.05	MUY BAJO
		[A.28]	Indisponibilidad del personal	0.05					0.05	MUY BAJO
[cab2]	Fibra óptica	[I.1]	Fuego	0.7					0.7	ALTO
		[I.5]	Avería de origen físico o lógico	0.3					0.3	MEDIO
		[E.7]	Deficiencias en la organización	0.1					0.1	BAJO
		[E.23]	Errores de mantenimiento / actualización de equipos (hardware)	0.2					0.2	BAJO
		[E.28]	Indisponibilidad del personal	0.05					0.05	MUY BAJO
		[A.23]	Manipulación de los equipos	0.1		0			0.05	MUY BAJO
[L] INSTALACIONES										
[site]	Data Center	[N.*]	Desastres naturales	1					1	MUY ALTO

		[I.1]	Fuego	1					1	MUY ALTO
		[I.2]	Daños por agua	0.05					0.05	MUY BAJO
		[I.7]	Condiciones inadecuadas de temperatura o humedad	0.9					0.9	MUY ALTO
		[I.9]	Interrupción de otros servicios y suministros esenciales	0.5					0.5	MEDIO
		[E.25]	Pérdida de equipos	0.2		0.05			0.1	BAJO
		[A.11]	Acceso no autorizado		0.3	0.4			0.4	MEDIO
		[A.26]	Ataque destructivo	0.9					0.9	MUY ALTO
		[A.27]	Ocupación enemiga	1		0.5			0.8	ALTO
		[A.28]	Indisponibilidad del personal	0.8					0.8	ALTO
[P] PERSONAL										
[ueex]	Usuario externo	[I.8]	Fallo de servicios de comunicaciones	0.6					0.6	ALTO
		[E.1]	Errores de los usuarios	0.1	0.5	0.2			0.3	MEDIO
		[E.18]	Destrucción de la información	0.2					0.2	BAJO
		[E.19]	Fugas de información			0.2			0.2	BAJO
		[E.20]	Vulnerabilidades de los programas (software)	0.2	0.3	0.1			0.2	BAJO
		[E.24]	Caída del sistema por agotamiento de recursos	0.4					0.4	MEDIO
		[E.25]	Pérdida de equipos	0.1	0.05				0.1	BAJO
		[A.6]	Abuso de privilegios de acceso		0.1	0.2			0.2	BAJO
		[A.7]	Uso no previsto	0.2	0.05	0.1			0.1	BAJO
		[A.15]	Modificación deliberada de la información		0.2				0.2	BAJO
		[A.18]	Destrucción de información	0.5					0.5	MEDIO
		[A.25]	Robo	0.5		0.5			0.5	MEDIO
		[A.29]	Extorsión	0.6	0.5	0.7			0.6	ALTO
[uex1]	Personal de TI	[I.4]	Contaminación electromagnética	0.5					0.5	MEDIO
		[I.7]	Condiciones inadecuadas de temperatura o humedad	0.5					0.5	MEDIO
		[E.1]	Errores de los usuarios	0.3	0	0			0.1	BAJO
		[E.7]	Deficiencias en la organización	0.5					0.5	MEDIO
		[A.19]	Divulgación de información			0.2			0.2	BAJO
		[A.29]	Extorsión	0.05					0.05	MUY BAJO
		[A.30]	Ingeniería social	0.1	0.2	0.3			0.2	BAJO
[adm1]	Administrador del data center	[I.4]	Contaminación electromagnética	0.5					0.5	MEDIO
		[I.7]	Condiciones inadecuadas de temperatura o humedad	0.5					0.5	MEDIO
		[I.11]	Emanaciones electromagnética			0.3			0.3	MEDIO
		[E.28]	Indisponibilidad del personal	0.9					0.9	MUY ALTO
		[A.28]	Indisponibilidad del personal	0.2					0.2	BAJO

Fuente: Elaborada por los autores en base a MAGERIT- V 3.0 - Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro II

5.1.6. Estimación del Impacto

Se utilizó la tabla Valoración del Impacto de las Amenazas en los activos de TI de la Unidad de Red Telemática - UNPRG. El impacto se obtuvo de la multiplicación del valor del activo por el desgaste que puede ser causado por las amenazas. De eso se obtuvo el nivel de impacto de las amenazas en los activos. Amenazas como fuego, fallo en el servicio de comunicaciones, caída del sistema por agotamiento de recursos y denegación del servicio son amenazas que tendrían un nivel de impacto de alto y muy alto en los activos de TI de la Unidad de Red Telemática de la Universidad Nacional Pedro Ruiz Gallo.

Tabla 39: Valoración del Impacto de las Amenazas en los activos de TI de la Unidad de Red Telemática - UNPRG.

VALORACIÓN DEL IMPACTO								
ACTIVO		AMENAZA		VALOR DE ACTIVO	DESGASTE	IMPACTO	ESCALA	NIVEL
CÓDIGO	NOMBRE	CÓDIGO	NOMBRE					
[S] SERVICIOS								
[sges]	Gestión de Actas virtuales y matricula online	[I.6]	Corte de suministro	3	0.9	2.7	MEDIO	3
		[I.8]	Fallo de servicios de comunicaciones		0.5	1.5	BAJO	2
		[I.9]	Interrupción de otros servicios y suministros esenciales		0.8	2.4	MEDIO	3
		[E.1]	Errores de los usuarios		0.1	0.3	BAJO	2
		[E.20]	Vulnerabilidades de los programas (software)		0.1	0.3	BAJO	2
		[E.24]	Caída del sistema por agotamiento de recursos		0.5	1.5	BAJO	2
		[A.24]	Denegación del servicio		0.6	1.8	BAJO	2
[sgeo]	Gestión de Actas virtuales OCCA	[I.8]	Fallo de servicios de comunicaciones	2.4	0.5	1.2	BAJO	2
		[I.9]	Interrupción de otros servicios y suministros esenciales		0.6	1.44	BAJO	2
		[E.1]	Errores de los usuarios		0.07	0.168	BAJO	2
		[E.20]	Vulnerabilidades de los programas (software)		0.1	0.24	BAJO	2
		[A.5]	Suplantación de la identidad del usuario		0.8	1.84	BAJO	2
		[A.24]	Denegación del servicio		0.6	1.44	BAJO	2
[SW] APLICACIONES								
[swsc]	Sistema académico actas virtuales UNPRG	[N.1]	Fuego	5	1	5	ALTO	4
		[I.8]	Fallo de servicios de comunicaciones		1	5	ALTO	4
		[I.9]	Interrupción de otros servicios y suministros esenciales		0.6	3	MEDIO	3
		[E.2]	Errores del administrador		0.3	1.5	BAJO	2
		[E.21]	Errores de mantenimiento / actualización de programas (software)		0.3	1.5	BAJO	2
		[E.23]	Errores de mantenimiento / actualización de equipos (hardware)		0.5	2.5	MEDIO	3
		[E.24]	Caída del sistema por agotamiento de recursos		1	5	ALTO	4
		[A.24]	Denegación del servicio		1	5	ALTO	4
[swoc]	Sistema académico OCCA	[I.1]	Fuego	3.25	1	3.25	ALTO	4
		[I.5]	Avería de origen físico o lógico		0.5	1.625	BAJO	2
		[I.6]	Corte de suministro		0.8	2.6	MEDIO	3
		[I.7]	Condiciones inadecuadas de temperatura o humedad		0.5	1.625	BAJO	2
		[I.8]	Fallo de servicios de comunicaciones		0.7	2.275	MEDIO	3
		[I.9]	Interrupción de otros servicios y suministros esenciales		0.5	1.625	BAJO	2
		[I.10]	Degradación de los soportes de almacenamiento de la información		0.7	2.275	MEDIO	3

		[E.2]	Errores del administrador		0.1	0.325	BAJO	2
		[E.20]	Vulnerabilidades de los programas (software)		0.5	1.51667	BAJO	2
		[E.21]	Errores de mantenimiento / actualización de programas (software)		0.7	2.275	MEDIO	3
		[E.24]	Caída del sistema por agotamiento de recursos		1	3.25	ALTO	4
		[A.24]	Denegación del servicio		1	3.25	ALTO	4
[HW] EQUIPOS INFORMÁTICOS								
[serv]	Servidores							
[ser1]	Servidor de dominio	[N.1]	Fuego	3.75	1	3.75	ALTO	4
		[I.5]	Avería de origen físico o lógico		0.5	1.875	BAJO	2
		[I.6]	Corte de suministro		0.5	1.875	BAJO	2
		[I.7]	Condiciones inadecuadas de temperatura o humedad		0.5	1.875	BAJO	2
		[I.8]	Fallo de servicios de comunicaciones		0.5	1.875	BAJO	2
		[I.9]	Interrupción de otros servicios y suministros esenciales		0.2	0.75	BAJO	2
		[I.10]	Degradación de los soportes de almacenamiento de la información		0.1	0.375	BAJO	2
		[E.9]	Errores de re-encaminamiento		0.2	0.75	BAJO	2
		[E.20]	Vulnerabilidades de los programas (software)		0.8	3.125	ALTO	4
		[E.21]	Errores de mantenimiento / actualización de programas (software)		0.2	0.75	BAJO	2
		[E.23]	Errores de mantenimiento / actualización de equipos (hardware)		0.2	0.75	BAJO	2
		[E.24]	Caída del sistema por agotamiento de recursos		0.6	2.25	MEDIO	3
		[A.4]	Manipulación de la configuración		0.1	0.375	BAJO	2
		[A.24]	Denegación del servicio		0.9	3.375	ALTO	4
[ser2]	Servidor de proxy	[I.1]	Fuego	2	1	2	BAJO	2
		[I.5]	Avería de origen físico o lógico		0.5	1	BAJO	2
		[I.6]	Corte de suministro		0.5	1	BAJO	2
		[I.7]	Condiciones inadecuadas de temperatura o humedad		0.5	1	BAJO	2
		[I.8]	Fallo de servicios de comunicaciones		0.5	1	BAJO	2
		[I.9]	Interrupción de otros servicios y suministros esenciales		0.2	0.4	BAJO	2
		[I.10]	Degradación de los soportes de almacenamiento de la información		0.1	0.2	BAJO	2
		[E.2]	Errores del administrador		0.07	0.13333	BAJO	2
		[E.4]	Errores de configuración		0.2	0.4	BAJO	2
		[E.20]	Vulnerabilidades de los programas (software)		0.3	0.66667	BAJO	2
		[E.21]	Errores de mantenimiento / actualización de programas (software)		0.1	0.2	BAJO	2
		[E.23]	Errores de mantenimiento / actualización de equipos (hardware)		0.7	1.4	BAJO	2
		[E.24]	Caída del sistema por agotamiento de recursos		0.5	1	BAJO	2
		[E.28]	Indisponibilidad del personal		0.2	0.4	BAJO	2
		[A.24]	Denegación del servicio		0.9	1.8	BAJO	2
[ser3]	Servidor de base de datos	[I.1]	Fuego	5	1	5	ALTO	4
		[I.5]	Avería de origen físico o lógico		0.5	2.5	MEDIO	3
		[I.6]	Corte de suministro		0.5	2.5	MEDIO	3
		[I.7]	Condiciones inadecuadas de temperatura o humedad		0.5	2.5	MEDIO	3
		[I.8]	Fallo de servicios de comunicaciones		0.5	2.5	MEDIO	3
		[I.9]	Interrupción de otros servicios y suministros esenciales		0.3	1.5	BAJO	2
		[I.10]	Degradación de los soportes de almacenamiento de la información		0.1	0.5	BAJO	2
		[E.2]	Errores del administrador		0.2	0.83333	BAJO	2
		[E.14]	Escapes de información		0.7	3.5	ALTO	4
		[E.15]	Alteración accidental de la información		0.5	2.5	MEDIO	3
		[E.20]	Vulnerabilidades de los programas (software)		0.2	1.16667	BAJO	2
		[E.21]	Errores de mantenimiento / actualización de programas (software)		0.1	0.5	BAJO	2
		[E.23]	Errores de mantenimiento / actualización de equipos (hardware)		0.1	0.5	BAJO	2
		[E.24]	Caída del sistema por agotamiento de recursos		0.5	2.5	MEDIO	3
		[A.15]	Modificación deliberada de la información		0.4	2	BAJO	2
		[A.24]	Denegación del servicio		0.5	2.5	MEDIO	3

		[A.28]	Indisponibilidad del personal		0.8	4	ALTO	4
[ser4]	Servidor de base de datos - backup	[I.1]	Fuego	4.5	0.1	0.45	BAJO	2
		[I.6]	Corte de suministro		0.5	2.25	MEDIO	3
		[I.7]	Condiciones inadecuadas de temperatura o humedad		0.5	2.25	MEDIO	3
		[I.8]	Fallo de servicios de comunicaciones		0.5	2.25	MEDIO	3
		[I.9]	Interrupción de otros servicios y suministros esenciales		0.5	2.25	MEDIO	3
		[I.10]	Degradación de los soportes de almacenamiento de la información		0.5	2.25	MEDIO	3
		[E.2]	Errores del administrador		0.2	1.05	BAJO	2
		[E.14]	Escapes de información		0.9	4.05	ALTO	4
		[E.15]	Alteración accidental de la información		0.5	2.25	MEDIO	3
		[E.18]	Destrucción de la información		0.5	2.25	MEDIO	3
		[E.20]	Vulnerabilidades de los programas (software)		0.3	1.2	BAJO	2
		[E.21]	Errores de mantenimiento / actualización de programas (software)		0.35	1.575	BAJO	2
		[E.23]	Errores de mantenimiento / actualización de equipos (hardware)		0.5	2.25	MEDIO	3
		[E.24]	Caída del sistema por agotamiento de recursos		0.5	2.25	MEDIO	3
		[E.28]	Indisponibilidad del personal		0.2	0.9	BAJO	2
		[A.15]	Modificación deliberada de la información		0.5	2.25	MEDIO	3
		[A.18]	Destrucción de información		0.6	2.7	MEDIO	3
		[A.24]	Denegación del servicio		0.5	2.25	MEDIO	3
		[A.28]	Indisponibilidad del personal		0.1	0.45	BAJO	2
[ser5]	Servidor web	[I.1]	Fuego	2.2	0.9	1.98	BAJO	2
		[I.5]	Avería de origen físico o lógico		0.9	1.98	BAJO	2
		[I.6]	Corte de suministro		0.05	0.11	BAJO	2
		[I.7]	Condiciones inadecuadas de temperatura o humedad		1	2.2	MEDIO	3
		[I.8]	Fallo de servicios de comunicaciones		1	2.2	MEDIO	3
		[I.9]	Interrupción de otros servicios y suministros esenciales		0.5	1.1	BAJO	2
		[I.10]	Degradación de los soportes de almacenamiento de la información		0.5	1.1	BAJO	2
		[E.14]	Escapes de información		0.05	0.11	BAJO	2
		[E.15]	Alteración accidental de la información		0.2	0.44	BAJO	2
		[E.20]	Vulnerabilidades de los programas (software)		0.2	0.44	BAJO	2
		[E.21]	Errores de mantenimiento / actualización de programas (software)		0.1	0.165	BAJO	2
		[E.23]	Errores de mantenimiento / actualización de equipos (hardware)		0.1	0.22	BAJO	2
		[E.24]	Caída del sistema por agotamiento de recursos		1	2.2	MEDIO	3
		[A.24]	Denegación del servicio		1	2.2	MEDIO	3
[ser6]	Servidor de archivos	[I.1]	Fuego	2	0.9	1.8	BAJO	2
		[I.5]	Avería de origen físico o lógico		0.9	1.8	BAJO	2
		[I.6]	Corte de suministro		0.1	0.1	BAJO	2
		[I.7]	Condiciones inadecuadas de temperatura o humedad		1	2	BAJO	2
		[I.8]	Fallo de servicios de comunicaciones		1	2	BAJO	2
		[I.9]	Interrupción de otros servicios y suministros esenciales		0.8	1.6	BAJO	2
		[I.10]	Degradación de los soportes de almacenamiento de la información		0.1	0.2	BAJO	2
		[E.1]	Errores de los usuarios		0.1	0.16667	BAJO	2
		[E.14]	Escapes de información		0.2	0.4	BAJO	2
		[E.20]	Vulnerabilidades de los programas (software)		0.1	0.16667	BAJO	2
		[E.21]	Errores de mantenimiento / actualización de programas (software)		0.15	0.3	BAJO	2
		[E.23]	Errores de mantenimiento / actualización de equipos (hardware)		0.1	0.2	BAJO	2
		[E.24]	Caída del sistema por agotamiento de recursos		1	2	BAJO	2
		[A.5]	Suplantación de la identidad del usuario		0.2	0.46667	BAJO	2
		[A.24]	Denegación del servicio		1	2	BAJO	2
[ser7]	Servidor de datos - OCCA	[I.1]	Fuego	2.2	0.9	1.98	BAJO	2
		[I.5]	Avería de origen físico o lógico		0.9	1.98	BAJO	2
		[I.6]	Corte de suministro		0.05	0.11	BAJO	2
		[I.7]	Condiciones inadecuadas de temperatura o humedad		1	2.2	MEDIO	3

		[I.8]	Fallo de servicios de comunicaciones		1	2.2	MEDIO	3
		[I.9]	Interrupción de otros servicios y suministros esenciales		0.8	1.76	BAJO	2
		[I.10]	Degradación de los soportes de almacenamiento de la información		0.8	1.76	BAJO	2
		[E.20]	Vulnerabilidades de los programas (software)		0.3	0.58667	BAJO	2
		[E.21]	Errores de mantenimiento / actualización de programas (software)		0.125	0.275	BAJO	2
		[E.23]	Errores de mantenimiento / actualización de equipos (hardware)		0.6	1.32	BAJO	2
		[E.24]	Caída del sistema por agotamiento de recursos		1	2.2	MEDIO	3
		[A.24]	Denegación del servicio		1	2.2	MEDIO	3
[ser8]	Servidor de base de datos - backup-OCCA	[I.1]	Fuego	2.75	0.9	2.475	MEDIO	3
		[I.5]	Avería de origen físico o lógico		0.9	2.475	MEDIO	3
		[I.6]	Corte de suministro		0.05	0.1375	BAJO	2
		[I.7]	Condiciones inadecuadas de temperatura o humedad		1	2.75	MEDIO	3
		[I.8]	Fallo de servicios de comunicaciones		1	2.75	MEDIO	3
		[I.9]	Interrupción de otros servicios y suministros esenciales		0.9	2.475	MEDIO	3
		[I.10]	Degradación de los soportes de almacenamiento de la información		0.8	2.2	MEDIO	3
		[E.2]	Errores del administrador		0.1	0.18333	BAJO	2
		[E.20]	Vulnerabilidades de los programas (software)		0.1	0.32083	BAJO	2
		[E.21]	Errores de mantenimiento / actualización de programas (software)		0.075	0.20625	BAJO	2
		[E.23]	Errores de mantenimiento / actualización de equipos (hardware)		0.1	0.275	BAJO	2
		[E.24]	Caída del sistema por agotamiento de recursos		1	2.75	MEDIO	3
		[A.6]	Abuso de privilegios de acceso		0.1	0.32083	BAJO	2
		[A.24]	Denegación del servicio		1	2.75	MEDIO	3
[netw]	Soporte de red							
[swit]	Switch	[I.1]	Fuego	2	1	2	BAJO	2
		[I.5]	Avería de origen físico o lógico		1	2	BAJO	2
		[I.6]	Corte de suministro		1	2	BAJO	2
		[I.7]	Condiciones inadecuadas de temperatura o humedad		1	2	BAJO	2
		[I.8]	Fallo de servicios de comunicaciones		1	2	BAJO	2
		[I.9]	Interrupción de otros servicios y suministros esenciales		1	2	BAJO	2
		[E.1]	Errores de los usuarios		0.1	0.13333	BAJO	2
		[E.2]	Errores del administrador		0.05	0.1	BAJO	2
		[E.9]	Errores de re-encaminamiento		0.05	0.1	BAJO	2
		[E.23]	Errores de mantenimiento / actualización de equipos (hardware)		0.9	1.8	BAJO	2
		[E.24]	Caída del sistema por agotamiento de recursos		0.9	1.8	BAJO	2
		[A.24]	Denegación del servicio		1	2	BAJO	2
[rout]	Router	[I.1]	Fuego	2	1	2	BAJO	2
		[I.5]	Avería de origen físico o lógico		0.5	1	BAJO	2
		[I.6]	Corte de suministro		0.05	0.1	BAJO	2
		[I.7]	Condiciones inadecuadas de temperatura o humedad		1	2	BAJO	2
		[I.8]	Fallo de servicios de comunicaciones		1	2	BAJO	2
		[I.9]	Interrupción de otros servicios y suministros esenciales		1	2	BAJO	2
		[E.2]	Errores del administrador		0.1	0.10667	BAJO	2
		[E.9]	Errores de re-encaminamiento		0.9	1.8	BAJO	2
		[E.23]	Errores de mantenimiento / actualización de equipos (hardware)		0.5	1	BAJO	2
		[E.24]	Caída del sistema por agotamiento de recursos		0.5	1	BAJO	2
		[A.24]	Denegación del servicio		0.5	1	BAJO	2
[fire]	Firewall	[I.1]	Fuego	3.7	1	3.66667	ALTO	4
		[I.5]	Avería de origen físico o lógico		0.5	1.83333	BAJO	2
		[I.6]	Corte de suministro		0.05	0.18333	BAJO	2
		[I.7]	Condiciones inadecuadas de temperatura o humedad		0.4	1.46667	BAJO	2
		[I.8]	Fallo de servicios de comunicaciones		0.5	1.83333	BAJO	2
		[I.9]	Interrupción de otros servicios y suministros esenciales		0.5	1.83333	BAJO	2
		[I.10]	Degradación de los soportes de almacenamiento de la información		0.5	1.83333	BAJO	2

		[E.20]	Vulnerabilidades de los programas (software)		0.8	2.81111	MEDIO	3
		[E.21]	Errores de mantenimiento / actualización de programas (software)		0.1	0.36667	BAJO	2
		[E.23]	Errores de mantenimiento / actualización de equipos (hardware)		0.5	1.83333	BAJO	2
		[E.24]	Caída del sistema por agotamiento de recursos		0.5	1.83333	BAJO	2
		[A.4]	Manipulación de la configuración		0.1	0.42778	BAJO	2
		[A.24]	Denegación del servicio		0.5	1.83333	BAJO	2
[COM] REDES DE COMUNICACIONES								
[cint]	Internet	[I.1]	Fuego	3	0.6	1.8	BAJO	2
		[I.5]	Avería de origen físico o lógico		0.8	2.4	MEDIO	3
		[I.6]	Corte de suministro		0.5	1.5	BAJO	2
		[I.7]	Condiciones inadecuadas de temperatura o humedad		0.8	2.4	MEDIO	3
		[I.8]	Fallo de servicios de comunicaciones		1	3	MEDIO	3
		[I.9]	Interrupción de otros servicios y suministros esenciales		0.2	0.6	BAJO	2
		[E.4]	Errores de configuración		0.01	0.03	MUY BAJO	1
		[E.9]	Errores de re-encaminamiento		0.05	0.15	BAJO	2
		[E.24]	Caída del sistema por agotamiento de recursos		0.5	1.5	BAJO	2
		[A.24]	Denegación del servicio		0.5	1.5	BAJO	2
[cwfi]	Red Inalámbrica	[I.6]	Corte de suministro	3	0.5	1.5	BAJO	2
		[I.7]	Condiciones inadecuadas de temperatura o humedad		0.3	0.9	BAJO	2
		[I.8]	Fallo de servicios de comunicaciones		0.9	2.7	MEDIO	3
		[I.9]	Interrupción de otros servicios y suministros esenciales		0.6	1.8	BAJO	2
		[E.23]	Errores de mantenimiento / actualización de equipos (hardware)		0.5	1.5	BAJO	2
		[E.25]	Pérdida de equipos		0.5	1.5	BAJO	2
		[A.24]	Denegación del servicio		0.8	2.4	MEDIO	3
[MEDIA] SOPORTE DE INFORMACIÓN								
[elect]	Electrónicos							
[ele1]	Cintas Magnéticas	[I.1]	Fuego	4.5	1	4.5	ALTO	4
		[I.5]	Avería de origen físico o lógico		1	4.5	ALTO	4
		[I.10]	Degradación de los soportes de almacenamiento de la información		1	4.5	ALTO	4
		[A.25]	Robo		0.95	4.275	ALTO	4
[ele2]	Disco externo USB	[I.1]	Fuego	3.75	1	3.75	ALTO	4
		[I.5]	Avería de origen físico o lógico		0.5	1.875	BAJO	2
		[I.10]	Degradación de los soportes de almacenamiento de la información		0.5	1.875	BAJO	2
		[E.1]	Errores de los usuarios		0.3	1.1875	BAJO	2
		[E.25]	Pérdida de equipos		0.7	2.625	MEDIO	3
[store]	Storage de respaldo de BD	[I.1]	Fuego	4.5	1	4.5	ALTO	4
		[I.5]	Avería de origen físico o lógico		0.5	2.25	MEDIO	3
		[I.9]	Interrupción de otros servicios y suministros esenciales		0.8	3.6	ALTO	4
		[I.10]	Degradación de los soportes de almacenamiento de la información		0.5	2.25	MEDIO	3
		[E.23]	Errores de mantenimiento / actualización de equipos (hardware)		0.5	2.25	MEDIO	3
		[A.24]	Denegación del servicio		0.05	0.225	BAJO	2
[noel]	No electrónico							
[mimp]	Material impreso	[I.1]	Fuego	5.3	1	5.33333	ALTO	4
		[E.7]	Deficiencias en la organización		0.4	2.13333	MEDIO	3
		[E.14]	Escapes de información		0.1	0.53333	BAJO	2
		[E.19]	Fugas de información		0.2	1.06667	BAJO	2
		[A.19]	Divulgación de información		0.1	0.53333	BAJO	2
		[A.25]	Robo		0.35	1.86667	BAJO	2
[AUX] EQUIPAMIENTO AUXILIAR								
[powr]	Acumulador de energía UPS	[I.1]	Fuego	5	1	5	ALTO	4
		[I.5]	Avería de origen físico o lógico		1	5	ALTO	4
		[I.6]	Corte de suministro		0.05	0.25	BAJO	2
		[I.7]	Condiciones inadecuadas de temperatura o humedad		0.1	0.5	BAJO	2

		[I.8]	Fallo de servicios de comunicaciones		0.01	0.05	MUY BAJO	1
		[I.9]	Interrupción de otros servicios y suministros esenciales		0.05	0.25	BAJO	2
		[E.1]	Errores de los usuarios		0.3	1.33333	BAJO	2
		[E.23]	Errores de mantenimiento / actualización de equipos (hardware)		0.7	3.5	ALTO	4
		[E.24]	Caída del sistema por agotamiento de recursos		1	5	ALTO	4
[psis]	Sistema de aire acondicionado	[I.1]	Fuego	5	1	5	ALTO	4
		[I.2]	Daños por agua		0.5	2.5	MEDIO	3
		[I.*]	Desastres industriales		0.5	2.5	MEDIO	3
		[I.3]	Contaminación mecánica		0.05	0.25	BAJO	2
		[I.4]	Contaminación electromagnética		0.05	0.25	BAJO	2
		[I.5]	Avería de origen físico o lógico		0.5	2.5	MEDIO	3
		[I.6]	Corte de suministro		0.1	0.5	BAJO	2
		[I.7]	Condiciones inadecuadas de temperatura o humedad		0.5	2.5	MEDIO	3
		[I.9]	Interrupción de otros servicios y suministros esenciales		0.9	4.5	ALTO	4
		[E.1]	Errores de los usuarios		0.4	2	BAJO	2
		[E.23]	Errores de mantenimiento / actualización de equipos (hardware)		0.5	2.5	MEDIO	3
		[E.24]	Caída del sistema por agotamiento de recursos		1	5	ALTO	4
		[A.11]	Acceso no autorizado		0.025	0.125	BAJO	2
		[A.23]	Manipulación de los equipos		0.25	1.25	BAJO	2
		[A.25]	Robo		0.5	2.5	MEDIO	3
[gelc]	Grupo electrógeno	[I.1]	Fuego	5	1	5	ALTO	4
		[I.2]	Daños por agua		1	5	ALTO	4
		[I.4]	Contaminación electromagnética		0.05	0.25	BAJO	2
		[I.5]	Avería de origen físico o lógico		1	5	ALTO	4
		[I.6]	Corte de suministro		0.05	0.25	BAJO	2
		[I.9]	Interrupción de otros servicios y suministros esenciales		0.2	1	BAJO	2
		[E.1]	Errores de los usuarios		0.2	1.16667	BAJO	2
		[E.23]	Errores de mantenimiento / actualización de equipos (hardware)		0.6	3	MEDIO	3
		[E.24]	Caída del sistema por agotamiento de recursos		1	5	ALTO	4
		[A.25]	Robo		0.5	2.5	MEDIO	3
		[A.28]	Indisponibilidad del personal		0.3	1.5	BAJO	2
[cable]	Cableado							
[cab1]	Cableado de red	[I.1]	Fuego	5.5	0.7	3.85	ALTO	4
		[I.2]	Daños por agua		0.7	3.85	ALTO	4
		[I.4]	Contaminación electromagnética		0.1	0.55	BAJO	2
		[I.5]	Avería de origen físico o lógico		0.7	3.85	ALTO	4
		[E.23]	Errores de mantenimiento / actualización de equipos (hardware)		0.2	1.1	BAJO	2
		[A.7]	Uso no previsto		0.2	1.30167	BAJO	2
		[A.23]	Manipulación de los equipos		0.125	0.6875	BAJO	2
		[A.25]	Robo		0.05	0.275	BAJO	2
		[A.28]	Indisponibilidad del personal		0.05	0.275	BAJO	2
[cab2]	Fibra óptica	[I.1]	Fuego	5.5	0.7	3.85	ALTO	4
		[I.5]	Avería de origen físico o lógico		0.3	1.65	BAJO	2
		[E.7]	Deficiencias en la organización		0.1	0.55	BAJO	2
		[E.23]	Errores de mantenimiento / actualización de equipos (hardware)		0.2	1.1	BAJO	2
		[E.28]	Indisponibilidad del personal		0.05	0.275	BAJO	2
		[A.23]	Manipulación de los equipos		0.05	0.275	BAJO	2
[L] INSTALACIONES								
[site]	Data Center	[N.*]	Desastres naturales	5.5	1	5.5	ALTO	4
		[I.1]	Fuego		1	5.5	ALTO	4
		[I.2]	Daños por agua		0.05	0.275	BAJO	2
		[I.7]	Condiciones inadecuadas de temperatura o humedad		0.9	4.95	ALTO	4
		[I.9]	Interrupción de otros servicios y suministros esenciales		0.5	2.75	MEDIO	3
		[E.25]	Pérdida de equipos		0.125	0.6875	BAJO	2

		[A.11]	Acceso no autorizado		0.35	1.925	BAJO	2
		[A.26]	Ataque destructivo		0.9	4.95	ALTO	4
		[A.27]	Ocupación enemiga		0.75	4.125	ALTO	4
		[A.28]	Indisponibilidad del personal		0.8	4.4	ALTO	4
[P] PERSONAL								
[ueex]	Usuario externo	[I.8]	Fallo de servicios de comunicaciones	2.5	0.6	1.5	BAJO	2
		[E.1]	Errores de los usuarios		0.3	0.66667	BAJO	2
		[E.18]	Destrucción de la información		0.2	0.5	BAJO	2
		[E.19]	Fugas de información		0.2	0.5	BAJO	2
		[E.20]	Vulnerabilidades de los programas (software)		0.2	0.5	BAJO	2
		[E.24]	Caída del sistema por agotamiento de recursos		0.4	1	BAJO	2
		[E.25]	Pérdida de equipos		0.075	0.1875	BAJO	2
		[A.6]	Abuso de privilegios de acceso		0.15	0.375	BAJO	2
		[A.7]	Uso no previsto		0.12	0.29167	BAJO	2
		[A.15]	Modificación deliberada de la información		0.2	0.5	BAJO	2
		[A.18]	Destrucción de información		0.5	1.25	BAJO	2
		[A.25]	Robo		0.5	1.25	BAJO	2
		[A.29]	Extorsión		0.6	1.5	BAJO	2
[uex1]	Personal de TI	[I.4]	Contaminación electromagnética	2.5	0.5	1.25	BAJO	2
		[I.7]	Condiciones inadecuadas de temperatura o humedad		0.5	1.25	BAJO	2
		[E.1]	Errores de los usuarios		0.1	0.25	BAJO	2
		[E.7]	Deficiencias en la organización		0.5	1.25	BAJO	2
		[A.19]	Divulgación de información		0.2	0.5	BAJO	2
		[A.29]	Extorsión		0.05	0.125	BAJO	2
		[A.30]	Ingeniería social		0.2	0.5	BAJO	2
[adm1]	Administrador del data center	[I.4]	Contaminación electromagnética	5.5	0.5	2.75	MEDIO	3
		[I.7]	Condiciones inadecuadas de temperatura o humedad		0.5	2.75	MEDIO	3
		[I.11]	Emanaciones electromagnética		0.3	1.65	BAJO	2
		[E.28]	Indisponibilidad del personal		0.9	4.95	ALTO	4
		[A.28]	Indisponibilidad del personal		0.2	1.1	BAJO	2

Fuente: Elaborada por los autores en base a MAGERIT- V 3.0 - Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro II

5.1.7. Determinación de Probabilidad de la amenaza

Se utilizó la tabla Probabilidad de Amenaza en los activos de TI de la Unidad de Red Telemática – UNPRG, en la cual se obtuvo que el 33% de las amenazas serían muy poco frecuente de que ocurrieran, 27% de las amenazas identificadas serían poco frecuentes de que ocurran, 29 % recibieron la probabilidad de que ocurran de manera normal, 9% con probabilidad de ocurrencia frecuente y 2% con probabilidad de ocurrencia de muy frecuente.

