Selección e Implementación de una Metodología de Análisis de Riesgos para una IES

Camilo Andrés Carrillo Niño

Wilson López Santos

Alexander Prada Perez

6 de Diciembre de 2021

1. Contexto y Justificación

Las IES - Instituciones de Educación Superior durante los últimos años se han enfrentado a una rápida transformación digital, especialmente a partir de inicios del año 2020 debido a la emergencia sanitaria causada por la enfermedad del COVID-19. Se ha identificado por parte de las instituciones un alto grado dependencia en las plataformas tecnológicas para el proceso formativo de los estudiantes, así como la necesidad de trasladar muchos de los procesos de apoyo administrativos y financieros hacia soluciones digitales que permitan contar con aspectos como:

- Acceso desde fuera del campus y las diferentes sedes de la universidad a los aplicativos y plataformas.
- Disponibilidad de la información tanto académica como administrativa.
- Posibilidad de asistencia virtual a clases, reuniones y turnos de trabajo.
- Control de entregas y notas en línea.
- Posibilidad de atender los diferentes requisitos de los estudiantes en línea, tales como certificados, estados de cuenta, inscripciones, cancelaciones y pagos.
- Suplir los procesos administrativos a través de diferentes soluciones tecnológicas que permitan trabajo en casa.

Sin embargo, la implementación de las tecnologías y plataformas que proporcionan estas funcionalidades conllevan riesgos de carácter tecnológico que deben ser mitigados oportunamente con el fin de evitar exponer no solamente la información personal de estudiantes y trabajadores sino, también, los estados financieros, los activos intangibles de la institución y su reputación misma.

En este sentido, se ha evidenciado que las entidades de educación superior son un objetivo de interés para los ciberatacantes pues en los sistemas tecnológicos de las universidades figura la información personal y financiera de estudiantes, responsables económicos, profesores, trabajadores y proveedores. Así mismo, los controles y seguimientos académicos a nivel de entregas, asistencias y notas suelen ser de especial interés para algunos elementos de la comunidad estudiantil, pues podrían ver en ello una posibilidad de alteración de la información para beneficio propio o de un tercero.

Dados estos antecedentes es necesario iniciar, para el caso de las entidades que aún no realizan esta tarea, con un proceso de análisis de riesgos que permita documentar todas aquellas falencias críticas que pueden estar sufriendo los activos y los servicios. Este punto de partida permitirá el establecimiento de controles oportunos y una ruta de trabajo eficaz que considere primero los activos críticos y posteriormente lleve a un cubrimiento total, es importante anotar que dada la naturaleza cambiante y evolutiva de la tecnología no se puede tratar de un proceso estático en el tiempo sino de uno que propenda por una mejora continua.

Además de las necesidades descritas anteriormente, otros antecedentes que soportan esta necesidad son los recientes intentos de ataque a otras instituciones de educación superior en el país:

- En abril 14 de 2021 se informó acerca de un intento de ataque informático a la Universidad de los Andes, el cual se determinó que fue un intento de ransomware (Redacción Universidad, 2021).

- El 28 de junio de 2021 se puso de manifiesto un ataque informático a la Universidad del Bosque, el cual dejó fuera de línea muchos de sus sistemas y plataformas durante un lapso de más de 24 horas (Redacción Educación, 2021).

Así las cosas, el presente proyecto busca con ayuda de la selección de una metodología, tarea inicial del proceso, realizar todas las actividades de análisis de riesgos de seguridad de la información e informática para una IES - Institución de Educación Superior, limitando el alcance al servicio de conectividad o redes de datos, pero abarcando elementos propios o importantes para la disponibilidad de otros servicios tales como Datacenter y centros de cableado, también se tendrá en cuenta la calidad en las instalaciones de medios físicos de transmisión que hacen parte importante de este servicio y que también en muchas ocasiones considerado un talón de Aquiles si no se encuentra lo suficientemente protegido.

A continuación, se enmarcarán las grandes actividades involucradas en el proceso que puede ser fácilmente replicado para todos los servicios tecnológicos de una entidad educativa, real finalidad y trabajo futuro, en términos de continuidad, del presente proyecto.

2. Elección de una Metodología de Análisis de Riesgos

2.1. Método de Ponderación de Criterios

También denominado análisis de matriz de priorización se trata de una disposición de las diferentes opciones a evaluar en filas, mientras que los criterios considerados se posicionan en columnas al frente de ellos. De esta manera se facilita la identificación de la opción que mejor cumple con los criterios a través de un planteamiento matemático que arroja una opción con el mayor porcentaje de cumplimiento de las necesidades establecidas (Betancourt, 2018).

Las ventajas de este método incluyen:

- Flexibilidad. Al permitir extender el análisis desde unas pocas opciones combinadas con una selección reducida de criterios hasta una lista extensa de opciones comparada por diversos criterios
- Trabajo en equipo. Los pesos asignados a los criterios, así como los puntajes asignados a cada una de las opciones evaluadas pueden ser discutidos y definidos en equipos a través de diferentes técnicas colaborativas tanto presenciales como a través de herramientas en línea
- Parametrizable. El método puede ser trasladado a una herramienta de software como una hoja de cálculo o una aplicación especializada, no solamente para permitir mayor facilidad en el análisis de listas extensas de opciones, sino para permitir colaboración, trazabilidad y reproducibilidad del análisis
- Consenso. Una matriz de priorización suele ser un argumento sólido para justificar la elección de la mejor opción, reduciendo la posibilidad de dudas y objeciones.