Tabla 40: Probabilidad de Amenaza en los activos de TI de la Unidad de Red Telemática - UNPRG

PROBABILIDAD DE AMENAZA					
ACTIVO		AMENAZA		VALORACIÓN DE LA PROBABILIDAD	
CÓDIGO	NOMBRE	CÓDIGO	NOMBRE	NIVEL	ESCALA CUALITATIVA
[S] SERVICIOS					
[sges]	Gestión de Actas virtuales y matricula online	[I.6]	Corte de suministro	3	Normal
		[I.8]	Fallo de servicios de comunicaciones	3	Normal
		[I.9]	Interrupción de otros servicios y suministros esenciales	5	Muy Frecuente
		[E.1]	Errores de los usuarios	2	Poco Frecuente
		[E.20]	Vulnerabilidades de los programas (software)	2	Poco Frecuente
		[E.24]	Caída del sistema por agotamiento de recursos	4	Frecuente
		[A.24]	Denegación del servicio	2	Poco Frecuente
[sgeo]	Gestión de Actas virtuales OCCA	[I.8]	Fallo de servicios de comunicaciones	3	Normal
		[I.9]	Interrupción de otros servicios y suministros esenciales	4	Frecuente
		[E.1]	Errores de los usuarios	5	Muy Frecuente
		[E.20]	Vulnerabilidades de los programas (software)	2	Poco Frecuente
		[A.5]	Suplantación de la identidad del usuario	2	Poco Frecuente
		[A.24]	Denegación del servicio	3	Normal
[SW] APLICACIONES					
[HW] EQUIPOS INFORMÁTICOS					
[serv]	Servidores				
[ser1]	Servidor de dominio	[N.1]	Fuego	1	Muy Poco Frecuente
		[I.5]	Avería de origen físico o lógico	2	Poco Frecuente
		[I.6]	Corte de suministro	4	Frecuente
		[I.7]	Condiciones inadecuadas de temperatura o humedad	3	Normal
		[I.8]	Fallo de servicios de comunicaciones	3	Normal
		[I.9]	Interrupción de otros servicios y suministros esenciales	4	Frecuente
		[I.10]	Degradación de los soportes de almacenamiento de la información	2	Poco Frecuente
		[E.9]	Errores de re-encaminamiento	1	Muy Poco Frecuente
		[E.20]	Vulnerabilidades de los programas (software)	2	Poco Frecuente
		[E.21]	Errores de mantenimiento / actualización de programas (software)	2	Poco Frecuente
		[E.23]	Errores de mantenimiento / actualización de equipos (hardware)	2	Poco Frecuente
		[E.24]	Caída del sistema por agotamiento de recursos	2	Poco Frecuente
		[A.4]	Manipulación de la configuración	1	Muy Poco Frecuente
		[A.24]	Denegación del servicio	2	Poco Frecuente

[ser2]	Servidor de proxy	[I.1]	Fuego	1	Muy Poco Frecuente
		[I.5]	Avería de origen físico o lógico	2	Poco Frecuente
		[I.6]	Corte de suministro	3	Normal
		[I.7]	Condiciones inadecuadas de temperatura o humedad	3	Normal
		[I.8]	Fallo de servicios de comunicaciones	4	Frecuente
		[I.9]	Interrupción de otros servicios y suministros esenciales	5	Muy Frecuente
		[I.10]	Degradación de los soportes de almacenamiento de la información	2	Poco Frecuente
		[E.2]	Errores del administrador	1	Muy Poco Frecuente
		[E.4]	Errores de configuración	1	Muy Poco Frecuente
		[E.20]	Vulnerabilidades de los programas (software)	1	Muy Poco Frecuente
		[E.21]	Errores de mantenimiento / actualización de programas (software)	1	Muy Poco Frecuente
		[E.23]	Errores de mantenimiento / actualización de equipos (hardware)	2	Poco Frecuente
		[E.24]	Caída del sistema por agotamiento de recursos	2	Poco Frecuente
		[E.28]	Indisponibilidad del personal	1	Muy Poco Frecuente
		[A.24]	Denegación del servicio	3	Normal
[ser3]	Servidor de base de datos	[I.1]	Fuego	1	Muy Poco Frecuente
		[I.5]	Avería de origen físico o lógico	1	Muy Poco Frecuente
		[I.6]	Corte de suministro	3	Normal
		[I.7]	Condiciones inadecuadas de temperatura o humedad	3	Normal
		[I.8]	Fallo de servicios de comunicaciones	3	Normal
		[I.9]	Interrupción de otros servicios y suministros esenciales	4	Frecuente
		[I.10]	Degradación de los soportes de almacenamiento de la información	2	Poco Frecuente
		[E.2]	Errores del administrador	2	Poco Frecuente
		[E.14]	Escapes de información	2	Poco Frecuente
		[E.15]	Alteración accidental de la información	1	Muy Poco Frecuente
		[E.20]	Vulnerabilidades de los programas (software)	2	Poco Frecuente
		[E.21]	Errores de mantenimiento / actualización de programas (software)	1	Muy Poco Frecuente
		[E.23]	Errores de mantenimiento / actualización de equipos (hardware)	1	Muy Poco Frecuente
		[E.24]	Caída del sistema por agotamiento de recursos	4	Frecuente
		[A.15]	Modificación deliberada de la información	1	Muy Poco Frecuente
		[A.24]	Denegación del servicio	2	Poco Frecuente

		[A.28]	Indisponibilidad del personal	3	Normal
[ser4]	Servidor de base de datos - backup	[I.1]	Fuego	1	Muy Poco Frecuente
		[I.6]	Corte de suministro	4	Frecuente
		[I.7]	Condiciones inadecuadas de temperatura o humedad	3	Normal
		[I.8]	Fallo de servicios de comunicaciones	3	Normal
		[I.9]	Interrupción de otros servicios y suministros esenciales	4	Frecuente
		[I.10]	Degradación de los soportes de almacenamiento de la información	1	Muy Poco Frecuente
		[E.2]	Errores del administrador	1	Muy Poco Frecuente
		[E.14]	Escapes de información	1	Muy Poco Frecuente
		[E.15]	Alteración accidental de la información	1	Muy Poco Frecuente
		[E.18]	Destrucción de la información	1	Muy Poco Frecuente
		[E.20]	Vulnerabilidades de los programas (software)	2	Poco Frecuente
		[E.21]	Errores de mantenimiento / actualización de programas (software)	2	Poco Frecuente
		[E.23]	Errores de mantenimiento / actualización de equipos (hardware)	2	Poco Frecuente
		[E.24]	Caída del sistema por agotamiento de recursos	1	Muy Poco Frecuente
		[E.28]	Indisponibilidad del personal	1	Muy Poco Frecuente
		[A.15]	Modificación deliberada de la información	1	Muy Poco Frecuente
		[A.18]	Destrucción de información	1	Muy Poco Frecuente
		[A.24]	Denegación del servicio	2	Poco Frecuente
		[A.28]	Indisponibilidad del personal	2	Poco Frecuente
[ser5]	Servidor web	[I.1]	Fuego	1	Muy Poco Frecuente
		[I.5]	Avería de origen físico o lógico	1	Muy Poco Frecuente
		[I.6]	Corte de suministro	1	Muy Poco Frecuente
		[I.7]	Condiciones inadecuadas de temperatura o humedad	3	Normal
		[I.8]	Fallo de servicios de comunicaciones	3	Normal
		[I.9]	Interrupción de otros servicios y suministros esenciales	3	Normal
		[I.10]	Degradación de los soportes de almacenamiento de la información	1	Muy Poco Frecuente
		[E.14]	Escapes de información	2	Poco Frecuente
		[E.15]	Alteración accidental de la información	1	Muy Poco Frecuente

		[E.20]	Vulnerabilidades de los programas (software)	1	Muy Poco Frecuente
		[E.21]	Errores de mantenimiento / actualización de programas (software)	2	Poco Frecuente
		[E.23]	Errores de mantenimiento / actualización de equipos (hardware)	2	Poco Frecuente
		[E.24]	Caída del sistema por agotamiento de recursos	3	Normal
		[A.24]	Denegación del servicio	2	Poco Frecuente
[ser6]	Servidor de archivos	[I.1]	Fuego	1	Muy Poco Frecuente
		[I.5]	Avería de origen físico o lógico	1	Muy Poco Frecuente
		[I.6]	Corte de suministro	4	Frecuente
		[I.7]	Condiciones inadecuadas de temperatura o humedad	3	Normal
		[I.8]	Fallo de servicios de comunicaciones	3	Normal
		[I.9]	Interrupción de otros servicios y suministros esenciales	3	Normal
		[I.10]	Degradación de los soportes de almacenamiento de la información	1	Muy Poco Frecuente
		[E.1]	Errores de los usuarios	3	Normal
		[E.14]	Escapes de información	3	Normal
		[E.20]	Vulnerabilidades de los programas (software)	1	Muy Poco Frecuente
		[E.21]	Errores de mantenimiento / actualización de programas (software)	1	Muy Poco Frecuente
		[E.23]	Errores de mantenimiento / actualización de equipos (hardware)	1	Muy Poco Frecuente
		[E.24]	Caída del sistema por agotamiento de recursos	4	Frecuente
		[A.5]	Suplantación de la identidad del usuario	2	Poco Frecuente
		[A.24]	Denegación del servicio	3	Normal
[ser7]	Servidor de datos - OCCA	[I.1]	Fuego	1	Muy Poco Frecuente
		[I.5]	Avería de origen físico o lógico	1	Muy Poco Frecuente
		[I.6]	Corte de suministro	4	Frecuente
		[I.7]	Condiciones inadecuadas de temperatura o humedad	3	Normal
		[I.8]	Fallo de servicios de comunicaciones	3	Normal
		[I.9]	Interrupción de otros servicios y suministros esenciales	3	Normal
		[I.10]	Degradación de los soportes de almacenamiento de la información	2	Poco Frecuente
		[E.20]	Vulnerabilidades de los programas (software)	2	Poco Frecuente
		[E.21]	Errores de mantenimiento / actualización de programas (software)	1	Muy Poco Frecuente
		[E.23]	Errores de mantenimiento / actualización de equipos (hardware)	1	Muy Poco Frecuente
		[E.24]	Caída del sistema por agotamiento de recursos	1	Muy Poco Frecuente

		[A.24]	Denegación del servicio	1	Muy Poco Frecuente
[ser8]	Servidor de base de datos - backup-OCCA	[I.1]	Fuego	1	Muy Poco Frecuente
		[I.5]	Avería de origen físico o lógico	2	Poco Frecuente
		[I.6]	Corte de suministro	3	Normal
		[I.7]	Condiciones inadecuadas de temperatura o humedad	3	Normal
		[I.8]	Fallo de servicios de comunicaciones	3	Normal
		[I.9]	Interrupción de otros servicios y suministros esenciales	3	Normal
		[I.10]	Degradación de los soportes de almacenamiento de la información	2	Poco Frecuente
		[E.2]	Errores del administrador	1	Muy Poco Frecuente
		[E.20]	Vulnerabilidades de los programas (software)	1	Muy Poco Frecuente
		[E.21]	Errores de mantenimiento / actualización de programas (software)	1	Muy Poco Frecuente
		[E.23]	Errores de mantenimiento / actualización de equipos (hardware)	1	Muy Poco Frecuente
		[E.24]	Caída del sistema por agotamiento de recursos	3	Normal
		[A.6]	Abuso de privilegios de acceso	1	Muy Poco Frecuente
		[A.24]	Denegación del servicio	3	Normal
[netw]	Soporte de red				
[swit]	Switch	[I.1]	Fuego	1	Muy Poco Frecuente
		[I.5]	Avería de origen físico o lógico	2	Poco Frecuente
		[I.6]	Corte de suministro	3	Normal
		[I.7]	Condiciones inadecuadas de temperatura o humedad	3	Normal
		[I.8]	Fallo de servicios de comunicaciones	3	Normal
		[I.9]	Interrupción de otros servicios y suministros esenciales	4	Frecuente
		[E.1]	Errores de los usuarios	1	Muy Poco Frecuente
		[E.2]	Errores del administrador	1	Muy Poco Frecuente
		[E.9]	Errores de re-encaminamiento	1	Muy Poco Frecuente
		[E.23]	Errores de mantenimiento / actualización de equipos (hardware)	3	Normal
		[E.24]	Caída del sistema por agotamiento de recursos	3	Normal
		[A.24]	Denegación del servicio	2	Poco Frecuente
[rout]	Router	[I.1]	Fuego	1	Muy Poco Frecuente
		[I.5]	Avería de origen físico o lógico	2	Poco Frecuente
		[I.6]	Corte de suministro	4	Frecuente

		[I.7]	Condiciones inadecuadas de temperatura o humedad	3	Normal
		[I.8]	Fallo de servicios de comunicaciones	3	Normal
		[I.9]	Interrupción de otros servicios y suministros esenciales	3	Normal
		[E.2]	Errores del administrador	1	Muy Poco Frecuente
		[E.9]	Errores de re-encaminamiento	1	Muy Poco Frecuente
		[E.23]	Errores de mantenimiento / actualización de equipos (hardware)	2	Poco Frecuente
		[E.24]	Caída del sistema por agotamiento de recursos	4	Frecuente
		[A.24]	Denegación del servicio	2	Poco Frecuente
[fire]	Firewall	[I.1]	Fuego	1	Muy Poco Frecuente
		[I.5]	Avería de origen físico o lógico	2	Poco Frecuente
		[I.6]	Corte de suministro	4	Frecuente
		[I.7]	Condiciones inadecuadas de temperatura o humedad	3	Normal
		[I.8]	Fallo de servicios de comunicaciones	3	Normal
		[I.9]	Interrupción de otros servicios y suministros esenciales	3	Normal
		[I.10]	Degradación de los soportes de almacenamiento de la información	3	Normal
		[E.20]	Vulnerabilidades de los programas (software)	5	Muy Frecuente
		[E.21]	Errores de mantenimiento / actualización de programas (software)	3	Normal
		[E.23]	Errores de mantenimiento / actualización de equipos (hardware)	3	Normal
		[E.24]	Caída del sistema por agotamiento de recursos	5	Muy Frecuente
		[A.4]	Manipulación de la configuración	1	Muy Poco Frecuente
		[A.24]	Denegación del servicio	2	Poco Frecuente
[COM] REDES DE COMUNICACIONES					
[cint]	Internet	[I.1]	Fuego	1	Muy Poco Frecuente
		[I.5]	Avería de origen físico o lógico	4	Frecuente
		[I.6]	Corte de suministro	3	Normal
		[I.7]	Condiciones inadecuadas de temperatura o humedad	3	Normal
		[I.8]	Fallo de servicios de comunicaciones	3	Normal
		[I.9]	Interrupción de otros servicios y suministros esenciales	3	Normal
		[E.4]	Errores de configuración	1	Muy Poco Frecuente
		[E.9]	Errores de re-encaminamiento	1	Muy Poco Frecuente
		[E.24]	Caída del sistema por agotamiento de recursos	1	Muy Poco Frecuente
		[A.24]	Denegación del servicio	1	Muy Poco Frecuente

[cwfi]	Red Inalámbrica	[I.6]	Corte de suministro	5	Muy Frecuente
		[I.7]	Condiciones inadecuadas de temperatura o humedad	3	Normal
		[I.8]	Fallo de servicios de comunicaciones	3	Normal
		[I.9]	Interrupción de otros servicios y suministros esenciales	3	Normal
		[E.23]	Errores de mantenimiento / actualización de equipos (hardware)	3	Normal
		[E.25]	Pérdida de equipos	2	Poco Frecuente
		[A.24]	Denegación del servicio	2	Poco Frecuente
[MEDIA] SOPORTE DE INFORMACIÓN					
[elect]	Electrónicos				
[ele1]	Cintas Magnéticas	[I.1]	Fuego	1	Muy Poco Frecuente
		[I.5]	Avería de origen físico o lógico	1	Muy Poco Frecuente
		[I.10]	Degradación de los soportes de almacenamiento de la información	1	Muy Poco Frecuente
		[A.25]	Robo	2	Poco Frecuente
[ele2]	Disco externo USB	[I.1]	Fuego	1	Muy Poco Frecuente
		[I.5]	Avería de origen físico o lógico	1	Muy Poco Frecuente
		[I.10]	Degradación de los soportes de almacenamiento de la información	1	Muy Poco Frecuente
		[E.1]	Errores de los usuarios	1	Muy Poco Frecuente
		[E.25]	Pérdida de equipos	1	Muy Poco Frecuente
[store]	Storage de respaldo de BD	[I.1]	Fuego	1	Muy Poco Frecuente
		[I.5]	Avería de origen físico o lógico	2	Poco Frecuente
		[I.9]	Interrupción de otros servicios y suministros esenciales	3	Normal
		[I.10]	Degradación de los soportes de almacenamiento de la información	2	Poco Frecuente
		[E.23]	Errores de mantenimiento / actualización de equipos (hardware)	2	Poco Frecuente
		[A.24]	Denegación del servicio	3	Normal
[noel]	No electrónico				
[mimp]	Material impreso	[I.1]	Fuego	1	Muy Poco Frecuente
		[E.7]	Deficiencias en la organización	3	Normal
		[E.14]	Escapes de información	2	Poco Frecuente
		[E.19]	Fugas de información	2	Poco Frecuente
		[A.19]	Divulgación de información	2	Poco Frecuente
		[A.25]	Robo	1	Muy Poco Frecuente

[AUX] EQUIPAMIENTO AUXILIAR					
[powr]	Acumulador de energía UPS	[I.1]	Fuego	1	Muy Poco Frecuente
		[I.5]	Avería de origen físico o lógico	3	Normal
		[I.6]	Corte de suministro	4	Frecuente
		[I.7]	Condiciones inadecuadas de temperatura o humedad	3	Normal
		[I.8]	Fallo de servicios de comunicaciones	3	Normal
		[I.9]	Interrupción de otros servicios y suministros esenciales	3	Normal
		[E.1]	Errores de los usuarios	2	Poco Frecuente
		[E.23]	Errores de mantenimiento / actualización de equipos (hardware)	2	Poco Frecuente
		[E.24]	Caída del sistema por agotamiento de recursos	3	Normal
[psis]	Sistema de aire acondicionado	[I.1]	Fuego	1	Muy Poco Frecuente
		[I.2]	Daños por agua	2	Poco Frecuente
		[I.*]	Desastres industriales	1	Muy Poco Frecuente
		[I.3]	Contaminación mecánica	2	Poco Frecuente
		[I.4]	Contaminación electromagnética	3	Normal
		[I.5]	Avería de origen físico o lógico	3	Normal
		[I.6]	Corte de suministro	3	Normal
		[I.7]	Condiciones inadecuadas de temperatura o humedad	3	Normal
		[I.9]	Interrupción de otros servicios y suministros esenciales	3	Normal
		[E.1]	Errores de los usuarios	2	Poco Frecuente
		[E.23]	Errores de mantenimiento / actualización de equipos (hardware)	2	Poco Frecuente
		[E.24]	Caída del sistema por agotamiento de recursos	4	Frecuente
		[A.11]	Acceso no autorizado	2	Poco Frecuente
		[A.23]	Manipulación de los equipos	1	Muy Poco Frecuente
		[A.25]	Robo	1	Muy Poco Frecuente
[gelc]	Grupo electrógeno	[I.1]	Fuego	1	Muy Poco Frecuente
		[I.2]	Daños por agua	2	Poco Frecuente
		[I.4]	Contaminación electromagnética	3	Normal
		[I.5]	Avería de origen físico o lógico	2	Poco Frecuente
		[I.6]	Corte de suministro	5	Muy Frecuente
		[I.9]	Interrupción de otros servicios y suministros esenciales	3	Normal
		[E.1]	Errores de los usuarios	2	Poco Frecuente
		[E.23]	Errores de mantenimiento / actualización de equipos (hardware)	2	Poco Frecuente
		[E.24]	Caída del sistema por agotamiento de recursos	3	Normal

		[A.25]	Robo	2	Poco Frecuente
		[A.28]	Indisponibilidad del personal	2	Poco Frecuente
[cable]	Cableado				
[cab1]	Cableado de red	[I.1]	Fuego	1	Muy Poco Frecuente
		[I.2]	Daños por agua	1	Muy Poco Frecuente
		[I.4]	Contaminación electromagnética	3	Normal
		[I.5]	Avería de origen físico o lógico	4	Frecuente
		[E.23]	Errores de mantenimiento / actualización de equipos (hardware)	3	Normal
		[A.7]	Uso no previsto	2	Poco Frecuente
		[A.23]	Manipulación de los equipos	3	Normal
		[A.25]	Robo	4	Frecuente
		[A.28]	Indisponibilidad del personal	1	Muy Poco Frecuente
[cab2]	Fibra óptica	[I.1]	Fuego	1	Muy Poco Frecuente
		[I.5]	Avería de origen físico o lógico	3	Normal
		[E.7]	Deficiencias en la organización	3	Normal
		[E.23]	Errores de mantenimiento / actualización de equipos (hardware)	2	Poco Frecuente
		[E.28]	Indisponibilidad del personal	1	Muy Poco Frecuente
		[A.23]	Manipulación de los equipos	3	Normal
[L] INSTALACIONES					
[site]	Data Center	[N.*]	Desastres naturales	1	Muy Poco Frecuente
		[I.1]	Fuego	1	Muy Poco Frecuente
		[I.2]	Daños por agua	1	Muy Poco Frecuente
		[I.7]	Condiciones inadecuadas de temperatura o humedad	3	Normal
		[I.9]	Interrupción de otros servicios y suministros esenciales	2	Poco Frecuente
		[E.25]	Pérdida de equipos	1	Muy Poco Frecuente
		[A.11]	Acceso no autorizado	1	Muy Poco Frecuente
		[A.26]	Ataque destructivo	1	Muy Poco Frecuente
		[A.27]	Ocupación enemiga	1	Muy Poco Frecuente
		[A.28]	Indisponibilidad del personal	1	Muy Poco Frecuente
[P] PERSONAL					
[ueex]	Usuario externo	[I.8]	Fallo de servicios de comunicaciones	2	Poco Frecuente

		[E.1]	Errores de los usuarios	2	Poco Frecuente
		[E.18]	Destrucción de la información	3	Normal
		[E.19]	Fugas de información	2	Poco Frecuente
		[E.20]	Vulnerabilidades de los programas (software)	3	Normal
		[E.24]	Caída del sistema por agotamiento de recursos	3	Normal
		[E.25]	Pérdida de equipos	1	Muy Poco Frecuente
		[A.6]	Abuso de privilegios de acceso	2	Poco Frecuente
		[A.7]	Uso no previsto	2	Poco Frecuente
		[A.15]	Modificación deliberada de la información	1	Muy Poco Frecuente
		[A.18]	Destrucción de información	1	Muy Poco Frecuente
		[A.25]	Robo	2	Poco Frecuente
		[A.29]	Extorsión	2	Poco Frecuente
[uex1]	Personal de TI	[I.4]	Contaminación electromagnética	4	Frecuente
		[I.7]	Condiciones inadecuadas de temperatura o humedad	4	Frecuente
		[E.1]	Errores de los usuarios	3	Normal
		[E.7]	Deficiencias en la organización	3	Normal
		[A.19]	Divulgación de información	2	Poco Frecuente
		[A.29]	Extorsión	2	Poco Frecuente
		[A.30]	Ingeniería social	2	Poco Frecuente
[adm1]	Administrador del data center	[I.4]	Contaminación electromagnética	4	Frecuente
		[I.7]	Condiciones inadecuadas de temperatura o humedad	4	Frecuente
		[I.11]	Emanaciones electromagnética	4	Frecuente
		[E.28]	Indisponibilidad del personal	2	Poco Frecuente
		[A.28]	Indisponibilidad del personal	2	Poco Frecuente

Fuente: Elaborada por los autores en base a MAGERIT- V 3.0 - Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro II

5.1.1. Estimación del Riesgo

La amenaza interrupción de otros servicios y suministros esenciales identificada en el activo [sges] recibe un nivel importante de riesgo. Interrupción de otros servicios y suministros esenciales, caída del sistema por agotamiento de recursos, denegación del servicio del activo [swsc] reciben un nivel de riesgo importante. Caída del sistema por agotamiento de recursos del activo [swoc] representa un nivel de riesgo crítico. Caída del sistema por agotamiento de recursos e indisponibilidad del personal del activo [ser3] representa un nivel de riesgo importante. Las amenazas de fuego e interrupción de otros servicios y suministros esenciales del activo [ser4] reciben un nivel de riesgo importante. La amenazas

vulnerabilidades de los programas de activo [fire] representa un nivel de riesgo importante. La amenazas avería de origen físico o lógico identificada del activo [cinf] representa un nivel importante de riesgo. El activo [store] cuya amenazas identificada interrupción de otros servicios y suministros esenciales representa un nivel importante de nivel de riesgo. Las amenazas de avería de origen físico o lógico y caída del sistema por agotamiento de recursos del activo [powr] representan un nivel de riesgo importante en el activo. El activo [psis] cuyas amenazas identificas como interrupción de otros servicios y suministros esenciales representa un nivel de riesgo importante. Y la amenaza caída del sistema por agotamiento de recursos representa un nivel de riesgo muy crítico de riesgo. La amenaza identificada en el activo [gelc] caída del sistema por agotamiento de recursos representa un nivel de riesgo importante. La amenaza avería de origen físico o lógico identificada en el activo [cab1] representa un nivel crítico en el activo. El activo [site] una de las amenazad identificadas como Condiciones inadecuadas de temperatura o humedad representa un nivel importante en el nivel de riesgo. Las amenazas contaminación electromagnética y condiciones inadecuadas de temperatura o humedad representan un nivel de riesgo importante de riesgo en el activo [adm1].

Tabla 41: Estimación del riesgo

ACTIVO		AMENAZA		IMPACTO	PROBABILIDAD	CÓDIGO RIESGO	RIESGO	NIVEL	ESCALA
CÓDIGO	NOMBRE	CÓDIGO	NOMBRE						
[S] SERVICIOS									
[sges]	Gestión de Actas virtuales y matricula online	[I.6]	Corte de suministro	3	3	R1	9	3	Apreciable
		[I.8]	Fallo de servicios de comunicaciones	2	3	R2	6	2	Bajo
		[I.9]	Interrupción de otros servicios y suministros esenciales	3	5	R3	15	4	Importante
		[E.1]	Errores de los usuarios	2	2	R4	4	1	Despreciable
		[E.20]	Vulnerabilidades de los programas (software)	2	2	R5	4	1	Despreciable
		[E.24]	Caída del sistema por agotamiento de recursos	2	4	R6	8	3	Apreciable
		[A.24]	Denegación del servicio	2	2	R7	4	1	Despreciable
[sgeo]	Gestión de Actas virtuales OCCA	[I.8]	Fallo de servicios de comunicaciones	2	3	R8	6	2	Bajo
		[I.9]	Interrupción de otros servicios y suministros esenciales	2	4	R9	8	3	Apreciable
		[E.1]	Errores de los usuarios	2	5	R10	10	3	Apreciable
		[E.20]	Vulnerabilidades de los programas (software)	2	2	R11	4	1	Despreciable
		[A.5]	Suplantación de la identidad del usuario	2	2	R12	4	1	Despreciable
		[A.24]	Denegación del servicio	2	3	R13	6	2	Bajo
[SW] APLICACIONES									
[HW] EQUIPOS INFORMÁTICOS									
[serv]	Servidores								
[ser1]	Servidor de dominio	[N.1]	Fuego	4	1	R34	4	1	Despreciable
		[I.5]	Avería de origen físico o lógico	2	2	R35	4	1	Despreciable
		[I.6]	Corte de suministro	2	4	R36	8	3	Apreciable
		[I.7]	Condiciones inadecuadas de temperatura o humedad	2	3	R37	6	2	Bajo
		[I.8]	Fallo de servicios de comunicaciones	2	3	R38	6	2	Bajo
		[I.9]	Interrupción de otros servicios y suministros esenciales	2	4	R39	8	3	Apreciable
		[I.10]	Degradación de los soportes de almacenamiento de la información	2	2	R40	4	1	Despreciable
		[E.9]	Errores de re-encaminamiento	2	1	R41	2	1	Despreciable
		[E.20]	Vulnerabilidades de los programas (software)	4	2	R42	8	3	Apreciable
		[E.21]	Errores de mantenimiento / actualización de programas (software)	2	2	R43	4	1	Despreciable
		[E.23]	Errores de mantenimiento / actualización de equipos (hardware)	2	2	R44	4	1	Despreciable
		[E.24]	Caída del sistema por agotamiento de recursos	3	2	R45	6	2	Bajo
		[A.4]	Manipulación de la configuración	2	1	R46	2	1	Despreciable
		[A.24]	Denegación del servicio	4	2	R47	8	3	Apreciable

[ser2]	Servidor de proxy	[I.1]	Fuego	2	1	R48	2	1	Despreciable
		[I.5]	Avería de origen físico o lógico	2	2	R49	4	1	Despreciable
		[I.6]	Corte de suministro	2	3	R50	6	2	Bajo
		[I.7]	Condiciones inadecuadas de temperatura o humedad	2	3	R51	6	2	Bajo
		[I.8]	Fallo de servicios de comunicaciones	2	4	R52	8	3	Apreciable
		[I.9]	Interrupción de otros servicios y suministros esenciales	2	5	R53	10	3	Apreciable
		[I.10]	Degradación de los soportes de almacenamiento de la información	2	2	R54	4	1	Despreciable
		[E.2]	Errores del administrador	2	1	R55	2	1	Despreciable
		[E.4]	Errores de configuración	2	1	R56	2	1	Despreciable
		[E.20]	Vulnerabilidades de los programas (software)	2	1	R57	2	1	Despreciable
		[E.21]	Errores de mantenimiento / actualización de programas (software)	2	1	R58	2	1	Despreciable
		[E.23]	Errores de mantenimiento / actualización de equipos (hardware)	2	2	R59	4	1	Despreciable
		[E.24]	Caída del sistema por agotamiento de recursos	2	2	R60	4	1	Despreciable
		[E.28]	Indisponibilidad del personal	2	1	R61	2	1	Despreciable
		[A.24]	Denegación del servicio	2	3	R62	6	2	Bajo
[ser3]	Servidor de base de datos	[I.1]	Fuego	4	1	R63	4	1	Despreciable
		[I.5]	Avería de origen físico o lógico	3	1	R64	3	1	Despreciable
		[I.6]	Corte de suministro	3	3	R65	9	3	Apreciable
		[I.7]	Condiciones inadecuadas de temperatura o humedad	3	3	R66	9	3	Apreciable
		[I.8]	Fallo de servicios de comunicaciones	3	3	R67	9	3	Apreciable
		[I.9]	Interrupción de otros servicios y suministros esenciales	2	4	R68	8	3	Apreciable
		[I.10]	Degradación de los soportes de almacenamiento de la información	2	2	R69	4	1	Despreciable
		[E.2]	Errores del administrador	2	2	R70	4	1	Despreciable
		[E.14]	Escapes de información	4	2	R71	8	3	Apreciable
		[E.15]	Alteración accidental de la información	3	1	R72	3	1	Despreciable
		[E.20]	Vulnerabilidades de los programas (software)	2	2	R73	4	1	Despreciable
		[E.21]	Errores de mantenimiento / actualización de programas (software)	2	1	R74	2	1	Despreciable
		[E.23]	Errores de mantenimiento / actualización de equipos (hardware)	2	1	R75	2	1	Despreciable
		[E.24]	Caída del sistema por agotamiento de recursos	3	4	R76	12	4	Importante
		[A.15]	Modificación deliberada de la información	2	1	R77	2	1	Despreciable
		[A.24]	Denegación del servicio	3	2	R78	6	2	Bajo
		[A.28]	Indisponibilidad del personal	4	3	R79	12	4	Importante
[ser4]	Servidor de base de datos - backup	[I.1]	Fuego	2	1	R80	2	1	Despreciable
		[I.6]	Corte de suministro	3	4	R81	12	4	Importante
		[I.7]	Condiciones inadecuadas de temperatura o humedad	3	3	R82	9	3	Apreciable
		[I.8]	Fallo de servicios de comunicaciones	3	3	R83	9	3	Apreciable
		[I.9]	Interrupción de otros servicios y suministros esenciales	3	4	R84	12	4	Importante
		[I.10]	Degradación de los soportes de almacenamiento de la información	3	1	R85	3	1	Despreciable

		[E.2]	Errores del administrador	2	1	R86	2	1	Despreciable
		[E.14]	Escapes de información	4	1	R87	4	1	Despreciable
		[E.15]	Alteración accidental de la información	3	1	R88	3	1	Despreciable
		[E.18]	Destrucción de la información	3	1	R89	3	1	Despreciable
		[E.20]	Vulnerabilidades de los programas (software)	2	2	R90	4	1	Despreciable
		[E.21]	Errores de mantenimiento / actualización de programas (software)	2	2	R91	4	1	Despreciable
		[E.23]	Errores de mantenimiento / actualización de equipos (hardware)	3	2	R92	6	2	Bajo
		[E.24]	Caída del sistema por agotamiento de recursos	3	1	R93	3	1	Despreciable
		[E.28]	Indisponibilidad del personal	2	1	R94	2	1	Despreciable
		[A.15]	Modificación deliberada de la información	3	1	R95	3	1	Despreciable
		[A.18]	Destrucción de información	3	1	R96	3	1	Despreciable
		[A.24]	Denegación del servicio	3	2	R97	6	2	Bajo
		[A.28]	Indisponibilidad del personal	2	2	R98	4	1	Despreciable
[ser5]	Servidor web	[I.1]	Fuego	2	1	R99	2	1	Despreciable
		[I.5]	Avería de origen físico o lógico	2	1	R100	2	1	Despreciable
		[I.6]	Corte de suministro	2	1	R101	2	1	Despreciable
		[I.7]	Condiciones inadecuadas de temperatura o humedad	3	3	R102	9	3	Apreciable
		[I.8]	Fallo de servicios de comunicaciones	3	3	R103	9	3	Apreciable
		[I.9]	Interrupción de otros servicios y suministros esenciales	2	3	R104	6	2	Bajo
		[I.10]	Degradación de los soportes de almacenamiento de la información	2	1	R105	2	1	Despreciable
		[E.14]	Escapes de información	2	2	R106	4	1	Despreciable
		[E.15]	Alteración accidental de la información	2	1	R107	2	1	Despreciable
		[E.20]	Vulnerabilidades de los programas (software)	2	1	R108	2	1	Despreciable
		[E.21]	Errores de mantenimiento / actualización de programas (software)	2	2	R109	4	1	Despreciable
		[E.23]	Errores de mantenimiento / actualización de equipos (hardware)	2	2	R110	4	1	Despreciable
		[E.24]	Caída del sistema por agotamiento de recursos	3	3	R111	9	3	Apreciable
		[A.24]	Denegación del servicio	3	2	R112	6	2	Bajo
[ser6]	Servidor de archivos	[I.1]	Fuego	2	1	R113	2	1	Despreciable
		[I.5]	Avería de origen físico o lógico	2	1	R114	2	1	Despreciable
		[I.6]	Corte de suministro	2	4	R115	8	3	Apreciable
		[I.7]	Condiciones inadecuadas de temperatura o humedad	2	3	R116	6	2	Bajo
		[I.8]	Fallo de servicios de comunicaciones	2	3	R117	6	2	Bajo
		[I.9]	Interrupción de otros servicios y suministros esenciales	2	3	R118	6	2	Bajo
		[I.10]	Degradación de los soportes de almacenamiento de la información	2	1	R119	2	1	Despreciable
		[E.1]	Errores de los usuarios	2	3	R120	6	2	Bajo
		[E.14]	Escapes de información	2	3	R121	6	2	Bajo
		[E.20]	Vulnerabilidades de los programas (software)	2	1	R122	2	1	Despreciable
		[E.21]	Errores de mantenimiento / actualización de programas (software)	2	1	R123	2	1	Despreciable

		[E.23]	Errores de mantenimiento / actualización de equipos (hardware)	2	1	R124	2	1	Despreciable
		[E.24]	Caída del sistema por agotamiento de recursos	2	4	R125	8	3	Apreciable
		[A.5]	Suplantación de la identidad del usuario	2	2	R126	4	1	Despreciable
		[A.24]	Denegación del servicio	2	3	R127	6	2	Bajo
[ser7]	Servidor de datos - OCCA	[I.1]	Fuego	2	1	R128	2	1	Despreciable
		[I.5]	Avería de origen físico o lógico	2	1	R129	2	1	Despreciable
		[I.6]	Corte de suministro	2	4	R130	8	3	Apreciable
		[I.7]	Condiciones inadecuadas de temperatura o humedad	3	3	R131	9	3	Apreciable
		[I.8]	Fallo de servicios de comunicaciones	3	3	R132	9	3	Apreciable
		[I.9]	Interrupción de otros servicios y suministros esenciales	2	3	R133	6	2	Bajo
		[I.10]	Degradación de los soportes de almacenamiento de la información	2	2	R134	4	1	Despreciable
		[E.20]	Vulnerabilidades de los programas (software)	2	2	R135	4	1	Despreciable
		[E.21]	Errores de mantenimiento / actualización de programas (software)	2	1	R136	2	1	Despreciable
		[E.23]	Errores de mantenimiento / actualización de equipos (hardware)	2	1	R137	2	1	Despreciable
		[E.24]	Caída del sistema por agotamiento de recursos	3	1	R138	3	1	Despreciable
		[A.24]	Denegación del servicio	3	1	R139	3	1	Despreciable
[ser8]	Servidor de base de datos - backup-OCCA	[I.1]	Fuego	3	1	R140	3	1	Despreciable
		[I.5]	Avería de origen físico o lógico	3	2	R141	6	2	Bajo
		[I.6]	Corte de suministro	2	3	R142	6	2	Bajo
		[I.7]	Condiciones inadecuadas de temperatura o humedad	3	3	R143	9	3	Apreciable
		[I.8]	Fallo de servicios de comunicaciones	3	3	R144	9	3	Apreciable
		[I.9]	Interrupción de otros servicios y suministros esenciales	3	3	R145	9	3	Apreciable
		[I.10]	Degradación de los soportes de almacenamiento de la información	3	2	R146	6	2	Bajo
		[E.2]	Errores del administrador	2	1	R147	2	1	Despreciable
		[E.20]	Vulnerabilidades de los programas (software)	2	1	R148	2	1	Despreciable
		[E.21]	Errores de mantenimiento / actualización de programas (software)	2	1	R149	2	1	Despreciable
		[E.23]	Errores de mantenimiento / actualización de equipos (hardware)	2	1	R150	2	1	Despreciable
		[E.24]	Caída del sistema por agotamiento de recursos	3	3	R151	9	3	Apreciable
		[A.6]	Abuso de privilegios de acceso	2	1	R152	2	1	Despreciable
		[A.24]	Denegación del servicio	3	3	R153	9	3	Apreciable
[netw]	Soporte de red								
[swit]	Switch	[I.1]	Fuego	2	1	R154	2	1	Despreciable
		[I.5]	Avería de origen físico o lógico	2	2	R155	4	1	Despreciable
		[I.6]	Corte de suministro	2	3	R156	6	2	Bajo
		[I.7]	Condiciones inadecuadas de temperatura o humedad	2	3	R157	6	2	Bajo
		[I.8]	Fallo de servicios de comunicaciones	2	3	R158	6	2	Bajo
		[I.9]	Interrupción de otros servicios y suministros esenciales	2	4	R159	8	3	Apreciable
		[E.1]	Errores de los usuarios	2	1	R160	2	1	Despreciable

		[E.2]	Errores del administrador	2	1	R161	2	1	Despreciable
		[E.9]	Errores de re-encaminamiento	2	1	R162	2	1	Despreciable
		[E.23]	Errores de mantenimiento / actualización de equipos (hardware)	2	3	R163	6	2	Bajo
		[E.24]	Caída del sistema por agotamiento de recursos	2	3	R164	6	2	Bajo
		[A.24]	Denegación del servicio	2	2	R165	4	1	Despreciable
[rout]	Router	[I.1]	Fuego	2	1	R166	2	1	Despreciable
		[I.5]	Avería de origen físico o lógico	2	2	R167	4	1	Despreciable
		[I.6]	Corte de suministro	2	4	R168	8	3	Apreciable
		[I.7]	Condiciones inadecuadas de temperatura o humedad	2	3	R169	6	2	Bajo
		[I.8]	Fallo de servicios de comunicaciones	2	3	R170	6	2	Bajo
		[I.9]	Interrupción de otros servicios y suministros esenciales	2	3	R171	6	2	Bajo
		[E.2]	Errores del administrador	2	1	R172	2	1	Despreciable
		[E.9]	Errores de re-encaminamiento	2	1	R173	2	1	Despreciable
		[E.23]	Errores de mantenimiento / actualización de equipos (hardware)	2	2	R174	4	1	Despreciable
		[E.24]	Caída del sistema por agotamiento de recursos	2	4	R175	8	3	Apreciable
		[A.24]	Denegación del servicio	2	2	R176	4	1	Despreciable
[fire]	Firewall	[I.1]	Fuego	4	1	R177	4	1	Despreciable
		[I.5]	Avería de origen físico o lógico	2	2	R178	4	1	Despreciable
		[I.6]	Corte de suministro	2	4	R179	8	3	Apreciable
		[I.7]	Condiciones inadecuadas de temperatura o humedad	2	3	R180	6	2	Bajo
		[I.8]	Fallo de servicios de comunicaciones	2	3	R181	6	2	Bajo
		[I.9]	Interrupción de otros servicios y suministros esenciales	2	3	R182	6	2	Bajo
		[I.10]	Degradación de los soportes de almacenamiento de la información	2	3	R183	6	2	Bajo
		[E.20]	Vulnerabilidades de los programas (software)	3	5	R184	15	4	Importante
		[E.21]	Errores de mantenimiento / actualización de programas (software)	2	3	R185	6	2	Bajo
		[E.23]	Errores de mantenimiento / actualización de equipos (hardware)	2	3	R186	6	2	Bajo
		[E.24]	Caída del sistema por agotamiento de recursos	2	5	R187	10	3	Apreciable
		[A.4]	Manipulación de la configuración	2	1	R188	2	1	Despreciable
		[A.24]	Denegación del servicio	2	2	R189	4	1	Despreciable
[COM] REDES DE COMUNICACIONES									
[cint]	Internet	[I.1]	Fuego	2	1	R190	2	1	Despreciable
		[I.5]	Avería de origen físico o lógico	3	4	R191	12	4	Importante
		[I.6]	Corte de suministro	2	3	R192	6	2	Bajo
		[I.7]	Condiciones inadecuadas de temperatura o humedad	3	3	R193	9	3	Apreciable
		[I.8]	Fallo de servicios de comunicaciones	3	3	R194	9	3	Apreciable
		[I.9]	Interrupción de otros servicios y suministros esenciales	2	3	R195	6	2	Bajo
		[E.4]	Errores de configuración	1	1	R196	1	1	Despreciable
		[E.9]	Errores de re-encaminamiento	2	1	R197	2	1	Despreciable

		[E.24]	Caída del sistema por agotamiento de recursos	2	1	R198	2	1	Despreciable
		[A.24]	Denegación del servicio	2	1	R199	2	1	Despreciable
[cwfi]	Red Inalámbrica	[I.6]	Corte de suministro	2	5	R200	10	3	Apreciable
		[I.7]	Condiciones inadecuadas de temperatura o humedad	2	3	R201	6	2	Bajo
		[I.8]	Fallo de servicios de comunicaciones	3	3	R202	9	3	Apreciable
		[I.9]	Interrupción de otros servicios y suministros esenciales	2	3	R203	6	2	Bajo
		[E.23]	Errores de mantenimiento / actualización de equipos (hardware)	2	3	R204	6	2	Bajo
		[E.25]	Pérdida de equipos	2	2	R205	4	1	Despreciable
		[A.24]	Denegación del servicio	3	2	R206	6	2	Bajo
[MEDIA] SOPORTE DE INFORMACIÓN									
[elect]	Electrónicos								
[ele1]	Cintas Magnéticas	[I.1]	Fuego	4	1	R207	4	1	Despreciable
		[I.5]	Avería de origen físico o lógico	4	1	R208	4	1	Despreciable
		[I.10]	Degradación de los soportes de almacenamiento de la información	4	1	R209	4	1	Despreciable
		[A.25]	Robo	4	2	R210	8	3	Apreciable
[ele2]	Disco externo USB	[I.1]	Fuego	4	1	R211	4	1	Despreciable
		[I.5]	Avería de origen físico o lógico	2	1	R212	2	1	Despreciable
		[I.10]	Degradación de los soportes de almacenamiento de la información	2	1	R213	2	1	Despreciable
		[E.1]	Errores de los usuarios	2	1	R214	2	1	Despreciable
		[E.25]	Pérdida de equipos	3	1	R215	3	1	Despreciable
[store]	Storage de respaldo de BD	[I.1]	Fuego	4	1	R216	4	1	Despreciable
		[I.5]	Avería de origen físico o lógico	3	2	R217	6	2	Bajo
		[I.9]	Interrupción de otros servicios y suministros esenciales	4	3	R218	12	4	Importante
		[I.10]	Degradación de los soportes de almacenamiento de la información	3	2	R219	6	2	Bajo
		[E.23]	Errores de mantenimiento / actualización de equipos (hardware)	3	2	R220	6	2	Bajo
		[A.24]	Denegación del servicio	2	3	R221	6	2	Bajo
[noel]	No electrónico								
[mimp]	Material impreso	[I.1]	Fuego	4	1	R222	4	1	Despreciable
		[E.7]	Deficiencias en la organización	3	3	R223	9	3	Apreciable
		[E.14]	Escapes de información	2	2	R224	4	1	Despreciable
		[E.19]	Fugas de información	2	2	R225	4	1	Despreciable
		[A.19]	Divulgación de información	2	2	R226	4	1	Despreciable
		[A.25]	Robo	2	1	R227	2	1	Despreciable
[AUX] EQUIPAMIENTO AUXILIAR									
[powr]	Acumulador de energía UPS	[I.1]	Fuego	4	1	R228	4	1	Despreciable
		[I.5]	Avería de origen físico o lógico	4	3	R229	12	4	Importante
		[I.6]	Corte de suministro	2	4	R230	8	3	Apreciable
		[I.7]	Condiciones inadecuadas de temperatura o humedad	2	3	R231	6	2	Bajo

		[I.8]	Fallo de servicios de comunicaciones	1	3	R232	3	1	Despreciable
		[I.9]	Interrupción de otros servicios y suministros esenciales	2	3	R233	6	2	Bajo
		[E.1]	Errores de los usuarios	2	2	R234	4	1	Despreciable
		[E.23]	Errores de mantenimiento / actualización de equipos (hardware)	4	2	R235	8	3	Apreciable
		[E.24]	Caída del sistema por agotamiento de recursos	4	3	R236	12	4	Importante
[psis]	Sistema de aire acondicionado	[I.1]	Fuego	4	1	R237	4	1	Despreciable
		[I.2]	Daños por agua	3	2	R238	6	2	Bajo
		[I.*]	Desastres industriales	3	1	R239	3	1	Despreciable
		[I.3]	Contaminación mecánica	2	2	R240	4	1	Despreciable
		[I.4]	Contaminación electromagnética	2	3	R241	6	2	Bajo
		[I.5]	Avería de origen físico o lógico	3	3	R242	9	3	Apreciable
		[I.6]	Corte de suministro	2	3	R243	6	2	Bajo
		[I.7]	Condiciones inadecuadas de temperatura o humedad	3	3	R244	9	3	Apreciable
		[I.9]	Interrupción de otros servicios y suministros esenciales	4	3	R245	12	4	Importante
		[E.1]	Errores de los usuarios	2	2	R246	4	1	Despreciable
		[E.23]	Errores de mantenimiento / actualización de equipos (hardware)	3	2	R247	6	2	Bajo
		[E.24]	Caída del sistema por agotamiento de recursos	4	4	R248	16	5	Critico
		[A.11]	Acceso no autorizado	2	2	R249	4	1	Despreciable
		[A.23]	Manipulación de los equipos	2	1	R250	2	1	Despreciable
		[A.25]	Robo	3	1	R251	3	1	Despreciable
[gelc]	Grupo electrógeno	[I.1]	Fuego	4	1	R252	4	1	Despreciable
		[I.2]	Daños por agua	4	2	R253	8	3	Apreciable
		[I.4]	Contaminación electromagnética	2	3	R254	6	2	Bajo
		[I.5]	Avería de origen físico o lógico	4	2	R255	8	3	Apreciable
		[I.6]	Corte de suministro	2	5	R256	10	3	Apreciable
		[I.9]	Interrupción de otros servicios y suministros esenciales	2	3	R257	6	2	Bajo
		[E.1]	Errores de los usuarios	2	2	R258	4	1	Despreciable
		[E.23]	Errores de mantenimiento / actualización de equipos (hardware)	3	2	R259	6	2	Bajo
		[E.24]	Caída del sistema por agotamiento de recursos	4	3	R260	12	4	Importante
		[A.25]	Robo	3	2	R261	6	2	Bajo
		[A.28]	Indisponibilidad del personal	2	2	R262	4	1	Despreciable
[cable]	Cableado								
[cab1]	Cableado de red	[I.1]	Fuego	4	1	R263	4	1	Despreciable
		[I.2]	Daños por agua	4	1	R264	4	1	Despreciable
		[I.4]	Contaminación electromagnética	2	3	R265	6	2	Bajo
		[I.5]	Avería de origen físico o lógico	4	4	R266	16	5	Critico
		[E.23]	Errores de mantenimiento / actualización de equipos (hardware)	2	3	R267	6	2	Bajo
		[A.7]	Uso no previsto	2	2	R268	4	1	Despreciable

		[A.23]	Manipulación de los equipos	2	3	R269	6	2	Bajo
		[A.25]	Robo	2	4	R270	8	3	Apreciable
		[A.28]	Indisponibilidad del personal	2	1	R271	2	1	Despreciable
[cab2]	Fibra óptica	[I.1]	Fuego	4	1	R272	4	1	Despreciable
		[I.5]	Avería de origen físico o lógico	2	3	R273	6	2	Bajo
		[E.7]	Deficiencias en la organización	2	3	R274	6	2	Bajo
		[E.23]	Errores de mantenimiento / actualización de equipos (hardware)	2	2	R275	4	1	Despreciable
		[E.28]	Indisponibilidad del personal	2	1	R276	2	1	Despreciable
		[A.23]	Manipulación de los equipos	2	3	R277	6	2	Bajo
[L] INSTALACIONES									
[site]	Data Center	[N.*]	Desastres naturales	4	1	R278	4	1	Despreciable
		[I.1]	Fuego	4	1	R279	4	1	Despreciable
		[I.2]	Daños por agua	2	1	R280	2	1	Despreciable
		[I.7]	Condiciones inadecuadas de temperatura o humedad	4	3	R281	12	4	Importante
		[I.9]	Interrupción de otros servicios y suministros esenciales	3	2	R282	6	2	Bajo
		[E.25]	Pérdida de equipos	2	1	R283	2	1	Despreciable
		[A.11]	Acceso no autorizado	2	1	R284	2	1	Despreciable
		[A.26]	Ataque destructivo	4	1	R285	4	1	Despreciable
		[A.27]	Ocupación enemiga	4	1	R286	4	1	Despreciable
		[A.28]	Indisponibilidad del personal	4	1	R287	4	1	Despreciable
[P] PERSONAL									
[ueex]	Usuario externo	[I.8]	Fallo de servicios de comunicaciones	2	2	R288	4	1	Despreciable
		[E.1]	Errores de los usuarios	2	2	R289	4	1	Despreciable
		[E.18]	Destrucción de la información	2	3	R290	6	2	Bajo
		[E.19]	Fugas de información	2	2	R291	4	1	Despreciable
		[E.20]	Vulnerabilidades de los programas (software)	2	3	R292	6	2	Bajo
		[E.24]	Caída del sistema por agotamiento de recursos	2	3	R293	6	2	Bajo
		[E.25]	Pérdida de equipos	2	1	R294	2	1	Despreciable
		[A.6]	Abuso de privilegios de acceso	2	2	R295	4	1	Despreciable
		[A.7]	Uso no previsto	2	2	R296	4	1	Despreciable
		[A.15]	Modificación deliberada de la información	2	1	R297	2	1	Despreciable
		[A.18]	Destrucción de información	2	1	R298	2	1	Despreciable
		[A.25]	Robo	2	2	R299	4	1	Despreciable
		[A.29]	Extorsión	2	2	R300	4	1	Despreciable
[uex1]	Personal de TI	[I.4]	Contaminación electromagnética	2	4	R301	8	3	Apreciable
		[I.7]	Condiciones inadecuadas de temperatura o humedad	2	4	R302	8	3	Apreciable
		[E.1]	Errores de los usuarios	2	3	R303	6	2	Bajo
		[E.7]	Deficiencias en la organización	2	3	R304	6	2	Bajo

		[A.19]	Divulgación de información	2	2	R305	4	1	Despreciable
		[A.29]	Extorsión	2	2	R306	4	1	Despreciable
		[A.30]	Ingeniería social	2	2	R307	4	1	Despreciable
[adm1]	Administrador del data center	[I.4]	Contaminación electromagnética	3	4	R308	12	4	Importante
		[I.7]	Condiciones inadecuadas de temperatura o humedad	3	4	R309	12	4	Importante
		[I.11]	Emanaciones electromagnética	2	4	R310	8	3	Apreciable
		[E.28]	Indisponibilidad del personal	4	2	R311	8	3	Apreciable
		[A.28]	Indisponibilidad del personal	2	2	R312	4	1	Despreciable

Fuente: Elaborada por los autores en base a MAGERIT- V 3.0 - Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro II

5.1.2. Mapa de Calor

Tabla 42: Mapa de calor

		IMPACTO				
		5	4	3	2	1
PROBABILIDAD	5			R3,R184	R53,R187,R200,R256	
	4		R248,R266	R76,R81,R84,R191,R308,R309	R6,R9,R36,R39,R52,R68,R115,R125,R130,R159,R168,R175,R179,R230,R270,R301,R302,R310	
	3		R79,R218,R229,R236,R245,R260,R281	R1,R19,R24,R65,R66,R67,R82,R83,R102,R103,R111,R131,R132,R143,R144,R145,R151,R153,R193,R194,R202,R223,R242,R244	R2,R13,R18,R25,R37,R38,R50,R51,R62,R104,R116,R117,R118,R119,R120,R121,R127,R133,R142,R156,R157,R158,R163,R164,R169,R170,R171,R181,R182,R183,R185,R186,R192,R195,R201,R203,R204,R221,R231,R233,R241,R243,R254,R257,R265,R267,R269,R273,R274,R277,R290,R292,R293,R303,R304	R232
	2		R15,R33,R42,R47,R71,R210,R235,R253,R255,R311	R8,R45,R78,R92,R97,R112,R141,R146,R206,R217,R219,R220,R238,R247,R259,R261,R282	R4,R5,R7,R11,R12,R27,R30,R35,R40,R43,R44,R49,R54,R59,R60,R69,R70,R73,R90,R91,R98,R106,R109,R110,R126,R134,R135,R155,R165,R167,R174,R176,R178,R189,R205,R224,R225,R226,R234,R240,R246,R249,R258,R262,R268,R275,R288,R289,R291,R295,R296,R299,R300,R305,R306,R307,R312	
	1		R14,R22,R34,R63,R87,R177,R207,R208,R209,R211,R216,R222,R228,R237,R252,R263,R264,R272,R278,R279,R285,R286,R287	R26,R28,R31,R64,R72,R85,R88,R89,R93,R95,R96,R138,R139,R140,R215,R239,R251	R17,R23,R29,R41,R46,R48,R55,R56,R57,R58,R61,R74,R75,R77,R80,R86,R94,R99,R100,R101,R105,R107,R108,R113,R114,R122,R123,R124,R128,R129,R136,R137,R147,R148,R149,R150,R152,R154,R160,R161,R162,R166,R172,R173,R190,R197,R198,R199,R212,R213,R214,R227,R250,R271,R276,R280,R283,R284,R294,R297,R298	R196

Fuente: Elaborada por los autores en base a MAGERIT- V 3.0 - Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro II

Ya conociendo el nivel de riesgo que representan las amenazas, las colocamos en el mapa de calor para determinar a cuál de ellas se le van plantear las salvaguardas necesarias para poder reducir o eliminar el nivel de riesgo en los activos. En este caso las amenazas R32, R248, R266, R3, R184, R16, R76, R81, R84, R191, R308, R309, R53, R187, R200, R256, R20, R21, R79,R218, R229, R236, R245, R260, R281 son las amenazas que fueron utilizadas para el tratamiento de riesgo.

5.1.3. Tratamiento del Riesgo

Tabla 43:Tratamiento del Riesgo

ANÁLISIS DE RIESGO								TRATAMIENTO DE RIESGO					
ACTIVO	AMENAZA	IMPACTO	PROBABILIDAD	CÓDIGO RIESGO	RIESGO	NIVEL	ESCALA	SALVAGUARDA					
								CÓDIGO	NOMBRE	DESCRIPCIÓN	TIPO		EFECTO
CÓDIGO	CÓDIGO										CÓDIGO	NOMBRE	
[S] SERVICIOS													
[sges]	[I.9]	3	5	R3	15	4	Importante	S.A	Aseguramiento de la disponibilidad	Implementar procedimientos para controlar la interrupción del servicio en caso este se vea afectado por la carencia de otro recurso.	[PR]	Preventivas	Preventiva
[SW] APLICACIONES													
[swsc]	[I.9]	3	4	R16	12	4	Importante	SW.A	Copias de seguridad (backup)	Generar copias de seguridad de la información y del software, y ser comprobadas regularmente de acuerdo con la política de copias de seguridad de la organización.	[PR]	Preventivas	Preventiva
	[E.24]	4	3	R20	12	4	Importante	SW.SC	Se aplican perfiles de seguridad	Definir politicas de seguridad para mantener la continuidad del servico en caso este haya caido por carga de trabajo desmesurada.	[PR]	Preventivas	Preventiva
	[A.24]	4	3	R21	12	4	Importante	SW.SC	Se aplican perfiles de seguridad	Definir politicas de seguridad para mantener la continuidad del servico en caso este haya caido por carga de trabajo desmesurada.	[PR]	Preventivas	Preventiva
[swoc]	[E.24]	4	4	R32	16	5	Critico	SW.SC	Se aplican perfiles de seguridad	Definir politicas de seguridad para mantener la continuidad del servico en caso este haya caido por carga de trabajo desmesurada.	[PR]	Preventivas	Preventiva
								SW.A	Copias de seguridad (backup)	Generar copias de seguridad de la información y del software y ser comprobadas regularmente de acuerdo con la política de copias de seguridad de la organización.	[PR]	Preventivas	Preventiva
[HW] EQUIPOS INFORMÁTICOS													
[serv]													
[ser3]	[E.24]	3	4	R76	12	4	Importante	HW.A	Aseguramiento de la disponibilidad	Implementar procedimientos para controlar la interrupción del servicio en caso este se vea afectado por la carencia de otro recurso.	[PR]	Preventivas	Preventivas
	[A.28]	4	3	R79	12	4	Importante	HW.op	Operación	Se debe realizar un plan de acción en caso los trabajadores de la Unidad de Red Telemática no puedan ingresar a su lugar de trabajo para que los servicios no se vean afectados.	[PR]	Preventivas	Preventivas

[ser4]	[I.6]	3	4	R81	12	4	Importante	HW.op	Operación	Se debería aplicar un perfil de seguridad en caso el generador de energía se apague. Cuando el combustible de este se termina los servidores se apagan. para realizar la compra de mas combustible se tiene que mandar a realizar una solictud retrazando así la disponibilidad.	[PR]	Preventivas	Preventivas
	[I.9]	3	4	R84	12	4	Importante	HW.A	Aseguramiento de la disponibilidad	Deberían existir procedimientos para controlar la interrupción del servicio en caso este se vea afectado por la carencia de otro recurso.	[PR]	Preventivas	Preventivas
[netw]													
[fire]	[E.20]	3	5	R184	15	4	Importante	HW.CM	Cambios (actualizaciones y mantenimiento)	Llevar un correcto registro de las actualizaciones y mantenimientos en los programas para que agentes externos no provoquen la caída del activo.	[PR]	Preventivas	Preventivas
[COM] REDES DE COMUNICACIONES													
[cint]	[I.5]	3	4	R191	12	4	Importante	COM.A	Aseguramiento de la disponibilidad	La provisión del servicio proporcionados por las terceras partes deberían ser controlados y revisados regularmente, y también se deberían llevar a cabo auditorías regularmente.	[PR]	Preventivas	Preventivas
								COM.internet	Internet: uso de acceso a red lan UNPRG	Gestionar la provisión de los servicios, incluyendo el mantenimiento y la mejora de las políticas, procedimientos y controles de seguridad de la información existentes, teniendo en cuenta la criticidad de los procesos y sistemas de la organización.	[MN]	De monotorización	consolidan el efecto de las demás
[MEDIA] SOPORTE DE INFORMACIÓN													
[store]	[I.9]	4	3	R218	12	4	Importante	MP.clean	Limpieza de contenidos	El storage debe ser mantenido de una manera correcta para asegurar su continuidad, disponibilidad e integridad.	[PR]	Preventivas	Preventivas
								MP	Protección de los Soportes de Información	El storage de resplado debe estar situado o protegido para reducir los riesgos de las amenazas y los riesgos del entorno.	[PR]	Preventivas	Preventivas
[AUX] EQUIPAMIENTO AUXILIAR													
[powr]	[I.5]	4	3	R229	12	4	Importante	AUX.A	Aseguramiento de la disponibilidad	El acumulador de energía UPS equipo debería ser mantenido de una manera correcta para asegurar su continuidad, disponibilidad e integridad.	[IM]	Minimizadoras	acotan la degradación
	[E.24]	4	3	R236	12	4	Importante	AUX.power	Suministro eléctrico	El acumulador de energía UPD debería estar protegido de los fallos de energía y de otras interrupciones causadas por fallos en las instalaciones de suministro.	[PR]	Preventivas	Preventiva
[psis]	[I.9]	4	3	R245	12	4	Importante	AUX.A	Aseguramiento de la disponibilidad	El equipo de sistema de aire acondicionado debería ser mantenido de una manera correcta para asegurar su continuidad, disponibilidad e integridad.	[PR]	Preventivas	Preventiva

	[E.24]	4	4	R248	16	5	Critico	AUX.power	Suministro eléctrico	El sistema de aire acondicionado debería estar protegido de los fallos de energía y de otras interrupciones causadas por fallos en las instalaciones de suministro.	[PR]	Preventivas	Preventiva
[gelc]	[E.24]	4	3	R260	12	4	Importante	AUX.power	Suministro eléctrico	El grupo electrógeno debería estar protegido de los fallos de energía y de otras interrupciones causadas por fallos en las instalaciones de suministro.	[PR]	Preventivas	Preventiva
[cable]													
[cab1]	[I.5]	4	4	R266	16	5	Critico	AUX.wires	Protección del cableado	El cableado de red debería estar situado o protegido para reducir los riesgos de las amenazas y del entorno, así como de las oportunidades de robo.	[IM]	Minimizadoras	acotan la degradación
[L] INSTALACIONES													
[site]	[I.7]	4	3	R281	12	4	Importante	L.design	Diseño	Diseñar y aplicar una protección física contra el daño por fuego, inundación, humendad y otras formas de desastres industriales o provocadas por el hombre.	[MN]	De monotorización	consolidan el efecto de las demás
[P] PERSONAL													
[adm1]	[I.4]	3	4	R308	12	4	Importante	PS.AT	Formación y concienciación	Todos los empleados de la organización y, cuando corresponda, deberían recibir una formación y concientización adecuadas y actualizadas de las políticas y procedimientos de seguridad y salud en el trabajo, según corresponda a su puesto de trabajo.	[PR]	Preventivas	Preventiva
	[I.7]	3	4	R309	12	4	Importante	PS.A	Aseguramiento de la disponibilidad	Diseñar e implantar la protección física y las directrices para trabajar en las áreas seguras.	[PR]	Preventivas	Preventiva
											[AW]	de concienciación	consolidan el efecto de las demás

Fuente: Elaborada por los autores en base a MAGERIT- V 3.0 - Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro II

Se utilizó la tabla Tratamiento del Riesgo para las amenazas que representaban un nivel de riesgo importante y crítico para los activos de TI de la Unidad de Red Telemática. Se proporcionaron las salvaguardas que podrían tratar el riesgo. Para el activo [sges] se planteó la salvaguarda aseguramiento de la disponibilidad que tendría un efecto preventivo en el activo. En el caso del activo [swsc] se plantearon salvaguardas de copias de seguridad y aplicar perfiles de seguridad que tendrían un efecto preventivo. Para el activo [swoc] se planteó la salvaguardas perfiles de seguridad y copias de seguridad con tendrían un efecto preventivo.

Aseguramiento de la disponibilidad, operación fueron las salvaguardas planteadas para los activos [ser3] y [ser4] con un efecto preventivo.

Para el activo [fire] se planteó la salvaguarda cambios (actualizaciones y mantenimiento) con un efecto preventivo para el tratamiento del riesgo. Aseguramiento de la disponibilidad e internet: uso de acceso a red LAN UNPRG fueron las salvaguardas planteadas para el activo [cinf] con tendrían un efecto preventivo y en el caso de internet un efecto de consolidar el efecto de las demás.

Para el activo [store] se plantearon las salvaguardas limpieza de contenidos y protección de los soportes de seguridad con un efecto preventivo.

Aseguramiento de la disponibilidad y suministro fueron las salvaguardas planteadas para el activo [powr] que tendrían un efecto que acotan la degradación y preventivo.

Para el activo [psis] se plantearon las salvaguardas aseguramiento de la disponibilidad y suministro eléctrico con un efecto preventivo. Suministro eléctrico fue la salvaguarda planteada para el activo [gelc] que tendría un efecto preventivo. Se planteó la salvaguarda protección del cableado del activo [cab1] con un efecto de acotación de degradación para tratar el nivel de riesgo. Para tratar el nivel de riesgo en el activo [site] se planteó la salvaguarda de diseño con un efecto que consolide el efecto de las demás. Finalmente las salvaguardas formación con un efecto preventivo y aseguramiento de la disponibilidad con un efecto preventivo y de concientización fueron planteadas para el activo [adm1].

5.2. METODOLOGIA OCTAVE

5.2.1. Fase 1: Compilar perfiles de amenazas basado en activos

5.2.1.1. Proceso S1: Identificar información de la organización

a. S 1.1 Establecer criterios de evaluación de impacto

Tabla 44: Criterios de Valoración de Impacto.

REPUTACIÓN					
TIPO DE IMPACTO	MUY BAJO	BAJO	MEDIO	ALTO	MUY ALTO
Reputación	La reputación de la Unidad de Red Telemática se afecta en un mínimo porcentaje. Poco o nada de esfuerzo en la mejora de atención a los usuarios es necesario para recuperarse si se presenta la situación de pérdida de confianza los usuarios.	La reputación de la Unidad de Red Telemática se afecta. Poco esfuerzo en la mejora de atención a los usuarios es necesario para recuperarse si se presenta la situación de pérdida de confianza de los usuarios.	La reputación de la Unidad de Red Telemática se daña. Regular esfuerzo en la mejora de atención a los usuarios es necesario para recuperarse si se presenta la situación de pérdida de confianza de los usuarios.	La reputación de la Unidad de Red Telemática se daña. Se requiere mucho esfuerzo para mejorar la confianza de los usuarios.	La reputación de la Unidad de Red Telemática está irremediablemente destruida o dañada.
FINANCIERA					
TIPO DE IMPACTO	MUY BAJO	BAJO	MEDIO	ALTO	MUY ALTO
Costos Operativos	Aumento de menos de 1% anual en costos operativos.	Aumento de menos de 5% anual en costos operativos.	Aumento de 5% anual en costos operativos.	Aumento de 10% anual en costos operativos.	Aumento de más de 10% anual en costos operativos.
PRODUCTIVIDAD					
TIPO DE IMPACTO	MUY BAJO	BAJO	MEDIO	ALTO	MUY ALTO
Carga laboral	Aumento de carga laboral en menos de 10% en 28 días.	Aumento de carga laboral de 30% en 28 días.	Aumento de carga laboral de 50% en 28 días.	Aumento de carga laboral de 70% en 28 días.	Aumento de carga laboral a 100% en 28 días.
Interrupción del servicio	Interrupción de las operaciones por menos de 4 horas.	Interrupción de las operaciones de 5 a 10 horas.	Interrupción de las operaciones de 11 a 16 horas.	Interrupción de las operaciones de 16 a 24 horas.	Interrupción de las operaciones por más de 36 horas.
Administración y gestión	Pudiera impedir la operación efectiva de una parte de la Unidad de Red Telemática.	Probablemente impediría la operación efectiva de una parte de la Organización.	Impediría la operación efectiva de una parte de la Unidad de Red Telemática.	Impediría la operación efectiva de toda la Unidad de Red Telemática.	Impediría seriamente la operación efectiva de la Unidad de Red Telemática, pudiendo llegar a su cierre.

Fuente: Elaborado por los autores en base a Alberts, Christopher. OCTAVE-S Implementation Guide, Versión 1.0.

Fuente: Elaborado por los autores en base a Alberts, Christopher. OCTAVE-S Implementation Guide, Versión 1.0.

SEGURIDAD/SALUD					
TIPO DE IMPACTO	MUY BAJO	BAJO	MEDIO	ALTO	MUY ALTO
Vida	No existe amenaza sobre la vida de los usuarios y/o personal.	La amenaza sobre la vida de los usuarios y/o personal es mínima.	Existe amenaza que puede afectar la vida de los usuarios y/o personal, pero su recuperación es rápida.	Existe amenaza que puede afectar la vida de los usuarios y/o personal, su recuperación es lenta.	Puede haber pérdida de vidas de los usuarios o del personal
Seguridad / salud	Ocurrencia de accidentes que genera incapacidad menor a 2 días en el usuario y/o personal	Ocurrencia de accidentes que genera incapacidad entre 3 a 7 días en el usuario y/o personal	Ocurrencia de accidentes que genera incapacidad entre 8 a 15 días en el usuario y/o personal	Ocurrencia de accidentes que genera incapacidad entre 16 a 28 días en el usuario y/o personal	Ocurrencia de accidentes que genera incapacidad superior a los 28 días en el usuario y/o personal
Fuente: Elaborado por los autores en base a Alberts, Christopher. OCTAVE-S Implementation Guide, Versión 1.0.					
MULTAS/SANCIONES LEGALES					
TIPO DE IMPACTO	MUY BAJO	BAJO	MEDIO	ALTO	MUY ALTO
Multas	No genera sanciones	No genera sanciones significativas	Llamado de atención por parte de los entes de control	Genera sanciones significativas	Sanciones económicas por parte de autoridades legales o entes reguladores

Fuente: Elaborado por los autores en base a Alberts, Christopher. OCTAVE-S Implementation Guide, Versión 1.0.

El criterio de reputación para los niveles de evaluación fue realizado en base a la confianza de los usuarios en el sistema académico que la Unidad proporciona. Criterio financiero en base a los costos operativos que están entre 1 a 10% en caso estos se vean afectado. El activo de productividad en tres factores carga laboral, interrupción del servicio y administración y gestión; el primero con un aumento de 10 a 100% en un periodo de 28 días. Interrupción de servicio de 4 a 36 horas. El activo de seguridad/salud, en vida no afecta la vida de los usuarios/personal. Por ultimo en multas legales en base al actuar de los entes de control.

b. S 1.2 Identificar activos organizacionales.

Tabla 45: Identificación de activos organizacionales.

INFORMACIÓN, SISTEMAS Y APLICACIONES				
CÓDIGO	SISTEMA	INFORMACIÓN	APLICACIÓN Y SERVICIO	OTROS
[swsc]	Sistema de Actas virtuales y matricula online	- Matrículas - Historial académico - Horarios - Plan de estudios - Notas - Actas - Cronograma de matrículas - Programación de semestres - Programación de cursos - Grupos de cursos	Sistema académico actas virtuales UNPRG	- Servidor de dominio - Servidor proxy servidor de base de datos - Servidor de base de datos - backup - Sevidor web - Servidor de archivos -Servidor de base de datos - OCCA - Servidor de base de datos - OCCA - backup
[swoc]	- Sistema académico OCAA	- Notas antiguas - Guías de matrículas - Mensajes de la parte académica - Constancias de matrículas antiguas - Historial académicos pasados	- Gestión de Actas virtuales OCAA	- Servidor de dominio - Servidor proxy servidor de base de datos - Servidor de base de datos - backup - Sevidor web - Servidor de archivos -Servidor de base de datos - OCCA - Servidor de base de datos - OCCA - backup
[ser1]	Servidor de dominio		Acceso a Internet	- Internet - Acumulador de energía UPS - Sistema académico actas virtuales UNPRG - Sistema de académico OCAA - Firewall
[ser2]	Servidor de proxy		Acceso a Internet	- Internet - Acumulador de energía UPS - Sistema académico actas virtuales UNPRG - Sistema de académico OCAA - Firewall
[ser3]	Servidor de base de datos		Acceso a Internet	- Internet - Acumulador de energía UPS - Storage de respaldo de BD - Sistema académico actas virtuales UNPRG - Sistema de académico OCAA
[ser4]	Servidor de base de datos - backup		Acceso a Internet	- Internet - Acumulador de energía UPS - Storage de respaldo de BD - Sistema académico actas virtuales UNPRG - Sistema de académico OCAA
[ser5]	Servidor web		Acceso a Internet	- Internet - Acumulador de energía UPS - Sistema académico actas virtuales UNPRG - Sistema de académico OCAA - Firewall
[ser6]	Servidor de archivos		- Gestión de Actas virtuales y matricula online - Gestión de Actas virtuales OCAA	- Internet - Acumulador de energía UPS - Sistema académico actas virtuales UNPRG - Sistema de académico OCAA - Firewall
[ser7]	Servidor de base de datos - OCAA		- Gestión de Actas virtuales y matricula online - Gestión de Actas virtuales OCAA	- Internet - Acumulador de energía UPS - Storage de respaldo de BD - Sistema académico actas virtuales UNPRG - Sistema de académico OCAA

[ser8]	Servidor de base de datos - backup-OCAA		Acceso a Internet	- Internet - Acumulador de energía UPS - Storage de respaldo de BD - Sistema académico actas virtuales UNPRG - Sistema de académico OCAA
[swit]	Switch	- Administración de accesos y restricciones a la red		- Firewall
[rout]	Router	- Administración de accesos y restricciones a las aplicaciones		- Firewall
[fire]	Firewall	- Enrutamiento de red, acceso al servicio de Internet y capa de seguridad.		
PERSONAS				
CÓDIGO	PERSONAS	HABILIDADES Y CONOCIMIENTOS	SISTEMAS RELACIONADOS	ACTIVOS RELACIONADOS
[adm1]	Administrador del Data Center (Ing. Vladimir Gonzales Mechán)	Administrador de la Unidad de Red Telemática	Sistema académico actas virtuales UNPRG Sistema académico OCCA Servicio FTP Servicio Correo electrónico Gestión de Base de datos	- Switch - Router - Firewall
[uex1]	Personal de TI	Apoyo en los procesos y actividades de la Unidad de Red Telemática.	Servicio de correo electrónico	Equipo para operaciones de apoyo.
[ueex]	Usuarios finales	Uso de los sistemas	- Sistema académico actas virtuales UNPRG - Sistema de académico OCAA	Terminales Informáticas.

Fuente: Elaborado por los autores en base a Alberts, Christopher. OCTAVE-S Implementation Guide, Versión 1.0.

c. S 1.3 Evaluar prácticas de seguridad organizacional.

Tabla 46: Evaluación de prácticas de seguridad.

SEGURIDAD, CONCIENTIZACIÓN Y ENTRENAMIENTO										
ENUNCIADO	¿Hasta qué punto esta afirmación se refleja en su organización?				¿Qué actualmente su organización está haciendo bien en esta área?	¿Qué actualmente su organización no está haciendo bien en esta área?	¿Qué tan efectivamente su organización está implementando las prácticas en esta área?			
Los miembros del personal comprendan sus roles de seguridad y responsabilidades. Esto está documentado y verificado.	SI	ALGO	NO	NO SE SABE	Miembros del personal siguen la buena práctica de no divulgar información confidencial y definición de contraseñas.	No hay roles y responsabilidades definidas.	ROJO	AMARILLO	VERDE	NO APLICA
Hay suficiente experiencia interna para todas las versiones servicios, mecanismos y tecnologías. Esto está documentado y verificado.	SI	ALGO	NO	NO SE SABE	Los miembros del personal tienen tareas definidas.	No existe documentación formal de roles de seguridad.				
Existe una conciencia de seguridad, capacitación y recordatorios periódicos, los que se proporcionan para todo el personal. El entendimiento del personal está documentado y se verifica periódicamente.	SI	ALGO	NO	NO SE SABE		No hay documentación de servicios mecanismos y tecnología.				
Los miembros del personal siguen buenas prácticas como: Asegurar información de la que son responsables, No divulgar información confidencial a otros Tener capacidad suficiente para utilizar la información tecnología de hardware y software, Uso de buenas prácticas para definir contraseñas, Entender y seguir las políticas de seguridad y los reglamentos, Reconocer y reportar incidentes.	SI	ALGO	NO	NO SE SABE		Falta de capacitación para el personal de TI.				
						Personal no entiende todos los riesgos de seguridad.				

Fuente: Elaborado por los autores en base a Alberts, Christopher. OCTAVE-S Implementation Guide, Versión 1.0.

ESTRATEGIA DE SEGURIDAD										
ENUNCIADO	¿Hasta qué punto esta afirmación se refleja en su organización?				¿Qué actualmente su organización está haciendo bien en esta área?	¿Qué actualmente su organización no está haciendo bien en esta área?	¿Qué tan efectivamente su organización está implementando las prácticas en esta área?			
Las estrategias comerciales de la organización incorporan consideraciones de seguridad.	SI	ALGO	NO	NO SE SABE		La actual estrategia de seguridad de la empresa no es efectiva.	ROJO	AMARILLO	VERDE	NO APLICA
Las estrategias y políticas de seguridad toman en cuenta las estrategias y objetivos del negocio de la organización.	SI	ALGO	NO	NO SE SABE		La estrategia de seguridad no se encuentra bien documentada y le falta enfoque empresarial. No es proactiva.				
Las estrategias de seguridad, metas y objetivos son documentados y se revisan de forma rutinaria, se lo actualiza y se comunica a todos.	SI	ALGO	NO	NO SE SABE						

Fuente: Elaborado por los autores en base a Alberts, Christopher. OCTAVE-S Implementation Guide, Versión 1.0.

GESTIÓN DE SEGURIDAD										
ENUNCIADO	¿Hasta qué punto esta afirmación se refleja en su organización?				¿Qué actualmente su organización está haciendo bien en esta área?	¿Qué actualmente su organización no está haciendo bien en esta área?	¿Qué tan efectivamente su organización está implementando las prácticas en esta área?			
La Gerencia asigna fondos y recursos suficientes para actividades de información de seguridad.	SI	ALGO	NO	NO SE SABE	El equipo y el personal están de acuerdo en que la evaluación de riesgos es dar un paso en la dirección correcta que beneficiará a la organización	No hay fondos suficientes en el presupuesto para seguridad.	ROJO	AMARILLO	VERDE	NO APLICA
Los roles y responsabilidades de seguridad se definen para todo el personal de la organización.	SI	ALGO	NO	NO SE SABE		No hay roles definidos				
Todo el personal en todos los niveles de responsabilidad pone en práctica sus funciones asignadas. Existen procedimientos documentados para la autorización y supervisión de todo el personal (incluido el personal tercerizado) que trabajan con sensible información o que trabajan en lugares donde la información reside.	SI	ALGO	NO	NO SE SABE		Miembros del personal se encuentran satisfechos con el nivel de seguridad actual.				
Las prácticas de contratación y terminación de personal en la organización se toman en cuenta la seguridad informática.	SI	ALGO	NO	NO SE SABE						
La organización gestiona los riesgos de seguridad de la información: · Evalúa los riesgos para la seguridad de la información · Toma medidas para mitigar riesgos de seguridad de la información	SI	ALGO	NO	NO SE SABE						
Gerencia recibe y actúa sobre los informes de rutina relacionados con la seguridad de la información (por ejemplo, auditorías, registros y evaluaciones de vulnerabilidad).	SI	ALGO	NO	NO SE SABE						

Fuente: Elaborado por los autores en base a Alberts, Christopher. OCTAVE-S Implementation Guide, Versión 1.0.

POLÍTICAS DE SEGURIDAD Y REGULACIONES										
ENUNCIADO	¿Hasta qué punto esta afirmación se refleja en su organización?				¿Qué actualmente su organización está haciendo bien en esta área?	¿Qué actualmente su organización no está haciendo bien en esta área?	¿Qué tan efectivamente su organización está implementando las prácticas en esta área?			
La organización cuenta con un amplio conjunto de políticas actuales que periódicamente son revisadas y actualización.	SI	ALGO	NO	NO SE SABE		No todo el personal conoce sobre esta práctica.	ROJO	AMARILLO	VERDE	NO APLICA
Hay un procedimiento documentado de gestión de las políticas de seguridad, que incluye: · Creación · Administración (revisiones periódicas y actualizaciones) · Comunicación	SI	ALGO	NO	NO SE SABE		La gente no siempre sigue esta práctica.				
La organización dispone de un procedimiento documentado para evaluar y garantizar el cumplimiento de las políticas de seguridad, leyes y regulaciones aplicables, y requisitos de seguro.	SI	ALGO	NO	NO SE SABE		La práctica de seguridad no se revisa, no está documentada.				
La organización uniformemente refuerza sus políticas de seguridad.	SI	ALGO	NO	NO SE SABE						

Fuente: Elaborado por los autores en base a Alberts, Christopher. OCTAVE-S Implementation Guide, Versión 1.0.

GESTIÓN DE LA SEGURIDAD COLABORATIVA										
ENUNCIADO	¿Hasta qué punto esta afirmación se refleja en su organización?				¿Qué actualmente su organización está haciendo bien en esta área?	¿Qué actualmente su organización no está haciendo bien en esta área?	¿Qué tan efectivamente su organización está implementando las prácticas en esta área?			
La organización tiene políticas y procedimientos para proteger la información cuando trabaja con organizaciones externas (por ejemplo, terceros, colaboradores, subcontratistas o socios), incluidos • proteger la información que pertenece a otras organizaciones • Comprender las políticas y procedimientos de seguridad de las organizaciones externas. • finalizar el acceso a la información por parte de personal externo despedido	SI	ALGO	NO	NO SE SABE		Actualmente no se realiza ese tipo de actividades.	ROJO	AMARILLO	VERDE	NO APLICA
La organización documenta los requisitos de protección de la información y los comunica explícitamente a todos los terceros apropiados.	SI	ALGO	NO	NO SE SABE		Actualmente no se realiza ese tipo de actividades.				
La organización tiene mecanismos formales para verificar que todas las organizaciones de terceros, los servicios, mecanismos y tecnologías de seguridad tercerizados satisfacen sus necesidades y requisitos.	SI	ALGO	NO	NO SE SABE		Actualmente no se realiza ese tipo de actividades.				
La organización tiene políticas y procedimientos para colaborar con todas las organizaciones de terceros que • Brindar servicios de capacitación y sensibilización sobre seguridad • Desarrollar políticas de seguridad para la organización. • desarrollar planes de contingencia para la organización	SI	ALGO	NO	NO SE SABE		Actualmente no se realiza ese tipo de actividades.				

Fuente: Elaborado por los autores en base a Alberts, Christopher. OCTAVE-S Implementation Guide, Versión 1.0.

PLAN DE SEGURIDAD / RECUPERACIÓN DE DESASTRES										
ENUNCIADO	¿Hasta qué punto esta afirmación se refleja en su organización?				¿Qué actualmente su organización está haciendo bien en esta área?	¿Qué actualmente su organización no está haciendo bien en esta área?	¿Qué tan efectivamente su organización está implementando las prácticas en esta área?			
Se ha realizado un análisis de las operaciones, las aplicaciones y los datos críticos.	SI	ALGO	NO	NO SE SABE		No existe un plan de recuperación ante desastres naturales o emergencia	ROJO	AMARILLO	VERDE	NO APLICA
La organización ha documentado, revisado y probado: · Planes de continuidad del negocio y de operación en caso de emergencia · Plan de recuperación de desastres (s)	SI	ALGO	NO	NO SE SABE		No existe plan de continuidad del negocio.				
Los planes de contingencia, recuperación de desastres y de negocios consideran la continuidad física y electrónica y los requisitos de acceso y controles.	SI	ALGO	NO	NO SE SABE		No hay un plan de recuperación para sistemas o redes.				

Todo el personal: · Esta consciente de los planes de recuperación de desastres imprevistos y continuidad del negocio. · Comprende y es capaz de realizar sus responsabilidades.	SI	ALGO	NO	NO SE SABE		

Fuente: Elaborado por los autores en base a Alberts, Christopher. OCTAVE-S Implementation Guide, Versión 1.0.

CONTROL DE ACCESO FÍSICO									
ENUNCIADO	¿Hasta qué punto esta afirmación se refleja en su organización?				¿Qué actualmente su organización está haciendo bien en esta área?	¿Qué actualmente su organización no está haciendo bien en esta área?	¿Qué tan efectivamente su organización está implementando las prácticas en esta área?			
Si alguien del personal está encargado de esta área: Planes de seguridad de las instalaciones y procedimientos para salvaguardar las instalaciones, edificios y cualquier zona restringida y están documentados y probados.	SI	ALGO	NO	NO SE SABE		La seguridad física se ve afectada debido a que en ocasiones se comparten laptops, se conocen contraseñas de la otra persona y se comparte el espacio en la oficina.	ROJO	AMARILLO	VERDE	NO APLICA
Hay políticas y procedimientos documentados para la gestión de los visitantes.	SI	ALGO	NO	NO SE SABE						
Hay políticas y procedimientos documentados para controlar el acceso físico a las áreas de trabajo y hardware (ordenadores, dispositivos de comunicación, etc.) y soporte de software.	SI	ALGO	NO	NO SE SABE						
Las estaciones de trabajo y otros componentes que permiten acceso a información sensible están físicamente salvaguardados para prevenir el acceso no autorizado.	SI	ALGO	NO	NO SE SABE						

Fuente: Elaborado por los autores en base a Alberts, Christopher. OCTAVE-S Implementation Guide, Versión 1.0.

MONITOREO Y AUDITORIA DE SEGURIDAD FISICA									
ENUNCIADO	¿Hasta qué punto esta afirmación se refleja en su organización?				¿Qué actualmente su organización está haciendo bien en esta área?	¿Qué actualmente su organización no está haciendo bien en esta área?	¿Qué tan efectivamente su organización está implementando las prácticas en esta área?			
Se mantienen registros de mantenimiento para documentar las reparaciones y modificaciones de los componentes físicos de una instalación.	SI	ALGO	NO	NO SE SABE		Actualmente no se realiza ese tipo de actividades.	ROJO	AMARILLO	VERDE	NO APLICA
Las acciones de un individuo o grupo, con respecto a todos los medios controlados físicamente, pueden contabilizarse.	SI	ALGO	NO	NO SE SABE		Actualmente no se realiza ese tipo de actividades.				
Los registros de auditoría y monitoreo se examinan rutinariamente para detectar anomalías, y se toman medidas correctivas según sea necesario.	SI	ALGO	NO	NO SE SABE		Actualmente no se realiza ese tipo de actividades.				

Los requisitos de la organización para monitorear la seguridad física se comunican formalmente a todos los contratistas y proveedores de servicios que supervisan el acceso físico al edificio y las instalaciones, áreas de trabajo, hardware de TI y medios de software.	SI	ALGO	NO	NO SE SABE		Actualmente no se realiza ese tipo de actividades.
La organización verifica formalmente que los contratistas y proveedores de servicios hayan cumplido los requisitos para monitorear la seguridad física.	SI	ALGO	NO	NO SE SABE		

Fuente: Elaborado por los autores en base a Alberts, Christopher. OCTAVE-S Implementation Guide, Versión 1.0.

GESTIÓN DEL SISTEMA Y LA RED										
ENUNCIADO	¿Hasta qué punto esta afirmación se refleja en su organización?				¿Qué actualmente su organización está haciendo bien en esta área?	¿Qué actualmente su organización no está haciendo bien en esta área?	¿Qué tan efectivamente su organización está implementando las prácticas en esta área?			
Si alguien del personal está encargado de esta área: Existen planes de seguridad para salvaguardar el sistema y las redes.	SI	ALGO	NO	NO SE SABE	Acceso a servidores y sistemas están protegidos con contraseñas	No existe un plan documentado de seguridad.	ROJO	AMARILLO	VERDE	NO APLICA
La información confidencial está protegida en un almacenamiento seguro (por ejemplo, copias de seguridad almacenadas en otro sitio).	SI	ALGO	NO	NO SE SABE	Existen copias de seguridad.	No todos los sistemas están actualizados				
La integridad del software instalado es regularmente verificada.	SI	ALGO	NO	NO SE SABE		No hay planes de control de hardware y software planeados				
Todos los sistemas están actualizados a la fecha de acuerdo con revisiones, parches y recomendaciones de seguridad.	SI	ALGO	NO	NO SE SABE		No hay procedimientos formales para cambio de contraseñas o manejo de usuarios.				
Existe un plan documentado y comprobado para la copia de seguridad de los datos de software. Todo el personal entiende sus responsabilidades en virtud de los planes de copia de seguridad.	SI	ALGO	NO	NO SE SABE						
Todos los cambios de hardware y software son planeados, controlados y documentados. Los miembros del área de TI siguen procedimientos para cambiar y dar de baja contraseñas, cuentas y privilegios.	SI	ALGO	NO	NO SE SABE						
Solo los servicios necesarios están corriendo en los sistemas, todos los servicios que no son necesarios han sido eliminados.	SI	ALGO	NO	NO SE SABE						
Herramientas y mecanismos para el sistema de seguridad y administración de la red que se utilizan, se revisan de manera rutinaria, se actualizan o reemplazan.	SI	ALGO	NO	NO SE SABE						

Fuente: Elaborado por los autores en base a Alberts, Christopher. OCTAVE-S Implementation Guide, Versión 1.0.

MONITOREO Y AUDITORIA DE LA SEGURIDAD DE TI										
ENUNCIADO	¿Hasta qué punto esta afirmación se refleja en su organización?				¿Qué actualmente su organización está haciendo bien en esta área?	¿Qué actualmente su organización no está haciendo bien en esta área?	¿Qué tan efectivamente su organización está implementando las prácticas en esta área?			
Si alguien del personal está encargado de esta área: Sistema y red de monitoreo y herramientas de auditoría son habitualmente utilizados por la organización. Actividades inusuales se manejan de acuerdo con las políticas y procedimientos definidos.	SI	ALGO	NO	NO SE SABE	Se realizan monitoreo del sistema.	No se reporta actividad inusual.	ROJO	AMARILLO	VERDE	NO APLICA
Componentes del Firewall y otros componentes de seguridad son auditados periódicamente para revisar el cumplimiento de políticas.	SI	ALGO	NO	NO SE SABE		No hay políticas definidas.				

Fuente: Elaborado por los autores en base a Alberts, Christopher. OCTAVE-S Implementation Guide, Versión 1.0.

AUTENTICACIÓN Y AUTORIZACIÓN										
ENUNCIADO	¿Hasta qué punto esta afirmación se refleja en su organización?				¿Qué actualmente su organización está haciendo bien en esta área?	¿Qué actualmente su organización no está haciendo bien en esta área?	¿Qué tan efectivamente su organización está implementando las prácticas en esta área?			
Los controles de acceso apropiados y la autenticación del usuario (por ejemplo, permisos de archivos, configuración de red) consistentes con la política se usan para restringir el acceso del usuario a la información, sistemas sensibles, aplicaciones y servicios específicos y conexiones de red.	SI	ALGO	NO	NO SE SABE		Actualmente no se realiza ese tipo de actividades.	ROJO	AMARILLO	VERDE	NO APLICA
Existen políticas y procedimientos documentados para establecer y rescindir el derecho de acceso a la información tanto para individuos como para grupos.	SI	ALGO	NO	NO SE SABE						
Se proporcionan métodos o mecanismos para garantizar que no se acceda, altere o destruya la información confidencial de manera no autorizada. Los métodos o mecanismos se revisan y verifican periódicamente.	SI	ALGO	NO	NO SE SABE						
Los requisitos de la organización para controlar el acceso a los sistemas y la información se comunican formalmente a todos los contratistas y proveedores de servicios que brindan servicios de autenticación y autorización.	SI	ALGO	NO	NO SE SABE						
La organización verifica formalmente que los contratistas y proveedores de servicios hayan cumplido los requisitos de autenticación y autorización.	SI	ALGO	NO	NO SE SABE						

Fuente: Elaborado por los autores en base a Alberts, Christopher. OCTAVE-S Implementation Guide, Versión 1.0.

MANEJO DE LA VULNERABILIDAD										
ENUNCIADO	¿Hasta qué punto esta afirmación se refleja en su organización?				¿Qué actualmente su organización está haciendo bien en esta área?	¿Qué actualmente su organización no está haciendo bien en esta área?	¿Qué tan efectivamente su organización está implementando las prácticas en esta área?			
Si alguien del personal está encargado de esta área: Hay un conjunto de procedimientos documentados para manejo de vulnerabilidades, para: · Seleccionar las herramientas de evaluación de vulnerabilidad, listas de control y secuencias de comandos · Mantenerse al día con la vulnerabilidad conocida, tipos y métodos de ataque · Revisar las fuentes de información sobre anuncios de vulnerabilidad, alertas de seguridad y comunicación · Identificación de los componentes de infraestructura a ser evaluado · Programar evaluaciones de vulnerabilidad · Interpretar y responder a los resultados · Mantener un almacenamiento seguro y la disposición de datos vulnerables.	SI	ALGO	NO	NO SE SABE		No hay procedimientos definidos para poder manejar la vulnerabilidad en la organización.	ROJO	AMARILLO	VERDE	NO APLICA
Se siguen procedimientos de gestión de vulnerabilidades los que son periódicamente revisados y actualizados.	SI	ALGO	NO	NO SE SABE						
Evaluaciones de tecnología vulnerable se realizan en forma periódica, y las vulnerabilidades se abordan cuando se las identifica.	SI	ALGO	NO	NO SE SABE						

Fuente: Elaborado por los autores en base a Alberts, Christopher. OCTAVE-S Implementation Guide, Versión 1.0.

ENCRIPTACIÓN										
ENUNCIADO	¿Hasta qué punto esta afirmación se refleja en su organización?				¿Qué actualmente su organización está haciendo bien en esta área?	¿Qué actualmente su organización no está haciendo bien en esta área?	¿Qué tan efectivamente su organización está implementando las prácticas en esta área?			
Si alguien del personal está encargado de esta área: · Controles apropiados de seguridad se utilizan para proteger información sensible durante el almacenamiento y durante la transmisión (por ejemplo, el cifrado de datos, infraestructura de clave pública, tecnología de red privada virtual).	SI	ALGO	NO	NO SE SABE	Se maneja una red privada virtual.		ROJO	AMARILLO	VERDE	NO APLICA
Se utilizan protocolos de cifrado cuando se maneja sistemas, routers y firewalls a distancia.	SI	ALGO	NO	NO SE SABE						

Fuente: Elaborado por los autores en base a Alberts, Christopher. OCTAVE-S Implementation Guide, Versión 1.0.

SEGURIDAD DE DISEÑO Y ARQUITECTURA										
ENUNCIADO	¿Hasta qué punto esta afirmación se refleja en su organización?				¿Qué actualmente su organización está haciendo bien en esta área?	¿Qué actualmente su organización no está haciendo bien en esta área?	¿Qué tan efectivamente su organización está implementando las prácticas en esta área?			
Si alguien del personal está encargado de esta área: Arquitectura del sistema y diseño para sistemas nuevos y actualizaciones que incluyen las siguientes consideraciones: · Estrategias de seguridad, políticas y procedimientos · Antecedentes de compromisos de seguridad. · Resultados de las evaluaciones de riesgos de seguridad.	SI	ALGO	NO	NO SE SABE	Existe el diagrama de arquitectura de red de la institución	No se ha discutido con el personal sobre seguridad del diseño y la arquitectura	ROJO	AMARILLO	VERDE	NO APLICA
La organización tiene diagramas que muestran la seguridad en toda la empresa y la arquitectura de red que están actualizados.	SI	ALGO		NO SE SABE						

Fuente: Elaborado por los autores en base a Alberts, Christopher. OCTAVE-S Implementation Guide, Versión 1.0.

MANEJO DE INCIDENTES										
ENUNCIADO	¿Hasta qué punto esta afirmación se refleja en su organización?				¿Qué actualmente su organización está haciendo bien en esta área?	¿Qué actualmente su organización no está haciendo bien en esta área?	¿Qué tan efectivamente su organización está implementando las prácticas en esta área?			
Si alguien del personal está encargado de esta área: Existen procedimientos documentados para la identificación, presentación de informes, y procesos para responder a incidentes sospechosos y violaciones.	SI	ALGO	NO	NO SE SABE		No existen procedimientos para presentar informes o procesos para responder a incidentes sospechosos y violaciones.	ROJO	AMARILLO	VERDE	NO APLICA
Los procedimientos de manejo de incidentes son periódicamente probados, verificados y actualizados.	SI	ALGO	NO	NO SE SABE		Nunca se ha considerado desarrollar una política para tratar con incidentes sospechosos violaciones o autoridades policiales.				
Existen políticas y procedimientos documentados para trabajar con autoridades policiales.	SI	ALGO	NO	NO SE SABE		No se reportan incidentes o violaciones.				

Fuente: Elaborado por los autores en base a Alberts, Christopher. OCTAVE-S Implementation Guide, Versión 1.0.

Al término de la evaluación concluimos que la Unidad de Red Telemática de la Universidad Nacional Pedro Ruiz Gallo, no cumple con ellas en su mayoría, ya que al aplicar el estado semáforo observamos que la mayoría de ellas están en rojo; es decir que la Unidad de Red Telemática organización no está realizando las prácticas de seguridad en el área y que hay espacio significativo para la mejora.

5.2.1.2. Proceso S2: Crear perfiles de amenazas

a. S 2.1 Seleccionar activos críticos

Tabla 47: Activos críticos

CÓDIGO	ACTIVOS CRÍTICOS	NOTAS
[swsc]	Sistema académico actas virtuales UNPRG	El sistema de actas virtuales, es el sistema de gestión académica para pregrado.
[ser3]	Servidor de base de datos	Es el servidor que almacena la base de datos del sistema académico para pregrado.
[fire]	Firewall Central	Router principal de la red - UNPRG, realiza el enrutamiento de la red y permite acceso al servicio de internet.
[adm1]	Administrador del data center	El encargado de dirigir y autorizar todas las actividades y procesos de la Unidad de Red Telemática el Ingeniero Vladimir Gonzales Menchán.

Fuente: Elaborado por los autores en base a Alberts, Christopher. OCTAVE-S Implementation Guide, Versión 1.0.

Tabla 48: Descripción de activos críticos.

ACTIVO CRÍTICO [swsc]

ACTIVO CRÍTICO	RAZÓN DE SELECCIÓN
¿Cuál es el sistema crítico?	¿Por qué este sistema es crítico para la organización?
Gestión de Actas virtuales y matricula online	Este activo fue seleccionado como crítico porque es del que dependen los procesos fundamentales del servicio académico de la Unidad de Red Telemática. Los alumnos (matricula, historial, horario, plan de estudios, notas), registros académicos (registrar actas de docentes e ingresarlos al sistema), docentes (carga horaria, horarios e ingreso de notas) y el administrador de aplicaciones y base de datos (generar actas, cambio de notas, bloqueos de actas, conteo de actas, proceso de matrícula, activar actas, cronograma de matrículas, programación de semestres, programación de cursos, grupos).

DESCRIPCIÓN
¿Quién usa el sistema? / ¿Quién es responsable del sistema?
Estudiantes, Docentes, Administrador de Base de Datos.

ACTIVOS RELACIONADOS			
¿Qué activos están relacionados con este sistema?			
Sistemas	Información	Aplicaciones	Otros
- Servidor de dominio - Servidor proxy servidor de base de datos - Servidor de base de datos - backup - Sevidor web - Servidor de archivos -Servidor de base de datos - OCCA - Servidor de base de datos - OCCA - backup	- Matrículas - Historial académico - Horarios - Plan de estudios - Notas - Actas - Cromograma de matrículas - Programación de semestres - Programación de cursos - Grupos de cursos	Sistema académico actas virtuales UNPRG	

ACTIVO CRÍTICO [ser3]

ACTIVO CRÍTICO	RAZÓN DE SELECCIÓN
¿Cuál es el sistema crítico?	¿Por qué este sistema es crítico para la organización?
Servidor de base de datos	El lugar donde se almacenará toda la información obtenida en el proceso de matrícula, así mismo tiene información de todas las matrículas anteriores e información necesaria para la realización de dicho proceso.

DESCRIPCIÓN
¿Quién usa el sistema? / ¿Quién es responsable del sistema?
- Administrador de red telemática (Ing. Vladimir Gonzales)

ACTIVOS RELACIONADOS			
¿Qué activos están relacionados con este sistema?			
Sistemas	Información	Aplicaciones	Otros
- Sistema académico actas virtuales UNPRG - Sistema académico OCAA		- Gestión de Actas virtuales y matricula online - Gestión de Actas virtuales OCAA	- Internet - Acumulador de energía UPS - Storage de respaldo de BD - Sistema académico actas virtuales UNPRG - Sistema de académico OCAA

Fuente: Elaborado por los autores en base a Alberts, Christopher. OCTAVE-S Implementation Guide, Versión 1.0.

ACTIVO CRÍTICO [fire]

ACTIVO CRÍTICO	RAZÓN DE SELECCIÓN
¿Cuál es el sistema crítico?	¿Por qué este sistema es crítico para la organización?
Firewall	Enrutador principal de conexión a internet y capa de seguridad antes posibles ataques.

DESCRIPCIÓN
¿Quién usa el sistema? / ¿Quién es responsable del sistema?
- Administrador de red telemática (Ing. Vladimir Gonzales)

ACTIVOS RELACIONADOS			
¿Qué activos están relacionados con este sistema?			
Sistemas	Información	Aplicaciones	Otros
- Servidor de dominio - Servidor proxy servidor de base de datos - Servidor de base de datos - backup - Sevidor web - Servidor de archivos -Servidor de base de datos - OCCA - Servidor de base de datos - OCCA - backup - Switch - Router	- Enrutamiento de red, acceso al servicio de Internet y capa de seguridad.		

ACTIVO CRÍTICO [adm1]

ACTIVO CRÍTICO	RAZÓN DE SELECCIÓN
¿Cuál es la(s) persona(s) crítica(s)?	¿Por qué esta persona(s) es crítica para la organización?
Administrador del data center	Persona encargada de la administración de general de la unidad de red telemática, persona muy crítica por ser el único personal en el área.

DESCRIPCIÓN
¿Qué habilidades o conocimientos especiales son proporcionados por esta(s) persona(s)?
- Experto en administración de redes y servidores. - Conocimiento de todos los procesos de la unidad de red telemática. - Así mismo conocedor de todas las contraseñas de cada equipo de comunicación de red en la unidad.

ACTIVOS RELACIONADOS			
¿Qué activos están relacionados a este activo?			
Sistemas	Información	Aplicaciones	Otros
- Servidor de dominio - Servidor proxy servidor de base de datos - Servidor de base de datos - backup - Sevidor web - Servidor de archivos -Servidor de base de datos - OCCA - Servidor de base de datos - OCCA - backup			- Switch - Router - Firewall

Fuente: Elaborado por los autores en base a Alberts, Christopher. OCTAVE-S Implementation Guide, Versión 1.0.

b. S 2.2 Identificar los requisitos de seguridad para los activos críticos.

Tabla 49: Requisitos de seguridad de los activos críticos

ACTIVO CRÍTICO [swsc]
REQUERIMIENTOS DE SEGURIDAD
¿Cuáles son los requisitos de seguridad para este sistema?
- Confidencialidad: Solo el personal autorizado puede acceder y ver la información contenida en Sistema académico actas virtuales UNPRG y matricula online. Cada persona accede a la información mediante código de usuario y password único. - Integridad: Solo el personal autorizado puede modificar o eliminar la información contenida en Sistema académico actas virtuales UNPRG. Cada persona accede a la información mediante código de usuario y password único. - Disponibilidad El servicio de Gestión de Actas virtuales y matricula online UNPRG debe estar disponible para que el personal realice sus trabajos. El sistema debe estar activo en todos los procesos de matrícula. - Otros

Requerimiento de seguridad más importante
¿Qué requisito de seguridad es más importante para este sistema?
* Confidencialidad
* Integridad
* Disponibilidad
* Otros

ACTIVO CRÍTICO [ser3]
REQUERIMIENTOS DE SEGURIDAD
¿Cuáles son los requisitos de seguridad para este sistema?
- Confidencialidad Solo personal autorizado puede acceder y ver información sobre Servidor de base de datos. La información sensible de las matrículas no debe ser expuesta a personal no autorizado. - Integridad Solo personal autorizado puede modificar o eliminar información sobre Servidor de base de datos. La información sensible de las matrículas solo podrá modificarse previo permiso por la alta dirección y solo por personal autorizado. - Disponibilidad Servidor de base de datos debe estar disponible para que el personal realice sus trabajos. Esta información debe mantenerse disponible solo lo necesario para el alumno matriculado y para la realización de reportes. - Otros

Requerimiento de seguridad más importante
¿Qué requisito de seguridad es más importante para este sistema?
* Confidencialidad
* Integridad
* Disponibilidad
* Otros

Fuente: Elaborado por los autores en base a Alberts, Christopher. OCTAVE-S Implementation Guide, Versión 1.0.

ACTIVO CRÍTICO [fire]

REQUERIMIENTOS DE SEGURIDAD
¿Cuáles son los requisitos de seguridad para este sistema?
- Confidencialidad Solo personal autorizado puede acceder y ver información sobre Firewall. Solo personal autorizado tendrá acceso a la información almacenada en Firewall - Integridad Solo personal autorizado puede modificar o eliminar información sobre Firewall Esta información solo deberá ser modificada solo si sea necesario por el administrador de red telemática. - Disponibilidad Firewall debe estar disponible para que el personal realice sus trabajos. Deberá estar disponible antes algún caso de que se necesite agregar algún enrutamiento o denegar algún acceso por posibles ataques. - Otros

Requerimiento de seguridad más importante
¿Qué requisito de seguridad es más importante para este sistema?
* Confidencialidad
* Integridad
* Disponibilidad
* Otros

ACTIVO CRÍTICO [adm1]

REQUERIMIENTOS DE SEGURIDAD
¿Cuáles son los requisitos de seguridad para esta(s) persona(s)?
- Disponibilidad El conjunto de habilidades proporcionadas por el administrador de red telemática debe estar disponible cuando sea necesario. El administrador de red telemática debe estar laborando todo el tiempo correspondiente al proceso de matrículas por si surgen caídas en algún sistema o servidor. - Otros

Requerimiento de seguridad más importante
¿Qué requisito de seguridad es más importante para esta(s) persona(s)?
* Confidencialidad
* Integridad
* Disponibilidad
* Otros

Fuente: Elaborado por los autores en base a Alberts, Christopher. OCTAVE-S Implementation Guide, Versión 1.0.

c. S 2.3 Identificar amenazas a los activos críticos

Tabla 50: Hoja de trabajo de perfil de riesgo para Sistema académico actas virtuales UNPRG - Actores humanos que utilizan el acceso a la red.

AMENAZA					ACTORES DE AMENAZA	MOTIVO							
¿Para cuál rama hay una posibilidad no despreciable de una amenaza al activo? Marque estas ramas en el árbol. ¿Para cuál de las ramas restantes hay una posibilidad despreciable o nula de una amenaza para el activo? No marque estas ramas.					¿Qué actores plantean las mayores amenazas para el sistema a través de la red?	¿Qué tan fuerte es el motivo del actor?					¿Qué tan confiado está usted de este estimado?		
Activo	Acceso	Actor	Motivo	Resultado		Muy alto	alto	Medio	Bajo	Muy bajo	Muy	Algo	Nada
Sistema académico actas virtuales UNPRG	Red	Adentro	Accidental	Revelación	**Personas que pertenecen a la organización que actúan accidentalmente:** Personal administrativo y practicantes discutiendo información sensible en áreas públicas.							x	
				Modificación			x				x		
				Pérdida				x				x	
				Interrupción			x					x	
			Intencionado	Revelación	**Personas que pertenecen a la organización que actúan deliberadamente:** Personal administrativo o practicantes descontentos o personas que dan un mal uso al sistema académico de actas virtuales UNPRG.							**X**	
				Modificación								**X**	
				Pérdida								**X**	
				Interrupción								**X**	
		Afuera	Accidental	Revelación	**Personas ajenas a la organización que actúan accidentalmente:** Personal contratado para desarrollo del sistema.							x	
				Modificación								X	
				Pérdida								X	
				Interrupción								X	
			Intencionado	Revelación	**Personas ajenas a la organización que actúan deliberadamente:** Espías, hackers, terroristas, alumnos.		**x**					**x**	
				Modificación			**x**				**x**		
				Pérdida				**x**				**x**	
				Interrupción				**x**				**x**	

HISTORIA

¿Con qué frecuencia ha ocurrido esta amenaza en el pasado?	¿Qué tan exactos son estos datos?		
	Muy	Algo	Nada
0 veces en 2 años		x	
3 veces en 2 años	x		
1 veces en 2 años		x	
3 veces en 2 años		x	
0 veces en 2 años		x	
0 veces en 2 años		x	
0 veces en 2 años		x	
0 veces en 2 años		x	
0 veces en 2 años		x	
0 veces en 2 años		x	
0 veces en 2 años		x	
0 veces en 2 años		x	
7 veces en 2 años		x	
3 veces en 2 años		x	
1 veces en 2 años		x	
0 veces en 2 años		x	

Gente que pertenece a la organización que tiene acceso a la red	
De ejemplos de cómo personas que pertenecen a la organización actuando accidentalmente podrían utilizar el acceso a la red para amenazar el sistema.	Modificación de las bases de datos, O por accidente el administrador coloco mal los datos de algún usuario.
De ejemplos de cómo personas que pertenecen a la organización que actuando deliberadamente podrían utilizar el acceso a la red para amenazar el sistema.	

Gente que no pertenece a la organización que tiene acceso a la red	
De ejemplos de cómo personas que no pertenecen a la organización que actuando accidentalmente podrían utilizar el acceso a la red para amenazar el sistema.	
De ejemplos de cómo personas que no pertenecen a la organización que actuando deliberadamente podrían utilizar el acceso a la red para amenazar el sistema.	Cambio en las notas de los alumnos.

Fuente: Elaborado por los autores en base a Alberts, Christopher. OCTAVE-S Implementation Guide, Versión 1.0.

Dando respuesta a las preguntas planteadas en la Hoja de trabajo de perfil de riesgo para Sistema académico actas virtuales UNPRG - Actores humanos que utilizan el acceso a la red. Se identificaron las amenazas, el actor y en el motivo por el que ocurrieron. Así como también el nivel de confianza que se tiene de dicha información, el historial y ejemplos de cómo ocurrieron.

Tabla 51: Hoja de trabajo de perfil de riesgo para Sistema académico actas virtuales UNPRG - actores humanos que utilizan el acceso físico.

AMENAZA					**Actores de amenaZa**	**MOTIVO**							
¿Para cuál rama hay una posibilidad no despreciable de una amenaza al activo? Marque estas ramas en el árbol. ¿Para cuál de las ramas restantes hay una posibilidad despreciable o nula de una amenaza para el activo? No marque estas ramas.					¿Qué actores plantean las mayores amenazas para el sistema por medios físicos?	¿Qué tan fuerte es el motivo del actor?					¿Qué tan confiado está usted de este estimado?		
Activo	Acceso	Actor	Motivo	Resultado		Muy alto	alto	Medio	Bajo	muy bajo	Muy	Algo	Nada
Sistema académico actas virtuales UNPRG	Físico	Adentro	Accidental	Revelación	**Personas que pertenecen a la organización que actúan accidentalmente:** Personal administrativo o practicantes que usa las computadoras de otras personas.							X	
				Modificación								X	
				Pérdida								X	
				Interrupción								X	
			Intencionado	Revelación	**Personas que pertenecen a la organización que actúan deliberadamente:** Personal administrativo o practicantes descontentos.						**X**		
				Modificación							**X**		
				Pérdida							**X**		
				Interrupción							**X**		
		Afuera	Accidental	Revelación	**Personas ajenas a la organización que actúan accidentalmente:** Personal contratado para desarrollo del sistema.							X	
				Modificación								X	
				Pérdida								X	
				Interrupción								X	
			Intencionado	Revelación	**Personas ajenas a la organización que actúan deliberadamente:** Espías, terroristas, alumnos.						**X**		
				Modificación							**X**		
				Pérdida							**X**		
				Interrupción							**X**		

¿Con qué frecuencia ha ocurrido esta amenaza en el pasado?	¿Qué tan exactos son estos datos?		
	Muy	Algo	Nada
0 veces en 2 años		x	
0 veces en 2 años		x	
0 veces en 2 años		x	
0 veces en 2 años		x	
0 veces en 2 años	x		
0 veces en 2 años	x		
0 veces en 2 años	x		
0 veces en 2 años	x		
0 veces en 2 años		x	
0 veces en 2 años		x	
0 veces en 2 años		x	
0 veces en 2 años		x	
0 veces en 2 años	x		
0 veces en 2 años	x		
0 veces en 2 años	x		
0 veces en 2 años	x		

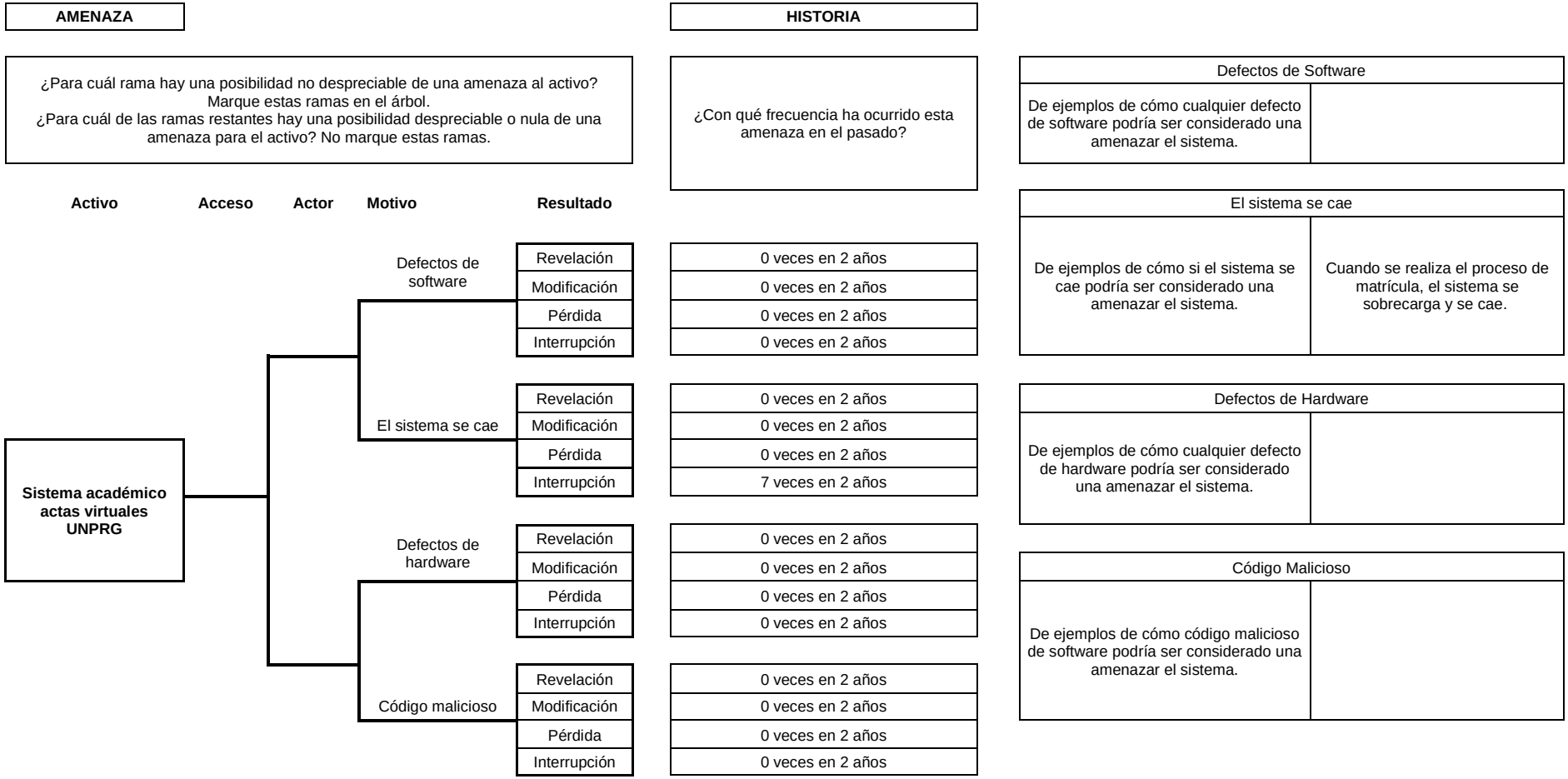
Gente que pertenece a la organización que usan el acceso físico	
Dé ejemplos de cómo personas que pertenecen a la organización actuando accidentalmente podrían usar el acceso físico para amenazar este sistema.	
Dé ejemplos de cómo personas que pertenecen a la organización que actuando deliberadamente podrían usar el acceso físico para amenazar este sistema	

Gente que no pertenece a la organización que usan el acceso físico	
Dé ejemplos de cómo personas que no pertenecen a la organización que actuando accidentalmente podrían usar el acceso físico para amenazar este sistema.	
Dé ejemplos de cómo personas que no pertenecen a la organización que actuando deliberadamente podrían usar el acceso físico para amenazar este sistema.	

Fuente: Elaborado por los autores en base a Alberts, Christopher. OCTAVE-S Implementation Guide, Versión 1.0.

En la Hoja de trabajo de perfil de riesgo para Sistema académico actas virtuales UNPRG - actores humanos que utilizan el acceso físico. No se identificaron amenazas.

Tabla 52: Hoja de trabajo de perfil de riesgo para Sistema académico actas virtuales UNPRG - Problemas del sistema



Fuente: Elaborado por los autores en base a Alberts, Christopher. OCTAVE-S Implementation Guide, Versión 1.0.

Tabla 53: Hoja de trabajo de perfil de riesgo para Sistema académico actas virtuales UNPRG- Otros problemas.

Amenaza					Historia
¿Para cuál rama hay una posibilidad no despreciable de una amenaza al activo? Marque estas ramas en el árbol. ¿Para cuál de las ramas restantes hay una posibilidad despreciable o nula de una amenaza para el activo? No marque estas ramas.					¿Con qué frecuencia ha ocurrido esta amenaza en el pasado?
Activo	**Acceso**	**Actor**	**Motivo**	**Resultado**	
Sistema académico actas virtuales UNPRG			Problemas con el suministro de energía	Revelación	0 veces en 2 años
				Modificación	0 veces en 2 años
				Pérdida	0 veces en 2 años
				Interrupción	3 veces en 2 años
			Problemas de telecomunicaciones	Revelación	0 veces en 2 años
				Modificación	0 veces en 2 años
				Pérdida	0 veces en 2 años
				Interrupción	0 veces en 2 años
			Problemas con sistemas de terceros	Revelación	0 veces en 2 años
				Modificación	0 veces en 2 años
				Pérdida	0 veces en 2 años
				Interrupción	0 veces en 2 años
			Desastres naturales	Revelación	0 veces en 2 años
				Modificación	0 veces en 2 años
				Pérdida	0 veces en 2 años
				Interrupción	0 veces en 2 años

Problemas con el suministro de energía	
De ejemplos de cómo cualquier problema con el suministro de energía podría ser considerado una amenazar el sistema.	Cuando hay corte de energía eléctrica, un motor entra en funcionamiento. Pero el combustible de dicho motor se termina y los servidores se apagan.

Problemas de telecomunicaciones	
De ejemplos de cómo cualquier problema de telecomunicaciones podría ser considerado una amenazar el sistema.	

Problemas con sistemas de terceros	
De ejemplos de cómo cualquier problema con sistemas de terceros podría ser considerado una amenazar el sistema.	

Desastres naturales	
De ejemplos de algún desastre natural podría ser considerado una amenazar el sistema.	

Fuente: Elaborado por los autores en base a Alberts, Christopher. OCTAVE-S Implementation Guide, Versión 1.0.

5.2.2. Fase 2: Identificar las vulnerabilidades de la infraestructura tecnológica.

5.2.1.1. Proceso S3: Examinar la infraestructura informática en relación con los activos críticos

a. S 3.1 Examinar rutas de acceso

Tabla 54: Rutas de acceso

SISTEMA DE INTERÉS
¿Qué sistema o sistemas están más estrechamente relacionados con el activo crítico?
Gestión de Actas virtuales y matricula online

SISTEMA DE INTERÉS	PUNTOS DE ACCESO INTERMEDIOS	ACCESO AL SISTEMA POR INDIVIDUOS	UBICACIÓN DE DONDE SE ALMACENAN	OTROS SISTEMAS O COMPONENTES
¿Cuál de las siguientes clases de componentes son parte del sistema de interés?	¿Cuál de las siguientes clases de componentes se utilizan para transmitir información y aplicaciones desde el sistema de interés hacia la gente? ¿Cuál de las siguientes clases de componentes podría servir como un punto de acceso intermedio?	¿De cuál de las siguientes clases de componentes puede la gente (por ejemplo, los usuarios, los atacantes) acceder al sistema de interés? Considere puntos de acceso internos	¿En qué clase de componente esta la información del sistema de interés almacenada por motivos de respaldo?	¿Cuál otro sistema accede a información del sistema de interés?
X **Servidores** Servidor de base de datos	x **Redes internas** Switch y comunicaciones en la Universidad	X **Estaciones de Trabajo** Computadoras de la Universidad	X **Dispositivos de almacenamiento de respaldos locales** Cintas magnéticas	Servidor de base de datos
Redes internas Switch y comunicaciones en la Universidad	X **Redes externas** Alumnos matriculándose	X **Laptops** Laptops de administrativos o alumnos	**Otros (Lista)**	
x **Estaciones de trabajo** Computadoras de la Universidad	**Otros (Lista)**	**PDAs/Componentes Wireless**		
Otros (Lista)		X **Estaciones de Trabajo fuera de la oficina** Acceso a la red desde afuera de la Universidad		
		Otros (Lista)		

Fuente: Elaborado por los autores en base a Alberts, Christopher. OCTAVE-S Implementation Guide, Versión 1.0.

b. S 3.2 Analizar procesos relacionados con la tecnología

Tabla 55: Procesos relacionados con la tecnología

CLASE	ACTIVO CRÍTICO				RESPONSABILIDAD
	[swsc]	[ser3]	[fire]	[adm1]	
Servidores					
Servidor de base de datos	x	x	x	x	Área de Tecnología
Servidor de base de datos backup	x	x			Área de Tecnología
Estaciones de trabajo					
Administrador	x	x	x		Área de Tecnología
Practicantes			x		Área de Tecnología
Redes internas					
Todos	x	x	x	x	Área de Tecnología
Redes externas					
Todos	x				Área de Tecnología
Laptops/Computadoras					
Administrador	x	x	x		Área de Tecnología
Usuarios	x				Área de Tecnología
Practicantes de TI			x		Área de Tecnología
Estaciones de trabajo fuera de la oficina.					
Administrador	x				Área de Tecnología
Usuarios	x				Área de Tecnología
Dispositivos de almacenamiento de respaldos locales					
Storage de respaldo de BD	x	x		x	Área de Tecnología
Servidor de base de datos	x	x		x	Área de Tecnología

Fuente: Elaborado por los autores en base a Alberts, Christopher. OCTAVE-S Implementation Guide, Versión 1.0.

5.2.1.2. Proceso S4: Identificar y analizar los riesgos.

Tabla 56: Hoja de trabajo de perfil de riesgo para Gestión de Actas virtuales y matricula online - Actores humanos que utilizan el acceso a la red

AMENAZA					IMPACTO				
ACTIVO	ACCESO	ACTOR	MOTIVO	RESULTADO	REPUTACIÓN	PRODUCTIVIDAD	MULTAS Y PENAS LEGALES	SEGURIDAD	FINANCIERA
Gestión de Actas virtuales y matricula online	Red	Adentro	Accidental	Revelación	bajo	bajo	bajo	bajo	bajo
				Modificación	medio	bajo	bajo	bajo	bajo
				Pérdida	bajo	bajo	bajo	bajo	bajo
				Interrupción	medio	bajo	bajo	bajo	bajo
			Intencionado	Revelación	bajo	bajo	bajo	bajo	bajo
				Modificación	bajo	medio	bajo	bajo	bajo
				Pérdida	bajo	bajo	bajo	bajo	bajo
				Interrupción	bajo	bajo	bajo	bajo	bajo
		Afuera	Accidental	Revelación	bajo	bajo	bajo	bajo	bajo
				Modificación	bajo	medio	bajo	bajo	bajo
				Pérdida	bajo	medio	bajo	bajo	bajo
				Interrupción	bajo	medio	bajo	bajo	bajo
			Intencionado	Revelación	bajo	bajo	bajo	bajo	bajo
				Modificación	bajo	medio	bajo	bajo	bajo
				Pérdida	bajo	bajo	bajo	bajo	bajo
				Interrupción	bajo	bajo	bajo	bajo	bajo

Fuente: Elaborado por los autores en base a Alberts, Christopher. OCTAVE-S Implementation Guide, Versión 1.0.

Tabla 57: Hoja de trabajo de perfil de riesgo para Gestión de Actas virtuales y matricula online - actores humanos que utilizan el acceso físico

AMENAZA					IMPACTO				
ACTIVO	**ACCESO**	**ACTOR**		**RESULTADO**	REPUTACIÓN	PRODUCTIVIDAD	MULTAS Y PENAS LEGALES	SEGURIDAD	FINANCIERA
Gestión de Actas virtuales y matricula online	Físico	Adentro	Accidental	Revelación	bajo	bajo	bajo	bajo	bajo
				Modificación	medio	bajo	bajo	bajo	bajo
				Pérdida	bajo	bajo	bajo	bajo	bajo
				Interrupción	medio	bajo	bajo	bajo	bajo
			Intencionado	Revelación	bajo	bajo	bajo	bajo	bajo
				Modificación	bajo	medio	bajo	bajo	bajo
				Pérdida	bajo	bajo	bajo	bajo	bajo
				Interrupción	bajo	bajo	bajo	bajo	bajo
		Afuera	Accidental	Revelación	bajo	bajo	bajo	bajo	bajo
				Modificación	bajo	medio	bajo	bajo	bajo
				Pérdida	bajo	medio	bajo	bajo	bajo
				Interrupción	bajo	medio	bajo	bajo	bajo
			Intencionado	Revelación	bajo	bajo	bajo	bajo	bajo
				Modificación	bajo	medio	bajo	bajo	bajo
				Pérdida	bajo	bajo	bajo	bajo	bajo
				Interrupción	bajo	bajo	bajo	bajo	bajo

Fuente: Elaborado por los autores en base a Alberts, Christopher. OCTAVE-S Implementation Guide, Versión 1.0.

Tabla 58: Hoja de trabajo de perfil de riesgo para Gestión de Actas virtuales y matricula online - Problemas del sistema

AMENAZAS					IMPACTO				
ACTIVO	**ACCESO**	**ACTOR**		**RESULTADO**	REPUTACIÓN	PRODUCTIVIDAD	MULTAS Y PENAS LEGALES	SEGURIDAD	FINANCIERA
Gestión de Actas virtuales y matricula online			Defectos de software	Revelación	bajo	bajo	bajo	bajo	bajo
				Modificación	medio	bajo	bajo	bajo	bajo
				Pérdida	bajo	bajo	bajo	bajo	bajo
				Interrupción	medio	bajo	bajo	bajo	bajo
			El sistema se cae	Revelación	bajo	bajo	bajo	bajo	bajo
				Modificación	bajo	medio	bajo	bajo	bajo
				Pérdida	bajo	bajo	bajo	bajo	bajo
				Interrupción	bajo	bajo	bajo	bajo	bajo
			Defectos de hardware	Revelación	bajo	bajo	bajo	bajo	bajo
				Modificación	bajo	medio	bajo	bajo	bajo
				Pérdida	bajo	medio	bajo	bajo	bajo
				Interrupción	bajo	medio	bajo	bajo	bajo
			Código malicioso	Revelación	bajo	bajo	bajo	bajo	bajo
				Modificación	bajo	medio	bajo	bajo	bajo
				Pérdida	bajo	bajo	bajo	bajo	bajo
				Interrupción	bajo	bajo	bajo	bajo	bajo

Fuente: Elaborado por los autores en base a Alberts, Christopher. OCTAVE-S Implementation Guide, Versión 1.0.

Tabla 59: Hoja de trabajo de perfil de riesgo para Gestión de Actas virtuales y matricula online- Otros problemas

AMENAZAS					IMPACTO				
ACTIVO	**ACCESO**	**ACTOR**		**RESULTADO**	REPUTACIÓN	PRODUCTIVIDAD	MULTAS Y PENAS LEGALES	SEGURIDAD	FINANCIERA
Gestión de Actas virtuales y matricula online			Problemas con el suministro de energía	Revelación	bajo	bajo	bajo	bajo	bajo
				Modificación	medio	bajo	bajo	bajo	bajo
				Pérdida	bajo	bajo	bajo	bajo	bajo
				Interrupción	medio	bajo	bajo	bajo	bajo
			Problemas de telecomunicaciones	Revelación	bajo	bajo	bajo	bajo	bajo
				Modificación	bajo	medio	bajo	bajo	bajo
				Pérdida	bajo	bajo	bajo	bajo	bajo
				Interrupción	bajo	bajo	bajo	bajo	bajo
			Problemas con sistemas de terceros	Revelación	bajo	bajo	bajo	bajo	bajo
				Modificación	bajo	medio	bajo	bajo	bajo
				Pérdida	bajo	medio	bajo	bajo	bajo
				Interrupción	bajo	medio	bajo	bajo	bajo
			Desastres naturales	Revelación	bajo	bajo	bajo	bajo	bajo
				Modificación	bajo	medio	bajo	bajo	bajo
				Pérdida	bajo	bajo	bajo	bajo	bajo
				Interrupción	bajo	bajo	bajo	bajo	bajo

Fuente: Elaborado por los autores en base a Alberts, Christopher. OCTAVE-S Implementation Guide, Versión 1.0.

5.2.1.3. Evaluar Probabilidades de amenazas

Tabla 60: Hoja de trabajo de perfil de riesgo para Sistema académico actas virtuales UNPRG - Actores humanos que utilizan el acceso a la red

AMENAZA						VALOR	CONFIANZA		
ACTIVO	**ACCESO**	**ACTOR**	**MOTIVO**		**RESULTADO**		MUY	ALGO	NADA
Gestión de Actas virtuales y matricula online	Red	Adentro	Accidental		Revelación	bajo		x	
					Modificación	medio	x		
					Pérdida	bajo		x	
					Interrupción	medio		x	
			Intencionado		Revelación	bajo		x	
					Modificación	medio		x	
					Pérdida	bajo		x	
					Interrupción	medio		x	
		Afuera	Accidental		Revelación	bajo		x	
					Modificación	medio		x	
					Pérdida	bajo		x	
					Interrupción	medio		x	
			Intencionado		Revelación	bajo		x	
					Modificación	medio		x	
					Pérdida	bajo		x	
					Interrupción	medio		x	

Fuente: Elaborado por los autores en base a Alberts, Christopher. OCTAVE-S Implementation Guide, Versión 1.0

Tabla 61: Hoja de trabajo de perfil de riesgo para Gestión de Actas virtuales y matricula online - actores humanos que utilizan el acceso físico

AMENAZA						VALOR	CONFIANZA		
ACTIVO	**ACCESO**	**ACTOR**	**MOTIVO**		**RESULTADO**		MUY	ALGO	NADA
Gestión de Actas virtuales y matricula online	Físico	Adentro	Accidental		Revelación	muy bajo	x		
					Modificación	muy bajo	x		
					Pérdida	muy bajo	x		
					Interrupción	muy bajo	x		
			Intencionado		Revelación	muy bajo	x		
					Modificación	muy bajo	x		
					Pérdida	muy bajo	x		
					Interrupción	muy bajo	x		
		Afuera	Accidental		Revelación	muy bajo	x		
					Modificación	muy bajo	x		
					Pérdida	muy bajo	x		
					Interrupción	muy bajo	x		
			Intencionado		Revelación	muy bajo	x		
					Modificación	muy bajo	x		
					Pérdida	muy bajo	x		
					Interrupción	muy bajo	x		

Fuente: Elaborado por los autores en base a Alberts, Christopher. OCTAVE-S Implementation Guide, Versión 1.0

Tabla 62: Hoja de trabajo de perfil de riesgo para Gestión de Actas virtuales y matricula online - Problemas del sistema

AMENAZAS						VALOR	CONFIANZA		
ACTIVO	**ACCESO**	**ACTOR**	**MOTIVO**		**RESULTADO**		MUY	ALGO	NADA
Gestión de Actas virtuales y matricula online			Defectos de software		Revelación	bajo		x	
					Modificación	bajo		x	
					Pérdida	bajo		x	
					Interrupción	medio		x	
			El sistema se cae		Revelación	bajo		x	
					Modificación	bajo		x	
					Pérdida	bajo		x	
					Interrupción	medio		x	
			Defectos de hardware		Revelación	bajo		x	
					Modificación	bajo		x	
					Pérdida	bajo		x	
					Interrupción	medio		x	
			Código malicioso		Revelación	bajo		x	
					Modificación	bajo		x	
					Pérdida	bajo		x	
					Interrupción	medio		x	

Fuente: Elaborado por los autores en base a Alberts, Christopher. OCTAVE-S Implementation Guide, Versión 1.0

Tabla 63: Hoja de trabajo de perfil de riesgo para Gestión de Actas virtuales y matricula online- Otros problemas

AMENAZAS						VALOR	CONFIANZA		
ACTIVO	**ACCESO**	**ACTOR**	**MOTIVO**		**RESULTADO**		MUY	ALGO	NADA
Gestión de Actas virtuales y matricula online			Problemas con el suministro de energía		Revelación	bajo		x	
					Modificación	bajo		x	
					Pérdida	bajo		x	
					Interrupción	bajo		x	
			Problemas de telecomunicaciones		Revelación	bajo		x	
					Modificación	bajo		x	
					Pérdida	bajo		x	
					Interrupción	bajo		x	
			Problemas con sistemas de terceros		Revelación	bajo		x	
					Modificación	bajo		x	
					Pérdida	bajo		x	
					Interrupción	bajo		x	
			Desastres naturales		Revelación	bajo		x	
					Modificación	bajo		x	
					Pérdida	bajo		x	
					Interrupción	bajo		x	

Fuente: Elaborado por los autores en base a Alberts, Christopher. OCTAVE-S Implementation Guide, Versión 1.0

5.2.2. Fase 3: Desarrollar estrategias y planes de seguridad

5.2.3.1. Proceso S5: Desarrollar estrategias de protección y planes de mitigación

a. S5.1 Describir la estrategia de protección actual

Tabla 64: Estrategias de protección - Conocimiento de seguridad y entrenamiento

1. Conocimiento de seguridad y entrenamiento

ESTRATEGIA DE CAPACITACIÓN	
¿Qué tan formal es la estrategia de capacitación de su organización? ¿Quiere hacer cambios adicionales a su estrategia de capacitación?	
La organización cuenta con una estrategia de capacitación documentada que incluye una evaluación del conocimiento de seguridad para la sensibilización y la formación en materia de seguridad para las tecnologías de apoyo.	Actual
La organización tiene una estrategia de capacitación informal e indocumentada.	Actual

EVALUAR EL CONOCIMIENTO DE SEGURIDAD	
¿Qué tan seguido se realizan entrenamientos de seguridad? ¿Quiere hacer cambios adicionales a su estrategia de capacitación?	
Se proveen entrenamientos periódicos sobre seguridad que a todos los empleados 1 vez cada año.	Actual
Se provee entrenamiento sobre seguridad a personas nuevas en la organización como parte de sus actividades de orientación.	Actual
La organización no provee un entrenamiento sobre seguridad. Cada miembro del personal aprende sobre problemas de seguridad por sí mismo.	Actual

ENTRENAMIENTO RELACIONADO CON SEGURIDAD	
¿En qué medida se requiere que los miembros del área de TI asistan a un entrenamiento relacionado con seguridad? ¿Quiere hacer cambios adicionales a su estrategia de capacitación?	
Los miembros del área de TI deben asistir a entrenamientos relacionados con seguridad para cualquier tecnología que utilicen.	Actual
Los miembros del área de TI pueden asistir a entrenamientos relacionados con seguridad para cualquier tecnología que utilicen si ellos lo piden.	Actual
La organización no provee oportunidades para que miembros del área de TI asistan a entrenamientos relacionados con seguridad para cualquier tecnología que utilicen.	Actual

ACTUALIZACIONES PERIÓDICAS DE SEGURIDAD	
¿Qué tan formal es el mecanismo de su organización para proveer actualizaciones periódicas de seguridad? ¿Quiere hacer cambios adicionales a su estrategia de capacitación?	
La organización tiene mecanismos formales para proveer miembros del personal con actualizaciones periódicas / boletines sobre problemas de seguridad importantes.	Actual
La organización no tiene un mecanismo para proveer a miembros del personal con actualizaciones periódicas / boletines sobre problemas de seguridad importantes.	Actual

VERIFICACIÓN DEL ENTRENAMIENTO	
¿Cuál es el mecanismo oficial de su organización para verificar que el personal reciba capacitación? ¿Quiere hacer cambios adicionales a su estrategia de capacitación?	
La organización tiene mecanismos formales para rastrear y verificar que los miembros del personal reciban entrenamiento sobre seguridad apropiado.	Actual
La organización tiene mecanismos informales para rastrear y verificar que los miembros del personal reciban entrenamiento sobre seguridad apropiado.	Actual
La organización no tiene mecanismos para rastrear y verificar que los miembros del personal reciban entrenamiento sobre seguridad apropiado.	Actual

Fuente: Elaborado por los autores en base a Alberts, Christopher. OCTAVE-S Implementation Guide, Versión 1.0.

Tabla 65: Estrategias de protección para el manejo colaborativo de la seguridad.

2. Estrategia de protección para el manejo colaborativo de la seguridad

COLABORADORES Y SOCIOS	
¿Qué tan formales son las políticas y procedimientos de su organización para proteger la información cuando se trabaja con colaboradores y socios? ¿Quiere hacer cambios adicionales a su estrategia de capacitación?	
La organización tiene políticas y procedimientos documentados para proteger la información cuando se trabaja con colaboradores y socios.	Actual
La organización tiene políticas y procedimientos documentados para proteger cierta la información cuando se trabaja con colaboradores y socios. La organización tiene políticas y procedimientos no documentados para proteger otros tipos de información cuando se trabaja con colaboradores y socios.	Actual
La organización tiene políticas y procedimientos informales y no documentados para proteger la información cuando se trabaja con colaboradores y socios.	Actual

CONTRATISTAS Y SUBCONTRATISTAS	
¿Qué tan formales son las políticas y procedimientos de su organización para proteger la información cuando se trabaja con contratistas y subcontratistas? ¿Quiere hacer cambios adicionales a su estrategia de capacitación?	
La organización tiene políticas y procedimientos documentados para proteger la información cuando se trabaja con contratistas y subcontratistas.	Actual
	Actual

La organización tiene políticas y procedimientos documentados para proteger cierta la información cuando se trabaja con contratistas y subcontratistas. La organización tiene políticas y procedimientos no documentados para proteger otros tipos de información cuando se trabaja con contratistas y subcontratistas.	
La organización tiene políticas y procedimientos informales y no documentados para proteger la información cuando se trabaja con contratistas y subcontratistas.	Actual

PROVEEDORES DE SERVICIOS	
¿Qué tan formales son las políticas y procedimientos de su organización para proteger la información cuando se trabaja con proveedores de servicios? ¿Quiere hacer cambios adicionales a su estrategia de capacitación?	
La organización tiene políticas y procedimientos documentados para proteger la información cuando se trabaja con proveedores de servicios.	Actual
La organización tiene políticas y procedimientos documentados para proteger cierta la información cuando se trabaja con proveedores de servicios. La organización tiene políticas y procedimientos no documentados para proteger otros tipos de información cuando se trabaja con proveedores de servicios.	Actual
La organización tiene políticas y procedimientos informales y no documentados para proteger la información cuando se trabaja con proveedores de servicios.	Actual

REQUERIMIENTOS	
¿Hasta qué punto la organización comunica formalmente sus requisitos de protección de la información a terceras partes? ¿Quiere hacer cambios adicionales a su estrategia de capacitación?	
La organización documenta los requisitos de protección de la información y las comunica explícitamente a terceras partes.	Actual
La organización comunica informalmente los requisitos de protección de información a terceras partes.	Actual
La organización no comunica sus requisitos de protección de información a terceras partes.	Actual

VERIFICACIÓN	
¿Hasta qué punto la organización verifica que terceras partes estén cumpliendo con los requisitos de protección de seguridad? ¿Quiere hacer cambios adicionales a su estrategia de capacitación?	
La organización tiene mecanismos formales para verificar que organizaciones de terceros, servicios de seguridad externos, mecanismos y tecnologías cumplan con sus requerimientos.	Actual
La organización tiene mecanismos informales para verificar que organizaciones de terceros, servicios de seguridad externos, mecanismos y tecnologías cumplan con sus requerimientos.	Actual
La organización no tiene mecanismos formales para verificar que organizaciones de terceros, servicios de seguridad externos, mecanismos y tecnologías cumplan con sus requerimientos.	Actual

CONOCIMIENTO DEL PERSONAL	
¿Hasta qué punto el programa de entrenamiento sobre conocimiento de seguridad de su organización incluye manejo colaborativo de seguridad? ¿Quiere hacer cambios adicionales a su estrategia de capacitación?	
El programa de entrenamiento sobre conocimiento de seguridad de la organización incluye información sobre el manejo colaborativo de seguridad, políticas y procedimientos. Este entrenamiento se da a todos los empleados 1 vez cada año.	Actual
	Actual

El programa de entrenamiento sobre conocimiento de seguridad de la organización incluye información sobre el manejo colaborativo de seguridad, políticas y procedimientos. Este entrenamiento se da a los nuevos empleados como parte de sus actividades de orientación.	
El programa de entrenamiento sobre conocimiento de seguridad de la organización no incluye información sobre el manejo colaborativo de seguridad, políticas y procedimientos. Este entrenamiento se da a todos los empleados 1 vez cada año. Los miembros del personal aprenden sobre manejo colaborativo de la seguridad por si mismos.	Actual

Fuente: Elaborado por los autores en base a Alberts, Christopher. OCTAVE-S Implementation Guide, Versión 1.0.

Tabla 66: Estrategia de protección para monitorear y auditar seguridad física

3. Estrategia de protección para monitorear y auditar seguridad física

RESPONSABILIDAD			
¿Quién es actualmente responsable para monitorear y auditar la seguridad física? ¿Quiere hacer cambios adicionales a su estrategia de capacitación?			
Tarea:	Actual		
	Interno	Externo	Combinado
Mantener registros de mantenimiento para documentar reparaciones y modificaciones al hardware.	X		
Monitorear acceso físico controlado por hardware.	X		
Monitorear acceso físico controlado por software.	X		
Monitorear acceso físico a áreas de trabajo restringidas.	X		
Revisar los registros de monitoreo periódicamente.	X		
Investigar y monitorear cualquier actividad inusual no identificada.	X		

PROCEDIMIENTOS	
¿Hasta qué punto son los procedimientos de esta área formalmente documentados? ¿Quiere hacer cambios adicionales a su estrategia de capacitación?	
Si el personal de su organización es parcial o completamente responsable por esta área:	
La organización ha documentado formalmente planes y procedimientos para monitorear acceso físico al edificio, áreas de trabajo, hardware y software.	Actual
La organización ha documentado formalmente algunos planes y procedimientos para monitorear acceso físico al edificio, áreas de trabajo, hardware y software. Algunas políticas y procedimientos son informales y no son documentados.	Actual
La organización tiene planes y procedimientos para monitorear acceso físico al edificio, áreas de trabajo, hardware y software que son informales y no documentados.	Actual

ENTRENAMIENTO	
¿Hasta qué punto se requiere que el personal de su organización asista a entrenamientos en esta área? ¿Quiere hacer cambios adicionales a su estrategia de capacitación?	
Si el personal de su organización es parcial o completamente responsable por esta área:	
Miembros designados del personal están obligados a asistir a entrenamientos para monitorear acceso físico al edificio, áreas de trabajo, hardware y software.	Actual
Miembros designados del personal pueden asistir a entrenamientos para monitorear acceso físico al edificio, áreas de trabajo, hardware y software si ellos lo piden.	Actual

La organización generalmente no provee oportunidades para que miembros designados del personal asistan a entrenamientos para monitorear acceso físico al edificio, áreas de trabajo, hardware y software.	Actual

Fuente: Elaborado por los autores en base a Alberts, Christopher. OCTAVE-S Implementation Guide, Versión 1.0.

Tabla 67: Estrategia de protección para autenticación y autorización

4. Estrategia de protección para autenticación y autorización

RESPONSABILIDAD			
¿Quién es actualmente responsable de la autenticación y autorización? ¿Quiere hacer cambios adicionales a su estrategia de capacitación?			
Tarea:	Actual		
	Interno	Externo	Combinado
Implementar control de acceso (permisos de archivos, configuración de la red) para restringir a usuarios acceso a información, sistemas susceptibles, aplicaciones y servicios específicos y conexiones de red.	X		
Implementar autenticación de usuarios (permisos de archivos, configuración de la red) para restringir a usuarios acceso a información, sistemas susceptibles, aplicaciones y servicios específicos y conexiones de red.	X		
Establecer y terminar acceso a sistemas e información para ambos individuos y grupos.	X		

PROCEDIMIENTOS	
¿Hasta qué punto están formalmente documentados los procesos en esta área? ¿Quiere hacer cambios adicionales a su estrategia de capacitación?	
Si el personal de su organización es parcial o completamente responsable por esta área:	
La organización ha documentado formalmente autorización y autenticación de procedimientos para restringir a usuarios acceso a información, sistemas susceptibles, aplicaciones y servicios específicos y conexiones de red.	Actual
La organización ha documentado formalmente autorización y autenticación de algunos procedimientos para restringir a usuarios acceso a información, sistemas susceptibles, aplicaciones y servicios específicos y conexiones de red. Algunos procedimientos en esta área son informales y no están documentados.	Actual
La organización tiene procedimientos informales y no documentados para la autorización y autenticación de procedimientos para restringir a usuarios acceso a información, sistemas susceptibles, aplicaciones y servicios específicos y conexiones de red.	Actual

ENTRENAMIENTO	
¿Hasta qué punto están formalmente documentados los procesos en esta área? ¿Quiere hacer cambios adicionales a su estrategia de capacitación?	
Si el personal de su organización es parcial o completamente responsable por esta área:	
Miembros designados del personal están obligados a asistir a entrenamientos para implementar medidas tecnológicas para restringir a usuarios acceso a información, sistemas susceptibles, aplicaciones y servicios específicos y conexiones de red.	Actual
Miembros designados del personal pueden asistir a entrenamientos para restringir a usuarios acceso a información, sistemas susceptibles, aplicaciones y servicios específicos y conexiones de red si ellos lo piden.	Actual
La organización generalmente no provee oportunidades para que miembros designados del personal asistan a entrenamientos para restringir a usuarios acceso a información, sistemas susceptibles, aplicaciones y servicios específicos y conexiones de red.	Actual

Fuente: Elaborado por los autores en base a Alberts, Christopher. OCTAVE-S Implementation Guide, Versión 1.0.

b. S5.2 Seleccionar enfoques de mitigación

Tabla 68: Hoja de trabajo de perfil de riesgo para Sistema académico actas virtuales UNPRG - Actores humanos que utilizan el acceso a la red

AMENAZA					ÁREAS DE PRÁCTICA DE SEGURIDAD															ENFOQUE		
Activo	Acceso	Actor	Motivo	Resultado	Estratégica						Operacional											
					1. Co nci	2. Est rate	3. Ges tión	4. Polí tica	5. Ges tión	6. Pla nes de	7. Co	8. Mo nito reo	9. Ges tión	10. Mo nito reo	11. Aut enti	12. Ges tión de	13. Enc rist	14. Dis eño	15. Ges tión	Ac ept	Apl aza	Mit iga
Sistema académico actas virtuales UNPRG	Red	Adentro	Accidental	Revelación	Y	R	R	R	R	R			R	R	Y	R	Y	R	R	x		
				Modificación	Y	R	R	R	R	R			R	R	Y	R	Y	R	R	x		
				Pérdida	Y	R	R	R	R	R			R	R	Y	R	Y	R	R	x		
				Interrupción	Y	R	R	R	R	R			R	R	Y	R	Y	R	R	x		
			Intencionado	Revelación	Y	R	R	R	R	R			R	R	Y	R	Y	R	R			
				Modificación	Y	R	R	R	R	R			R	R	Y	R	Y	R	R			
				Pérdida	Y	R	R	R	R	R			R	R	Y	R	Y	R	R			
				Interrupción	Y	R	R	R	R	R			R	R	Y	R	Y	R	R			
		Afuera	Accidental	Revelación	Y	R	R	R	R	R			R	R	Y	R	Y	R	R			
				Modificación	Y	R	R	R	R	R			R	R	Y	R	Y	R	R			
				Pérdida	Y	R	R	R	R	R			R	R	Y	R	Y	R	R			
				Interrupción	Y	R	R	R	R	R			R	R	Y	R	Y	R	R			
			Intencionado	Revelación	Y	R	R	R	R	R			R	R	Y	R	Y	R	R	x		
				Modificación	Y	R	R	R	R	R			R	R	Y	R	Y	R	R	x		
				Pérdida	Y	R	R	R	R	R			R	R	Y	R	Y	R	R	x		
				Interrupción	Y	R	R	R	R	R			R	R	Y	R	Y	R	R	x		

Fuente: Elaborado por los autores en base a Alberts, Christopher. OCTAVE-S Implementation Guide, Versión 1.0.

Tabla 69: Hoja de trabajo de perfil de riesgo para Sistema académico actas virtuales UNPRG - actores humanos que utilizan el acceso físico

AMENAZA					ÁREAS DE PRÁCTICA DE SEGURIDAD														ENFOQUE		
Activo	Acceso	Actor	Motivo	Resultado	Estratégica						Operacional										
					1. Concienciación y Formación en Seguridad	2. Estrategia de Seguridad.	3. Gestión de Seguridad.	4. Políticas y regulaciones de Seguridad.	5. Gestión de la Seguridad Colaborativa.	6. Planes de Contingencia/Recuperación de Desastres.	7. Control de Acceso Físico.	8. Monitoreo y Auditoría de Seguridad Física	9. Gestión de Sistemas y Redes.	10. Monitoreo y Auditoría de Seguridad de TI.	11. Autenticación y Autorización.	12. Gestión de Vulnerabilidades.	13. Encriptación.	14. Diseño y Arquitectura de Seguridad.	15. Gestión de Incidentes.	Aceptar	Aplazar	Mitigar
Sistema académico actas virtuales UNPRG	Físico	Adentro	Accidental	Revelación	Y	R	R	R	R	R	R	R						R	R			
				Modificación	Y	R	R	R	R	R	R	R						R	R			
				Pérdida	Y	R	R	R	R	R	R	R						R	R			
				Interrupción	Y	R	R	R	R	R	R	R						R	R			
			Intencionado	Revelación	Y	R	R	R	R	R	R	R						R	R			
				Modificación	Y	R	R	R	R	R	R	R						R	R			
				Pérdida	Y	R	R	R	R	R	R	R						R	R			
				Interrupción	Y	R	R	R	R	R	R	R						R	R			
		Afuera	Accidental	Revelación	Y	R	R	R	R	R	R	R						R	R			
				Modificación	Y	R	R	R	R	R	R	R						R	R			
				Pérdida	Y	R	R	R	R	R	R	R						R	R			
				Interrupción	Y	R	R	R	R	R	R	R						R	R			
			Intencionado	Revelación	Y	R	R	R	R	R	R	R						R	R			
				Modificación	Y	R	R	R	R	R	R	R						R	R			
				Pérdida	Y	R	R	R	R	R	R	R						R	R			
				Interrupción	Y	R	R	R	R	R	R	R						R	R			

Fuente: Elaborado por los autores en base a Alberts, Christopher. OCTAVE-S Implementation Guide, Versión 1.0.

Tabla 70: Hoja de trabajo de perfil de riesgo para Sistema académico actas virtuales UNPRG - Problemas del sistema

AMENAZA					ÁREAS DE PRÁCTICA DE SEGURIDAD														ENFOQUE		
Activo	Acceso	Actor	Motivo	Resultado	Estratégica						Operacional										
					1. Concienciación y Formación en Seguridad	2. Estrategia de Seguridad.	3. Gestión de Seguridad.	4. Políticas y regulaciones de Seguridad.	5. Gestión de la Seguridad Colaborativa.	6. Planes de Contingencia/Recuperación de Desastres.	7. Control de Acceso Físico.	8. Monitoreo y Auditoría de Seguridad Física.	9. Gestión de Sistemas y Redes.	10. Monitoreo y Auditoría de Seguridad de TI.	11. Autenticación y Autorización.	12. Gestión de Vulnerabilidades.	13. Encriptación.	14. Diseño y Arquitectura de Seguridad.	15. Gestión de Incidentes.	Aceptar	Aplazar	Mitigar
Sistema académico actas virtuales UNPRG			Defectos de software	Revelación	Y	R	R	R	R	R			R	R		R		R	R			
				Modificación	Y	R	R	R	R	R			R	R		R		R	R			
				Pérdida	Y	R	R	R	R	R			R	R		R		R	R			
				Interrupción	Y	R	R	R	R	R			R	R		R		R	R			
			El sistema se cae	Revelación	Y	R	R	R	R	R			R	R	Y	R		R	R			
				Modificación	Y	R	R	R	R	R			R	R	Y	R		R	R			
				Pérdida	Y	R	R	R	R	R			R	R	Y	R		R	R			
				Interrupción	Y	R	R	R	R	R			R	R	Y	R		R	R	x		
			Defectos de hardware	Revelación	Y	R	R	R	R	R			R	R		R		R	R			
				Modificación	Y	R	R	R	R	R			R	R		R		R	R			
				Pérdida	Y	R	R	R	R	R			R	R		R		R	R			
				Interrupción	Y	R	R	R	R	R			R	R		R		R	R			
			Código malicioso	Revelación	Y	R	R	R	R	R			R	R	Y	R		R	R			
				Modificación	Y	R	R	R	R	R			R	R	Y	R		R	R			
				Pérdida	Y	R	R	R	R	R			R	R	Y	R		R	R			
				Interrupción	Y	R	R	R	R	R			R	R	Y	R		R	R			

Fuente: Elaborado por los autores en base a Alberts, Christopher. OCTAVE-S Implementation Guide, Versión 1.0.

Tabla 71: Hoja de trabajo de perfil de riesgo para Sistema académico actas virtuales UNPRG- Otros problemas

AMENAZA					ÁREAS DE PRÁCTICA DE SEGURIDAD															ENFOQUE		
Activo	Acceso	Actor	Motivo	Resultado	Estratégica						Operacional											
					1. Concienciación y Formación en Seguridad	2. Estrategia de Seguridad.	3. Gestión de Seguridad.	4. Políticas y regulaciones de	5. Gestión de la Seguridad Colaborativa.	6. Planes de Contingencia/Recuperación de Desastres.	7. Control de Acceso Físico.	8. Monitoreo y Auditoría de Seguridad Física	9. Gestión de Sistemas y Redes.	10. Monitoreo y Auditoría de Seguridad de TI.	11. Autenticación y Autorización.	12. Gestión de Vulnerabilidades.	13. Encriptación.	14. Diseño y Arquitectura de Seguridad.	15. Gestión de Incidentes.	Aceptar	Aplazar	Mitigar
Sistema académico actas virtuales UNPRG		Problemas con el suministro de energía	Revelación		Y	R	R	R	R	R	R	R							R			
			Modificación		Y	R	R	R	R	R	R	R							R			
			Pérdida		Y	R	R	R	R	R	R	R							R			
			Interrupción		Y	R	R	R	R	R	R	R							R	x		
		Problemas de telecomunicaciones	Revelación		Y	R	R	R	R	R	R	R							R			
			Modificación		Y	R	R	R	R	R	R	R							R			
			Pérdida		Y	R	R	R	R	R	R	R							R			
			Interrupción		Y	R	R	R	R	R	R	R							R			
		Problemas con sistemas de terceros	Revelación		Y	R	R	R	R	R									R			
			Modificación		Y	R	R	R	R	R									R			
			Pérdida		Y	R	R	R	R	R									R			
			Interrupción		Y	R	R	R	R	R									R			
		Desastres naturales	Revelación		Y	R	R	R	R	R	R	R										
			Modificación		Y	R	R	R	R	R	R	R										
			Pérdida		Y	R	R	R	R	R	R	R										
			Interrupción		Y	R	R	R	R	R	R	R										

Fuente: Elaborado por los autores en base a Alberts, Christopher. OCTAVE-S Implementation Guide, Versión 1.0.

Como resultado de la evaluación de las amenazas en las prácticas de seguridad organización se optó por plantear un enfoque de mitigación de aceptación. Esto porque las amenazas identificadas en su mayoría no afectan en un impacto significativo a la Unidad de Red Telemática como organización y según el estudio realizado la Unidad puede realizar sus actividades y convivir con las amenazas identificadas.

5.3. Discusión general de la comparativa.

Luego de haberse aplicado las dos metodologías llegamos a las siguientes comparativas.

Tabla 72: Comparativa de las metodologías

METODOLOGÍA / VARIABLES	ACTIVOS	ESCENARIOS DE RIESGO	VALORACIÓN DE ESCENARIOS DE RIESGOS	NIVEL DE RIESGO	TRATAMIENTO DEL RIESGO
METODOLOGÍA MAGERIT	La metodología MAGERIT , para la identificación de los activos ya tiene un esquema plateado, como se nombró en el capítulo 3 del desarrollo metodológico, esta los agrupa en 8 capas, proporcionándoles un código , descripción del activo y el encargado del mismo; de los cuales la información y los servicios son los más importantes pero que a su vez están relacionados con otros activos, separándolos según su dependencia y	Amenazas: MAGERIT nos proporciona un catálogo de elementos de todas las amenazas que se consideran agrupándolas en 4 grupos (Desastres Naturales, Origen Industrial, Errores y Fallos no Intencionados, Ataques Intencionados), que puedan atacar a los activos. Cabe destacar que esa amenaza puede atacar al activo en una o más dimensiones	La metodología MAGETIR para la valoración de los escenarios de riesgos, lo realiza a través de dos factores, degradación del activo en caso la amenaza se materialice y la probabilidad de impacto que esta tiene en el activo. La degradación en porcentaje de se calcula en una escala de 5 niveles (muy bajo, bajo, medio, alto y muy alto)	MAGERIT, la obtención del riesgo se realiza mediante la multiplicación de impacto y la probabilidad de las amenazas. En el cual se puede identificar el nivel de riesgo que tenían los activos en caso las amenazas se materializaran. También a través de un mapa de calor nos ayuda a identificar cuál de los riegos es el más	MAGERIT, nos ofrece un catálogo de salvaguardas agrupadas en 8 grupos. Las cuales ya están definidas para proteger al activo que se vea en peligro por alguna amenaza.

	funcionamiento para luego valorarlos desde el punto de vista de proteger al activo en una determinada dimensión (Confidencialidad, Integridad ,Disponibilidad, autenticidad y Trazabilidad); utilizando criterios establecidos que nos permite saber que tan importante es proteger al activo en la organización.	mencionadas anteriormente. <u>Vulnerabilidades</u> MAGERIT, esta metodología evalúa las vulnerabilidades como las ineficiencias de las salvaguardas pertinentes para salvaguardar el valor propio o acumulado sobre el activo pero dada la delimitación del trabajo investigativo no se llega a evaluar la efectividad de las salvaguardas planteadas.	evaluando cuan desgastado se verá el activo en alguna de las 5 dimensiones en que este se evalúa. Para la probabilidad de impacto, que es la frecuencia con la que las amenazas atacan al activo (es anual) se evalúa en una escala de 5 niveles (muy poco frecuente, poco frecuente, normal, frecuente y muy frecuente).	crítico y se debería aplicar un tratamiento.	
METODOLOGÍA OCTAVE	La metodología OCTAVE-S, identifica los activos en dos grupos los cuales son Sistema, Información, Aplicaciones y servicios, y Personas. Después de esa identificación OCTAVE nos plantea evaluar las prácticas de seguridad organizacional a través de una encuesta con enunciados ya plantados respondiendo a preguntas como que está haciendo y que no	<u>Amenazas</u> OCTAVE ve las vulnerabilidades en la infraestuctura tecnológica de la organización. A través de pasos que nos ayudan a identificar los accesos, los responsables y activos relacionados a los activos críticos. <u>Vulnerabilidades</u> OCTAVE nos da una hoja de actividad en la cual a través de	OCTAVE valora las amenazas representadas en un árbol de amenazas que tiene el resultado en 4 valores (Revelación, Modificación, pérdida e interrupción) dicho árbol obtenido del catálogo de elementos, los actores de la amenaza y el motivo del actor de la amenaza y el nivel de	OCTAVE para evaluar el impacto de las amenazas, utiliza una hoja de trabajo en donde se utilizan los criterios establecidos en la fase 1, definiendo en 5 niveles (muy bajo, bajo, medio, alto y muy alto) el nivel de impacto que tienen las amenazas en los criterios establecidos.	OCTAVE se describen las estrategias de protección actual en la organización, y evalúa las áreas estratégica y operacional de la organización utilizando los prácticas de seguridad. Para llegar elegir el enfoque (Aceptar, aplazar y mitigar)

	está haciendo la organización. Después de eso OCTAVE nos sugiere elegir los 5 activos críticos para la organización de los cuales se detalla la razón del porque fueron elegidos, una breve descripción y los activos relacionados a dicho activo crítico. En base a ellos se sigue con el desarrollo de la metodología.	preguntas nos plantea cual sería la amenaza identificada en caso eso fuera a ocurrir , a través de los autores ya sean internos o externos.	confianza que se tiene del motivo, la historia de amenazas y el grado de confianza así como también ejemplos de las amenazas ocurridas.	También se estableces criterios de evaluación de probabilidad en 5 niveles (muy bajo, bajo, medio, alto y muy alto) , dependiendo la experiencia y el conocimiento de las amenazas que ocurrieron en la Unidad de Red Telemática así como también el nivel de confianza que se tiene al valorar la probabilidad de amenaza.	adecuado para dicha amenaza.

CAPÍTULO VI CONCLUSIONES Y RECOMENDACIONES

6.1. CONCLUSIONES

Siguiendo los procedimientos establecidos en cada uno de los marcos de referencia escogidos se concluye que:

- La metodología MAGERIT con su procedimiento técnico-operativo, procedimental; evalúa cada uno de los elementos que componen el Sistema de Gestión de Riesgos de TI que para MAGERIT son: activo, amenazas, impactos, frecuencias y salvaguardas. Para activos los procedimientos que se pueden observar son: Identificación, dependencias, y su valoración basada en las 5 dimensiones (Disponibilidad, Autenticidad, Confidencialidad, Integridad y Trazabilidad). Para amenazas se pueden observar los procedimientos de identificación y valoración a su vez nos proporciona el catálogo de amenazas. Para los impactos y frecuencias se determina una escala de valorización y para salvaguardas nos da un catálogo y una forma de cómo implementarlas. En el caso de la metodología OCTAVE su procedimiento tiene un enfoque corporativo, que evalúa cada uno de los elementos que componen el Sistema de Gestión de Riesgos de TI agrupados en Fases, Procedimientos y Actividades. La Fase 1: Construcción del perfil de amenazas basado en activos, abarcando los procesos de identificar información de la organización con actividades como establecer criterios de evaluación de impacto, identificación de activos organizacionales y evaluar prácticas de seguridad organizacional; y el proceso de crear perfil de amenazas con actividades como seleccionar activos críticos, identificar los requisitos de seguridad para los activos críticos e identificar amenazas a los activos críticos. La Fase 2: Identificar las vulnerabilidades de la infraestructura tecnológica con procedimientos como examinar la infraestructura informática en relación con los activos críticos con actividades como examinar rutas de acceso y analizar procesos relacionados con la tecnología. Por último, la Fase 3: Desarrollar estrategias y planes de seguridad como procesos como Identificar y analizar los riesgos con actividades como evaluar el impacto de las amenazas, establecer criterios de evaluación de probabilidad y evaluar probabilidades de amenazas y el proceso de Desarrollar estrategias de protección y planes de mitigación con actividades como describir la estrategia de protección actual y seleccionar enfoques de mitigación.

- La metodología MAGERIT nos llevó a determinar la criticidad de activos, los cuales determinan que hay activos como Sistema académico actas virtuales UNPRG, Servidor de base de datos, Acumulador de energía UPS, Sistema de aire acondicionado, Grupo electrógeno, Cableado de red, Fibra óptica, Data Center y Administrador del data center que son más críticos que otros. Con respecto a la identificación de amenazas el procedimiento ha determinado que las amenazas más críticas son Fuego, Corte de suministro, Fallo de servicios de comunicaciones, Caída del sistema por agotamiento de recursos, Denegación del servicio, Vulnerabilidades de los programas (software), Denegación del servicio, Escapes de información , Avería de origen físico o lógico, Condiciones inadecuadas de temperatura o humedad, Fallo de servicios de comunicaciones, Avería de origen físico o lógico, Interrupción de otros servicios y suministros esenciales, Condiciones inadecuadas de temperatura o humedad, Interrupción de otros servicios y suministros esenciales , Errores de mantenimiento / actualización de equipos (hardware), Caída del sistema por agotamiento de recursos, Errores de re-encaminamiento, Degradación de los soportes de almacenamiento de la información, Robo, Daños por agua , Desastres naturales ,Ataque destructivo e Indisponibilidad del personal. Con respecto a los impactos y la frecuencia nos han permitido determinar mediante un mapa de calor que el 45% de las amenazas se encuentran en un nivel de riesgo despreciable, el 30% se encuentra en un nivel bajo de riesgo, el 17% en un nivel apreciable, el 7% en un nivel importante y por último el 1% en un nivel crítico. Por ultimo en el tratamiento de las salvaguardas tenemos como resultado una matriz que nos permitió establecer en tipo y efecto que tendrían las salvaguardas en caso estas fueran aplicadas.
- La metodología OCATVE al evaluar las prácticas de seguridad organizacional y aplicar el estado semáforo, llegamos al resultado de que la Unidad de Ted Telemática no está realizando dichas prácticas como Estrategia de seguridad, Gestión de seguridad, políticas de seguridad y regulaciones, Gestión de la seguridad colaborativa, Plan de seguridad / Recuperación de desastres, Control de acceso físico, Monitoreo y Auditoria de seguridad física, Gestión del sistema y la red, Monitoreo y Auditoria de la seguridad de TI, Manejo de la vulnerabilidad, Seguridad de diseño y Arquitectura, Manejo de incidentes. O las está realizando hasta cierto punto como seguridad, concientización y entrenamiento, Autenticación y Autorización, Encriptación. Para la evaluación de las amenazas que se realizó a través de los árboles de amenaza, nos dio como resultado que las amenazas identificadas fueron a través del acceso a red, realizadas por personal que pertenece a la Unidad de Red Telemática y personas del exterior. La

primera por motivo accidental que como resultado hubo modificación, perdida e interrupción de la disponibilidad del activo y en la segunda hubo revelación, modificación e interrupción de la disponibilidad del activo. Otra amenaza identificada fue por problemas del sistema que como resultado hubo interrupción de la disponibilidad del activo cuando el sistema se cae. Y por último amenazas representadas por otros problemas como el suministro de energía que tuvo como resultado la interrupción de la disponibilidad del activo. En la evaluación de las amenazas que se representó a través del árbol de amenazas se tuvo como resultado que el impacto que tienen en los criterios es bajo y medio. Al igual que en la probabilidad cuyo resultado de la evaluación el valor fue en su mayoría bajo y medio.

Al describir las estrategias de protección actual tuvimos como resultado que la unidad de Red Telemática en su mayoría no cumple con las estrategias de protección. Por último, para la selección de enfoques de mitigación tenemos el árbol de amenazas que nos permitió visualizar el estado semáforo de las prácticas de seguridad para determinar si la amenaza se aceptaba, mitigaba o aplazaba.

- Que al definir los indicadores y criterios de medición en la Metodología MAGERIT se tuvo que definir una escala cuantitativa de 5 niveles (muy alto, alto, medio, bajo y muy bajo), para identificar el nivel de riesgo de la valorización de las amenazas; donde los rangos que se valoraron fueron de 0.01 a 1. Dicha escala fue asignada debido a que el resultado de la valorización de las amenazas estaba entre 0 y 100 por ciento. Y para la obtención del impacto se definió una escala cualitativa, donde los rangos que se valoraron fueron de 0.01 a 10. Dicha escala fue definida así ya que el nivel de impacto que se definió fue en una escala del 1 al 5.

  Para el nivel de riesgo se definieron niveles de tolerancia con una escala de despreciable, bajo, apreciable, importante y crítico, con un rango desde el 1 a 25.
- La metodología MAGERIT en caso específico de evaluar los escenarios de riesgos de la Unidad de Red Telemática conviene más que la metodología OCTAVE por estos motivos. La metodología MAGERIT nos permite una mejor identificación de los activos agrupándolas en capas permitiendo su mejor reconocimiento y definición. Así como su valoración proporcionándonos criterios y escalas para identificar que tan importante es el activo para la organización. Nos permite un mejor reconocimiento de las amenazas, ya que nos proporciona un catálogo de amenazas y la escala de valorización de las mismas. Nos permite conocer el impacto que tendría cada amenaza identificada en el activo así como la frecuencia. Nos proporciona una matriz completa del nivel de riesgo para poder identificar cuál de ellas son las que se tienen que tratar. Y finalmente Nos

proporciona un catálogo de salvaguardas para poder elegir la adecuada y proporcionar un correcto tratamiento de riesgo. En cambio, la Metodología OCTAVE nos proporciona todo un esquema ya estandarizado como el ya desarrollado pero que no nos brinda mucha información sobre cuán importante es el activo o cuan afectado este se ve ante una amenaza, ya que los criterios en los que se evalúan las escalas son datos proporcionados por la experiencia al igual que los datos obtenidos sobre el impacto que tienen sobre el activo. Y para el tratamiento de riesgo OCTAVE nos da la posibilidad de elegir si aceptamos, mitigamos o aplazamos.

6.2. RECOMENDACIONES

- Dado que la comparativa realizada de ambas metodologías ha sido aplicado a un caso específico en este caso en la Unidad de Red Telemática de la Universidad Nacional Pedro Ruiz Gallo y viendo de que esta no tiene sus procedimientos documentados, para reforzar los resultados obtenidos se recomienda de que sean aplicados otros estudios en otros contextos de tal manera que se refuerce los resultados obtenidos.
- Se recomienda incluir los criterios y escalas para la valoración de los activos como Obligaciones legales, Interese comerciales o económicos, Orden Público, Pérdida de confianza, Persecución de delitos, Tiempo de recuperación del servicio, Información clasificada (nacional) e Información clasificada (europea), criterios que no eran aplicables en el desarrollo de la investigación sin embargo MAGERIT nos dice que existen otros criterios aplicables sería recomendable incluirlos para mejorar el modelo realizado.
- Se recomienda se incluyan la Valoración económica, el coste que supondría recuperarse de un incidente que destrozara el activo y El valor de la interrupción del servicio; para mejorar el modelo realizado.
- Se recomienda se incluyan el cálculo del Impacto repercutido, Agregación de valores de impacto y Riesgo repercutido para mejorar el modelo realizado.
- Se recomienda se incluyan los árboles de dependencias ya que debido a la construcción del modelo que se adecue a la Unidad de Red Telemática no fueron incluidos.
- Se recomienda incluyan la eficacia de la protección y Vulnerabilidades de las salvaguardas que MAGERIT plantea ya que debido a la delimitación de la investigación no fueron incluidas.

BIBLIOGRAFIA Y REFERENCIAS DE CONSULTA

Christopher Alberts, A. D. (2005). OCTAVE-S Guía de Implementación v 1.0 . HANDBOOK.

Chumán, J. G. (2015). Aplicación de la metología MAGERIT para el análisis y Gestión de riesgos en los serviores de los sistemas de gestión académica de la Universidad Nacional Pedro Ruiz Gallo. Lambayeque.

Dirección General de Modernización Administrativa, P. e. (2012). Metodología de Análisis y Gestión de Riesgos de los Sistemas de Informacion. Libro II - Catálago de Elementos. Madrid: Ministerio de Hacienda y Administraciones Públicas.

Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica. (2012). Metodología de Análisis y Gestión de Riesgos de los Sistemas de Informacion. Libro I - Método. Madrid: Ministerio de Hacienda y Administraciones Públicas.

EY, C. (2015). Sin riesgo no hay recompensa - Encuesta sobre Gobierno, Riesgo y Cumplimiento 2015 [archivo PDF]. Obtenido de http://www.ey.com/Publication/vwLUAssets/Encuesta_sobre_Gobierno,_Riesgo_y_Cumplimiento_2015/$FILE/EY-encuesta-GRC.pdf

Guevara Chumán, J. G. (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. Lambayeque.

LTDA, A. d.-S. (2013). Publicaciones . Obtenido de Ing. Olga M Páez : www.elmayorportaldegerencia.com

Peña Velázquez, J. (2011). Aplicación de la metodología MAGERIT en el análisis de riesgo del flujo de información en el área de gestión de una empresa dedicada a la aplicación de exámenes de control de confianza. Mexico. Obtenido de Aplicación de la metodología MAGERIT en el análisis de riesgo del flujo de información en el área de gestión de una empresa dedicada a la aplicación de exámenes de control de confianza. .

Reyes Bedoya, D. E. (2014). El Análisis de Riesgos Informáticos y su incidencia en la seguridad e integridad de la información en la Facultad de Ingeniería Civil y Mecánica de la Universidad Técnica de Ambato. Ecuador .

Riesgos, G. d. (España: La Fábrica de Pensamiento del Instituto de Auditores Internos.). Obtenido de Definición e Implantación de Apetito de Riesgo: https://auditoresinternos.es/uploads/media_items/apetito-de-riesgo-libro.original.pdf

Westerman, G. F. (Diciembre de 2006). It Risk Management: From IT Necessity to Strategic Business Value. Obtenido de https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1010226

ANEXOS

Anexo 1: Tabla Clasificación de activos

CLASIFICACIÓN DE ACTIVOS
[D] DATOS
[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
[prp] desarrollo propio (in house)
[sub] desarrollo a medida (subcontratado)
[std] estándar (off the shelf)
[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
[HW] EQUIPOS INFORMÁTICOS
[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
(1) 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. (2) 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. (3) 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. (4) 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. (5) Son aquellos equipos preparados para hacerse cargo inmediato de los equipos en producción. (6) Dícese de impresoras y servidores de impresión. (7) Son los equipos que se instalan entre dos zonas de confianza. (8) 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
[sub] subcontratas
[prov] proveedores

Anexo 2: Tabla de identificación de activos

ACTIVOS DE LA UNIDAD DE RED TELEMÁTICA DE LA UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO			
ACTIVO		DESCRIPCIÓN	ENCARGADO
CÓDIGO	NOMBRE		
[S] SERVICIOS			
[SW] APLICACIONES			
[HW] EQUIPOS INFORMÁTICOS			
[serv]	Servidores		
[netw]	Soporte de red		
[COM] REDES DE COMUNICACIONES			
[MEDIA] SOPORTE DE INFORMACIÓN			
[elect]	Electrónicos		
[ele2]			
[noel]	No electrónico		
[AUX] EQUIPAMIENTO AUXILIAR			
[cable]	Cableado		
[L] INSTALACIONES			
[P] PERSONAL			

Anexo 3: Tabla de dependencias

ACTIVOS Y SUS DEPENDENCIAS DE LA UNIDAD DE RED TELEMÁTICA DE LA UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO		
ACTIVO		DEPENDENCIA
CÓDIGO	NOMBRE	
[S] SERVICIOS		
[SW] APLICACIONES		
[HW] EQUIPOS INFORMÁTICOS		
[serv]	Servidores	
[netw]	Soporte de red	
[COM] REDES DE COMUNICACIONES		
[MEDIA] SOPORTE DE INFORMACIÓN		
[elect]	Electrónicos	
[noel]	No electrónico	
[AUX] EQUIPAMIENTO AUXILIAR		
[cable]	Cableado	
[L] INSTALACIONES		
[P] PERSONAL		

Anexo 4: Tabla de valoración de activos

VALORACIÓN DE ACTIVOS DE LA UNIDAD DE RED TELEMÁTICA DE LA UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO							
ACTIVO		DIMENSIÓN					TOTAL
CÓDIGO	NOMBRE	DISPONIBILIDAD	INTEGRIDAD	CONFIDENCIALIDAD	AUTENTICIDAD	TRAZABILIDAD	
[S] SERVICIOS							
[SW] APLICACIONES							
[HW] EQUIPOS INFORMÁTICOS							
[serv]	Servidores						
[netw]	Soporte de red						
[COM] REDES DE COMUNICACIONES							
[MEDIA] SOPORTE DE INFORMACIÓN							
[elect]	Electrónicos						
[noel]	No electrónico						
[AUX] EQUIPAMIENTO AUXILIAR							
[cable]	Cableado						
[L] INSTALACIONES							
[P] PERSONAL							

Anexo 5: Tabla de identificación de amenazas

TABLA DE IDENTIFICACIÓN DE AMENAZAS EN LOS ACTIVOS DE LA UNIDAD DE RED TELEMÁTICA				
ACTIVO		AMENAZA		
CÓDIGO	NOMBRE	CÓDIGO	NOMBRE	DIMENSIÓN AFECTADA
[S] SERVICIOS				
[SW] APLICACIONES				
[HW] EQUIPOS INFORMÁTICOS				
[serv]	Servidores			
[netw]	Soporte de red			
[COM] REDES DE COMUNICACIONES				
[MEDIA] SOPORTE DE INFORMACIÓN				
[elect]	Electrónicos			
[noel]	No electrónico			
[AUX] EQUIPAMIENTO AUXILIAR				
[cable]	Cableado			
[L] INSTALACIONES				
[P] PERSONAL				

Anexo 6: Tabla de valoración de amenazas

TABLA VALORACIÓN DE ACTIVOS DE LA UNIDAD DE RED TELEMÁTICA										
ACTIVO		AMENAZA		DIMENSIÓN					TOTAL	NIVEL
CÓDIGO	NOMBRE	CÓDIGO	NOMBRE	DISPONIBILIDAD	INTEGRIDAD	CONFIDENCIALIDAD	AUTENTICIDAD	TRAZABILIDAD		
[S] SERVICIOS										
[SW] APLICACIONES										
[HW] EQUIPOS INFORMÁTICOS										
[serv]	Servidores									
[netw]	Soporte de red									
[COM] REDES DE COMUNICACIONES										
[MEDIA] SOPORTE DE INFORMACIÓN										
[elect]	Electrónicos									
[noel]	No electrónico									
[AUX] EQUIPAMIENTO AUXILIAR										
[cable]	Cableado									
[L] INSTALACIONES										
[P] PERSONAL										

Anexo 7: Tabla de impactos de las amenazas

TABLA VALORACIÓN DEL IMPACTO								
ACTIVO		AMENAZA		VALOR DE ACTIVO	DESGASTE	IMPACTO	ESCALA	NIVEL
CÓDIGO	NOMBRE	CÓDIGO	NOMBRE					
[S] SERVICIOS								
[SW] APLICACIONES								
[HW] EQUIPOS INFORMÁTICOS								
[serv]	Servidores							
[netw]	Soporte de red							
[COM] REDES DE COMUNICACIONES								
[MEDIA] SOPORTE DE INFORMACIÓN								
[elect]	Electrónicos							
[noel]	No electrónico							
[AUX] EQUIPAMIENTO AUXILIAR								
[cable]	Cableado							
[L] INSTALACIONES								
[P] PERSONAL								

Anexo 8: Tabla probabilidad de ocurrencia

TABLA DE PROBABILIDAD DE AMENAZA					
ACTIVO		AMENAZA		VALORACIÓN DE LA PROBABILIDAD	
CÓDIGO	NOMBRE	CÓDIGO	NOMBRE	NIVEL	ESCALA CUALITATIVA
[S] SERVICIOS					
[SW] APLICACIONES					
[HW] EQUIPOS INFORMÁTICOS					
[serv]	Servidores				
[netw]	Soporte de red				
[COM] REDES DE COMUNICACIONES					
[MEDIA] SOPORTE DE INFORMACIÓN					
[elect]	Electrónicos				
[noel]	No electrónico				
[AUX] EQUIPAMIENTO AUXILIAR					
[cable]	Cableado				
[L] INSTALACIONES					
[P] PERSONAL					

Anexo 9: Tabla riesgo

ACTIVO		AMENAZA		IMPACTO	PROBABILIDAD	CÓDIGO RIESGO	RIESGO	NIVEL	ESCALA
CÓDIGO	NOMBRE	CÓDIGO	NOMBRE						
[S] SERVICIOS									
[SW] APLICACIONES									
[HW] EQUIPOS INFORMÁTICOS									
[serv]	Servidores								
[netw]	Soporte de red								
[COM] REDES DE COMUNICACIONES									
[MEDIA] SOPORTE DE INFORMACIÓN									
[elect]	Electrónicos								
[noel]	No electrónico								
[AUX] EQUIPAMIENTO AUXILIAR									
[cable]	Cableado								
[L] INSTALACIONES									
[P] PERSONAL									

Anexo 10: Tabla Tratamiento del riesgo

ANÁLISIS DE RIESGO								TRATAMIENTO DE RIESGO					
ACTIVO	AMENAZA	IMPACTO	PROBABILIDAD	CÓDIGO RIESGO	RIESGO	NIVEL	ESCALA	SALVAGUARDA					
											TIPO		
CÓDIGO	CÓDIGO							CÓDIGO	NOMBRE	DESCRIPCIÓN	CÓDIGO	NOMBRE	EFECTO
[S] SERVICIOS													
[SW] APLICACIONES													
[HW] EQUIPOS INFORMÁTICOS													
[COM] REDES DE COMUNICACIONES													
[MEDIA] SOPORTE DE INFORMACIÓN													
[AUX] EQUIPAMIENTO AUXILIAR													
[cable]													
[L] INSTALACIONES													
[P] PERSONAL													

Anexo 11: Criterios de evaluación de impacto

REPUTACIÓN					
TIPO DE IMPACTO	MUY BAJO	BAJO	MEDIO	ALTO	MUY ALTO
Reputación					

FINANCIERA					
TIPO DE IMPACTO	MUY BAJO	BAJO	MEDIO	ALTO	MUY ALTO
Costos Operativos					

PRODUCTIVIDAD					
TIPO DE IMPACTO	MUY BAJO	BAJO	MEDIO	ALTO	MUY ALTO
Carga laboral					
Interrupción del servicio					
Administración y gestión					

SEGURIDAD/SALUD					
TIPO DE IMPACTO	MUY BAJO	BAJO	MEDIO	ALTO	MUY ALTO
Vida					
Seguridad / salud					

MULTAS/SANCIONES LEGALES					
TIPO DE IMPACTO	MUY BAJO	BAJO	MEDIO	ALTO	MUY ALTO
Multas					

Anexo 12: Hoja de trabajo: activos organizacionales

INFORMACIÓN, SISTEMAS Y APLICACIONES				
CÓDIGO	SISTEMA	INFORMACIÓN	APLICACIÓN Y SERVICIO	OTROS

PERSONAS				
CÓDIGO	PERSONAS	HABILIDADES Y CONOCIMIENTOS	SISTEMAS RELACIONADOS	ACTIVOS RELACIONADOS

Anexo 13: Hojas de trabajo: Prácticas de seguridad organizacional.

SEGURIDAD, CONCIENTIZACIÓN Y ENTRENAMIENTO										
ENUNCIADO	¿Hasta qué punto esta afirmación se refleja en su organización?				¿Qué actualmente su organización está haciendo bien en esta área?	¿Qué actualmente su organización no está haciendo bien en esta área?	¿Qué tan efectivamente su organización está implementando las prácticas en estas áreas?			
Los miembros del personal comprendan sus roles de seguridad y responsabilidades. Esto está documentado y verificado.	SI	ALGO	NO	NO SE SABE			ROJO	AMARILLO	VERDE	NO APLICA
Hay suficiente experiencia interna para todas las versiones servicios, mecanismos y tecnologías. Esto está documentado y verificado.	SI	ALGO	NO	NO SE SABE						
Existe una conciencia de seguridad, capacitación y recordatorios periódicos, los que se proporcionan para todo el personal. El entendimiento del personal está documentado y se verifica periódicamente.	SI	ALGO	NO	NO SE SABE						
Los miembros del personal siguen buenas prácticas como: Asegurar información de la que son responsables, No divulgar información confidencial a otros Tener capacidad suficiente para utilizar la información tecnología de hardware y software, Uso de buenas prácticas para definir contraseñas, Entender y seguir las políticas de seguridad y los reglamentos, Reconocer y reportar incidentes	SI	ALGO	NO	NO SE SABE						

ESTRATEGIA DE SEGURIDAD										
ENUNCIADO	¿Hasta qué punto esta afirmación se refleja en su organización?				¿Qué actualmente su organización está haciendo bien en esta área?	¿Qué actualmente su organización no está haciendo bien en esta área?	¿Qué tan efectivamente su organización está implementando las prácticas en estas áreas?			
Las estrategias comerciales de la organización incorporan consideraciones de seguridad.	SI	ALGO	NO	NO SE SABE			ROJO	AMARILLO	VERDE	NO APLICA
Las estrategias y políticas de seguridad toman en cuenta las estrategias y objetivos del negocio de la organización.	SI	ALGO	NO	NO SE SABE						
Las estrategias de seguridad, metas y objetivos son documentados y se revisan de forma rutinaria, se lo actualiza y se comunica a todos.	SI	ALGO	NO	NO SE SABE						

GESTIÓN DE SEGURIDAD										
ENUNCIADO	¿Hasta qué punto esta afirmación se refleja en su organización?				¿Qué actualmente su organización está haciendo bien en esta área?	¿Qué actualmente su organización no está haciendo bien en esta área?	¿Qué tan efectivamente su organización está implementando las prácticas en estas áreas?			
La Gerencia asigna fondos y recursos suficientes para actividades de información de seguridad.	SI	ALGO	NO	NO SE SABE			ROJO	AMARILLO	VERDE	NO APLICA
Los roles y responsabilidades de seguridad se definen para todo el personal de la organización.	SI	ALGO	NO	NO SE SABE						
Todo el personal en todos los niveles de responsabilidad pone en práctica sus funciones asignadas. Existen procedimientos documentados para la autorización y supervisión de todo el personal (incluido el personal tercerizado) que trabajan con sensible información o que trabajan en lugares donde la información reside.	SI	ALGO	NO	NO SE SABE						

Las prácticas de contratación y terminación de personal en la organización se toman en cuenta la seguridad informática.	SI	ALGO	NO	NO SE SABE		
La organización gestiona los riesgos de seguridad de la información: · Evalúa los riesgos para la seguridad de la información · Toma medidas para mitigar riesgos de seguridad de la información	SI	ALGO	NO	NO SE SABE		
Gerencia recibe y actúa sobre los informes de rutina relacionados con la seguridad de la información (por ejemplo, auditorías, registros y evaluaciones de vulnerabilidad).	SI	ALGO	NO	NO SE SABE		

POLÍTICAS DE SEGURIDAD Y REGULACIONES										
ENUNCIADO	¿Hasta qué punto esta afirmación se refleja en su organización?				¿Qué actualmente su organización está haciendo bien en esta área?	¿Qué actualmente su organización no está haciendo bien en esta área?	¿Qué tan efectivamente su organización está implementando las prácticas en estas áreas?			
La organización cuenta con un amplio conjunto de políticas actuales que periódicamente son revisadas y actualización.	SI	ALGO	NO	NO SE SABE			ROJO	AMARILLO	VERDE	NO APLICA
Hay un procedimiento documentado de gestión de las políticas de seguridad, que incluye: · Creación · Administración (revisiones periódicas y actualizaciones) · Comunicación	SI	ALGO	NO	NO SE SABE						
La organización dispone de un procedimiento documentado para evaluar y garantizar el cumplimiento de las políticas de seguridad, leyes y regulaciones aplicables, y requisitos de seguro.	SI	ALGO	NO	NO SE SABE						
La organización uniformemente refuerza sus políticas de seguridad.	SI	ALGO	NO	NO SE SABE						

GESTIÓN DE LA SEGURIDAD COLABORATIVA										
ENUNCIADO	¿Hasta qué punto esta afirmación se refleja en su organización?				¿Qué actualmente su organización está haciendo bien en esta área?	¿Qué actualmente su organización no está haciendo bien en esta área?	¿Qué tan efectivamente su organización está implementando las prácticas en estas áreas?			
La organización tiene políticas y procedimientos para proteger la información cuando trabaja con organizaciones externas (por ejemplo, terceros, colaboradores, subcontratistas o socios), incluidos • proteger la información que pertenece a otras organizaciones • Comprender las políticas y procedimientos de seguridad de las organizaciones externas. • finalizar el acceso a la información por parte de personal externo despedido	SI	ALGO	NO	NO SE SABE			ROJO	AMARILLO	VERDE	NO APLICA
La organización documenta los requisitos de protección de la información y los comunica explícitamente a todos los terceros apropiados.	SI	ALGO	NO	NO SE SABE						
La organización tiene mecanismos formales para verificar que todas las organizaciones de terceros, los servicios, mecanismos y tecnologías de seguridad tercerizados satisfacen sus necesidades y requisitos.	SI	ALGO	NO	NO SE SABE						
La organización tiene políticas y procedimientos para colaborar con todas las organizaciones de terceros que • Brindar servicios de capacitación y sensibilización sobre seguridad • Desarrollar políticas de seguridad para la organización. • desarrollar planes de contingencia para la organización	SI	ALGO	NO	NO SE SABE						

PLAN DE SEGURIDAD / RECUPERACIÓN DE DESASTRES										
ENUNCIADO	¿Hasta qué punto esta afirmación se refleja en su organización?				¿Qué actualmente su organización está haciendo bien en esta área?	¿Qué actualmente su organización no está haciendo bien en esta área?	¿Qué tan efectivamente su organización está implementando las prácticas en estas áreas?			
Se ha realizado un análisis de las operaciones, las aplicaciones y los datos críticos.	SI	ALGO	NO	NO SE SABE			ROJO	AMARILLO	VERDE	NO APLICA
La organización ha documentado, revisado y probado: · Planes de continuidad del negocio y de operación en caso de emergencia · Plan de recuperación de desastres (s)	SI	ALGO	NO	NO SE SABE						
Los planes de contingencia, recuperación de desastres y de negocios consideran la continuidad física y electrónica y los requisitos de acceso y controles.	SI	ALGO	NO	NO SE SABE						
Todo el personal: · Esta consciente de los planes de recuperación de desastres imprevistos y continuidad del negocio. · Comprende y es capaz de realizar sus responsabilidades.	SI	ALGO	NO	NO SE SABE						

CONTROL DE ACCESO FÍSICO										
ENUNCIADO	¿Hasta qué punto esta afirmación se refleja en su organización?				¿Qué actualmente su organización está haciendo bien en esta área?	¿Qué actualmente su organización no está haciendo bien en esta área?	¿Qué tan efectivamente su organización está implementando las prácticas en estas áreas?			
Si alguien del personal está encargado de esta área: Planes de seguridad de las instalaciones y procedimientos para salvaguardar las instalaciones, edificios y cualquier zona restringida y están documentados y probados.	SI	ALGO	NO	NO SE SABE			ROJO	AMARILLO	VERDE	NO APLICA
Hay políticas y procedimientos documentados para la gestión de los visitantes.	SI	ALGO	NO	NO SE SABE						
Hay políticas y procedimientos documentados para controlar el acceso físico a las áreas de trabajo y hardware (ordenadores, dispositivos de comunicación, etc.) y soporte de software.	SI	ALGO	NO	NO SE SABE						
Las estaciones de trabajo y otros componentes que permiten acceso a información sensible están físicamente salvaguardados para prevenir el acceso no autorizado.	SI	ALGO	NO	NO SE SABE						

MONITOREO Y AUDITORIA DE SEGURIDAD FISICA										
ENUNCIADO	¿Hasta qué punto esta afirmación se refleja en su organización?				¿Qué actualmente su organización está haciendo bien en esta área?	¿Qué actualmente su organización no está haciendo bien en esta área?	¿Qué tan efectivamente su organización está implementando las prácticas en estas áreas?			
Se mantienen registros de mantenimiento para documentar las reparaciones y modificaciones de los componentes físicos de una instalación.	SI	ALGO	NO	NO SE SABE			ROJO	AMARILLO	VERDE	NO APLICA
Las acciones de un individuo o grupo, con respecto a todos los medios controlados físicamente, pueden contabilizarse.	SI	ALGO	NO	NO SE SABE						
Los registros de auditoría y monitoreo se examinan rutinariamente para detectar anomalías, y se toman medidas correctivas según sea necesario.	SI	ALGO	NO	NO SE SABE						
Los requisitos de la organización para monitorear la seguridad física se comunican formalmente a todos los contratistas y proveedores de servicios que supervisan el acceso físico al edificio y las instalaciones, áreas de trabajo, hardware de TI y medios de software.	SI	ALGO	NO	NO SE SABE						
La organización verifica formalmente que los contratistas y proveedores de servicios hayan cumplido los requisitos para monitorear la seguridad física.	SI	ALGO	NO	NO SE SABE						

GESTIÓN DEL SISTEMA Y LA RED										
ENUNCIADO	¿Hasta qué punto esta afirmación se refleja en su organización?				¿Qué actualmente su organización está haciendo bien en esta área?	¿Qué actualmente su organización no está haciendo bien en esta área?	¿Qué tan efectivamente su organización está implementando las prácticas en estas áreas?			
Si alguien del personal está encargado de esta área: Existen planes de seguridad para salvaguardar el sistema y las redes.	SI	ALGO	NO	NO SE SABE			ROJO	AMARILLO	VERDE	NO APLICA
La información confidencial está protegida en un almacenamiento seguro (por ejemplo, copias de seguridad almacenadas en otro sitio).	SI	ALGO	NO	NO SE SABE						
La integridad del software instalado es regularmente verificada.	SI	ALGO	NO	NO SE SABE						
Todos los sistemas están actualizados a la fecha de acuerdo con revisiones, parches y recomendaciones de seguridad.	SI	ALGO	NO	NO SE SABE						
Existe un plan documentado y comprobado para la copia de seguridad de los datos de software. Todo el personal entiende sus responsabilidades en virtud de los planes de copia de seguridad.	SI	ALGO	NO	NO SE SABE						
Todos los cambios de hardware y software son planeados, controlados y documentados. Los miembros del área de TI siguen procedimientos para cambiar y dar de baja contraseñas, cuentas y privilegios.	SI	ALGO	NO	NO SE SABE						
Solo los servicios necesarios están corriendo en los sistemas, todos los servicios que no son necesarios han sido eliminados.	SI	ALGO	NO	NO SE SABE						
Herramientas y mecanismos para el sistema de seguridad y administración de la red que se utilizan, se revisan de manera rutinaria, se actualizan o reemplazan.	SI	ALGO	NO	NO SE SABE						

MONITOREO Y AUDITORIA DE LA SEGURIDAD DE TI										
ENUNCIADO	¿Hasta qué punto esta afirmación se refleja en su organización?				¿Qué actualmente su organización está haciendo bien en esta área?	¿Qué actualmente su organización no está haciendo bien en esta área?	¿Qué tan efectivamente su organización está implementando las prácticas en estas áreas?			
Si alguien del personal está encargado de esta área: Sistema y red de monitoreo y herramientas de auditoría son habitualmente utilizados por la organización. Actividades inusuales se manejan de acuerdo con las políticas y procedimientos definidos.	SI	ALGO	NO	NO SE SABE			ROJO	AMARILLO	VERDE	NO APLICA
Componentes del Firewall y otros componentes de seguridad son auditados periódicamente para revisar el cumplimiento de políticas.	SI	ALGO	NO	NO SE SABE						

AUTENTICACIÓN Y AUTORIZACIÓN										
ENUNCIADO	¿Hasta qué punto esta afirmación se refleja en su organización?				¿Qué actualmente su organización está haciendo bien en esta área?	¿Qué actualmente su organización no está haciendo bien en esta área?	¿Qué tan efectivamente su organización está implementando las prácticas en estas áreas?			
Los controles de acceso apropiados y la autenticación del usuario (por ejemplo, permisos de archivos, configuración de red) consistentes con la política se usan para restringir el acceso del usuario a la información, sistemas sensibles, aplicaciones y servicios específicos y conexiones de red.	SI	ALGO	NO	NO SE SABE			ROJO	AMARILLO	VERDE	NO APLICA
Existen políticas y procedimientos documentados para establecer y rescindir el derecho de acceso a la información tanto para individuos como para grupos.	SI	ALGO	NO	NO SE SABE						
Se proporcionan métodos o mecanismos para garantizar que no se acceda, altere o destruya la información confidencial de manera no autorizada. Los métodos o mecanismos se revisan y verifican periódicamente.	SI	ALGO	NO	NO SE SABE						
Los requisitos de la organización para controlar el acceso a los sistemas y la información se comunican formalmente a todos los contratistas y proveedores de servicios que brindan servicios de autenticación y autorización.	SI	ALGO	NO	NO SE SABE						
La organización verifica formalmente que los contratistas y proveedores de servicios hayan cumplido los requisitos de autenticación y autorización.	SI	ALGO	NO	NO SE SABE						

MANEJO DE LA VULNERABILIDAD										
ENUNCIADO	¿Hasta qué punto esta afirmación se refleja en su organización?				¿Qué actualmente su organización está haciendo bien en esta área?	¿Qué actualmente su organización no está haciendo bien en esta área?	¿Qué tan efectivamente su organización está implementando las prácticas en estas áreas?			
Si alguien del personal está encargado de esta área: Hay un conjunto de procedimientos documentados para manejo de vulnerabilidades, para: · Seleccionar las herramientas de evaluación de vulnerabilidad, listas de control y secuencias de comandos · Mantenerse al día con la vulnerabilidad conocida, tipos y métodos de ataque · Revisar las fuentes de información sobre anuncios de vulnerabilidad, alertas de seguridad y comunicación · Identificación de los componentes de infraestructura a ser evaluado · Programar evaluaciones de vulnerabilidad · Interpretar y responder a los resultados · Mantener un almacenamiento seguro y la disposición de datos vulnerables.	SI	ALGO	NO	NO SE SABE		No hay procedimientos definidos para poder manejar la vulnerabilidad en la organización.	ROJO	AMARILLO	VERDE	NO APLICA
Se siguen procedimientos de gestión de vulnerabilidades los que son periódicamente revisados y actualizados.	SI	ALGO	NO	NO SE SABE						
Evaluaciones de tecnología vulnerable se realizan en forma periódica, y las vulnerabilidades se abordan cuando se las identifica.	SI	ALGO	NO	NO SE SABE						

ENCRIPTACIÓN										
ENUNCIADO	¿Hasta qué punto esta afirmación se refleja en su organización?				¿Qué actualmente su organización está haciendo bien en esta área?	¿Qué actualmente su organización no está haciendo bien en esta área?	¿Qué tan efectivamente su organización está implementando las prácticas en estas áreas?			
Si alguien del personal está encargado de esta área: · Controles apropiados de seguridad se utilizan para proteger información sensible durante el almacenamiento y durante la transmisión (por ejemplo, el cifrado de datos, infraestructura de clave pública, tecnología de red privada virtual).	SI	ALGO	NO	NO SE SABE			ROJO	AMARILLO	VERDE	NO APLICA
Se utilizan protocolos de cifrado cuando se maneja sistemas, routers y firewalls a distancia.	SI	ALGO	NO	NO SE SABE						

SEGURIDAD DE DISEÑO Y ARQUITECTURA										
ENUNCIADO	¿Hasta qué punto esta afirmación se refleja en su organización?				¿Qué actualmente su organización está haciendo bien en esta área?	¿Qué actualmente su organización no está haciendo bien en esta área?	¿Qué tan efectivamente su organización está implementando las prácticas en estas áreas?			
Si alguien del personal está encargado de esta área: Arquitectura del sistema y diseño para sistemas nuevos y actualizaciones que incluyen las siguientes consideraciones: · Estrategias de seguridad, políticas y procedimientos · Antecedentes de compromisos de seguridad. · Resultados de las evaluaciones de riesgos de seguridad.	SI	ALGO	NO	NO SE SABE			ROJO	AMARILLO	VERDE	NO APLICA
La organización tiene diagramas que muestran la seguridad en toda la empresa y la arquitectura de red que están actualizados.	SI	ALGO	NO	NO SE SABE						

MANEJO DE INCIDENTES										
ENUNCIADO	¿Hasta qué punto esta afirmación se refleja en su organización?				¿Qué actualmente su organización está haciendo bien en esta área?	¿Qué actualmente su organización no está haciendo bien en esta área?	¿Qué tan efectivamente su organización está implementando las prácticas en estas áreas?			
Si alguien del personal está encargado de esta área: Existen procedimientos documentados para la identificación, presentación de informes, y procesos para responder a incidentes sospechosos y violaciones.	SI	ALGO	NO	NO SE SABE			ROJO	AMARILLO	VERDE	NO APLICA
Los procedimientos de manejo de incidentes son periódicamente probados, verificados y actualizados.	SI	ALGO	NO	NO SE SABE						
Existen políticas y procedimientos documentados para trabajar con autoridades policiales.	SI	ALGO	NO	NO SE SABE						

Anexo 14: Hoja de trabajo: activo crítico.

ACTIVO CRÍTICO	RAZÓN DE SELECCIÓN
¿Cuál es el sistema crítico?	¿Por qué este sistema es crítico para la organización?

DESCRIPCIÓN
¿Quién usa el sistema? / ¿Quién es responsable del sistema?

ACTIVOS RELACIONADOS			
¿Qué activos están relacionados con este sistema?			
Sistemas	Información	Aplicaciones	Otros

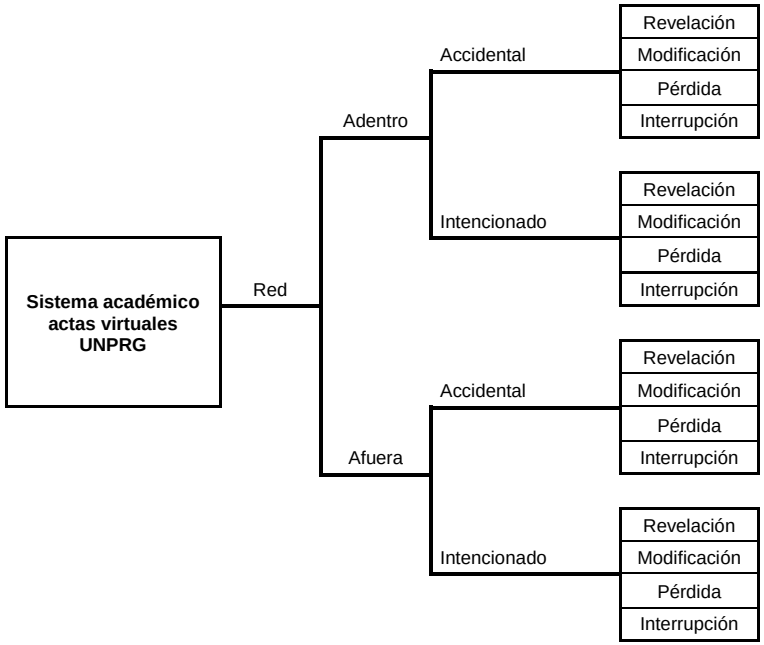
Anexo 15: Hoja de trabajo: Requisitos de seguridad para los activos.

REQUERIMIENTOS DE SEGURIDAD
¿Cuáles son los requisitos de seguridad para este sistema?
- Confidencialidad: - Integridad: - Disponibilidad - Otros

Requerimento de seguridad más importante
¿Qué requisito de seguridad es más importante para este sistema?
* Confidencialidad
* Integridad
* Disponibilidad
* Otros

Anexo 16: Hoja de Trabajo: Identificación de amenazas de los activos

Amenaza	**Actores de amenaza**	**Motivo**	
¿Para cuál rama hay una posibilidad no despreciable de una amenaza al activo? Marque estas ramas en el árbol. ¿Para cuál de las ramas restantes hay una posibilidad despreciable o nula de una amenaza para el activo? No marque estas ramas.	¿Qué actores plantean las mayores amenazas para el sistema a través de la red?	¿Qué tan fuerte es el motivo del actor?	¿Qué tan confiado está usted de este estimado?



Actor	Motivo	Resultado		Muy alto	alto	Medio	Bajo	Muy bajo	Muy	Algo	Nada
Adentro	Accidental	Revelación	**Personas que pertenecen a la organización que actúan accidentalmente:**								
		Modificación									
		Pérdida									
		Interrupción									
	Intencionado	Revelación	**Personas que pertenecen a la organización que actúan deliberadamente:**								
		Modificación									
		Pérdida									
		Interrupción									
Afuera	Accidental	Revelación	**Personas ajenas a la organización que actúan accidentalmente:**								
		Modificación									
		Pérdida									
		Interrupción									
	Intencionado	Revelación	**Personas ajenas a la organización que actúan deliberadamente:**								
		Modificación									
		Pérdida									
		Interrupción									

Historia

¿Con qué frecuencia ha ocurrido esta amenaza en el pasado?	¿Qué tan exactos son estos datos?

	Muy	Algo	Nada

Gente que pertenece a la organización que tiene acceso a la red	
De ejemplos de cómo personas que pertenecen a la organización actuando accidentalmente podrían utilizar el acceso a la red para amenazar el sistema.	
De ejemplos de cómo personas que pertenecen a la organización que actuando deliberadamente podrían utilizar el acceso a la red para amenazar el sistema.	

Gente que no pertenece a la organización que tiene acceso a la red	
De ejemplos de cómo personas que no pertenecen a la organización que actuando accidentalmente podrían utilizar el acceso a la red para amenazar el sistema.	
De ejemplos de cómo personas que no pertenecen a la organización que actuando deliberadamente podrían utilizar el acceso a la red para amenazar el sistema.	

Anexo 17: Hoja de Trabajo: Análisis de procesos relacionados con la tecnología

CLASE	ACTIVO CRÍTICO				RESPONSABILIDAD
Servidores					
Estaciones de trabajo					
Redes internas					
Redes externas					
Laptops/Computadoras					
Estaciones de trabajo fuera de la oficina.					
Dispositivos de almacenamiento de respaldos locales					

Anexo 18: Hoja de trabajo: rutas de acceso

SISTEMA DE INTERÉS	PUNTOS DE ACCESO INTERMEDIOS	ACCESO AL SISTEMA POR INDIVIDUOS	UBICACIÓN DE DONDE SE ALMACENAN	OTROS SISTEMAS O COMPONENTES
¿Cuál de las siguientes clases de componentes son parte del sistema de interés?	¿Cuál de las siguientes clases de componentes se utilizan para transmitir información y aplicaciones desde el sistema de interés hacia la gente? ¿Cuál de las siguientes clases de componentes podría servir como un punto de acceso intermedio?	¿De cuál de las siguientes clases de componentes puede la gente (por ejemplo, los usuarios, los atacantes) acceder al sistema de interés? Considere puntos de acceso internos	¿En qué clase de componente esta la información del sistema de interés almacenada por motivos de respaldo?	¿Cuál otro sistema accede a información del sistema de interés?

☐	**Servidores**	☐	**Redes internas**	☐	**Estaciones de Trabajo**	☐	**Dispositivos de almacenamiento de respaldos locales**	☐	
☐	**Redes internas**	☐	**Redes externas**	☐	**Laptops**				
☐	**Estaciones de trabajo**	☐	**Otros (Lista)**	☐	**PDAs/Componentes Wireless**	☐	**Otros (Lista)**		
☐	**Otros (Lista)**			☐	**Estaciones de Trabajo fuera de la oficina**				
				☐	**Otros (Lista)**				

Anexo 19: Hoja de Trabajo: impacto de las amenazas

AMENAZA					IMPACTO				
Activo	Acceso	Actor	Motivo	Resultado	Reputación	Productividad	Multas y penas legales	Seguridad	Financiera
☐		Adentro	Accidental	Revelación					
				Modificación					
				Pérdida					
				Interrupción					
			Intencionado	Revelación					
				Modificación					
				Pérdida					
				Interrupción					
		Afuera	Accidental	Revelación					
				Modificación					
				Pérdida					
				Interrupción					
			Intencionado	Revelación					
				Modificación					
				Pérdida					
				Interrupción					

Anexo 20: Hoja de trabajo: Probabilidad de amenaza.

AMENAZA					Valor	CONFIANZA		
Activo	**Acceso**	**Actor**	**Motivo**	**Resultado**		MUY	ALGO	NADA
		Adentro	Accidental	Revelación				
				Modificación				
				Pérdida				
				Interrupción				
			Intencionado	Revelación				
				Modificación				
				Pérdida				
				Interrupción				
		Afuera	Accidental	Revelación				
				Modificación				
				Pérdida				
				Interrupción				
			Intencionado	Revelación				
				Modificación				
				Pérdida				
				Interrupción				

Anexo 21: Hoja de Trabajo: Selección de enfoque de mitigación.