Para conseguir una comparación efectiva, la metodología consta un conjunto de pasos ordenados que se describen brevemente a continuación.

i. Definir el objetivo. A través de este paso se define cual es el objeto del análisis y por qué es necesario
ii. Enunciar las opciones disponibles. A pesar de que las opciones pueden parecer claras desde el principio, en este paso es necesario acotar una lista con las opciones válidas que harán parte del análisis
iii. Establecer los Criterios. De igual manera se deben definir los factores que generan valor al objetivo buscado
iv. Asignar un peso ponderado a cada criterio. De esta manera se define cuáles son los criterios con mayor valor y en qué medida aportan al objetivo buscado
v. Definir un nivel de cumplimiento de cada una de las opciones para cada uno de los criterios. Es un paso que se realiza colaborativamente y que consiste en asignar un valor a cada una de las casillas de la matriz, teniendo en cuenta cómo cada una de las opciones se enfrenta a cada uno de los criterios

2.2. Aplicación del Método de Ponderación de Criterios

En los siguientes pasos se describe el procedimiento que se llevó a cabo para la elección de la metodología más conveniente para el desarrollo de este proyecto

2.2.1. Opciones por Considerar

- **ISO 27005:** El estándar publicado por la Organización Internacional de Estándares con referencia al control y manejo de riesgos en seguridad de la información (International Standard Organization, 2018).
- **Magerit:** Metodología creada por el Órgano de Administración Electrónica del Ministerio de Transformación Económica y Digital del gobierno español (Secretaría General de Administración Digital, 2012).
- **Mehari:** Método concertado de administración del riesgo, originado por el gobierno francés y utilizado por la Unión Europea (European Agency for Cybersecurity, 2018)**.**
- **Microsoft Security Management Guide:** Es el conjunto de pasos, recomendaciones y prácticas publicado por Microsoft para el aseguramiento de sus tecnologías por parte de organizaciones que utilizan sus productos. Pero que también puede ser utilizado con otros productos y plataformas (Microsoft, 2021).
- **NIST 800-30:** Guía para la evaluación del riesgo en sistemas de información, concebida y utilizada por el gobierno federal de los Estados Unidos (National Institute of Standards and Technology, 2012).

2.2.2. Criterios por Evaluar

- **Facilidad:** Dado el plazo del que se dispone para el desarrollo del proyecto, los recursos de los que se dispone y un nivel de interacción limitado con respecto a otras áreas de la organización; es necesario adoptar una metodología que facilite su implementación sin muchas dependencias ni prerrequisitos y que permita el desarrollo de simplificados que aporten valor rápidamente a los objetivos del proyecto.
- **Documentación:** Es necesario contar con documentación suplementaria que permita consulta y soporte para las actividades a realizar en el desarrollo del proyecto.
- **Cobertura de Controles:** Se requiere una etapa de recomendaciones que permitan a la organización escoger el tratamiento y los controles más convenientes para los riesgos identificados.
- **Autonomía de Implementación:** Debido a que la colaboración con otros departamentos y áreas de la organización se encuentra limitada, el desarrollo del proyecto se enmarcará por una metodología que permita autonomía en la toma de decisiones y el desarrollo de actividades al interior de la Dirección de Sistemas y Tecnologías de la Información. Sin necesidad de escalar o consultar a otros departamentos.
- **Pertinencia:** La metodología debe favorecer el marco y el alcance de este proyecto dentro de los criterios aquí descritos y orientar los esfuerzos de forma fluida y sostenida.
- **Entregables:** La metodología debe producir documentos, esquemas y artefactos sintetizados, de fácil lectura y entendimiento. Que no dependan de sistemas o plataformas propietarias para poder ser distribuidos a los stakeholders.
- **Flexibilidad:** Es necesario contar con un marco flexible, adaptable y ajustable. Que permita la originalidad en el desarrollo de cada uno de sus pasos, así como la combinación con otras literaturas y técnicas. De manera que el proyecto se desarrolle con elementos de innovación y de mejora continua.
- **Costo:** Serán de preferente elección las metodologías de Acceso Abierto (Open Source), que no generen costos por licenciamiento y que no requieran autorización o auditoría por parte de un tercero para su utilización.

2.2.3. Asignación de Pesos

A través de un trabajo en equipo se ponderaron los criterios anteriormente descritos, identificando la importancia de cada uno de ellos. Las técnicas utilizadas para el desarrollo de esta actividad son el análisis

multicriterio y el método analítico de jerarquía, AHP por sus siglas en inglés (Vargas, 2010), y algunos aportes originales del grupo de trabajo en pro del desarrollo del proyecto. El proceso llevado a cabo se describe a continuación.

En un primer lugar se estableció una matriz de comparación de criterios con el fin de identificar aquellos criterios que son más importantes para el desarrollo del proyecto y en qué medida.

En esta matriz los criterios son comparados por pares, entre el criterio que identifica la fila y el criterio que identifica la columna. La asignación del valor a cada casilla se rige por las siguientes reglas:

1. Si los dos criterios son de igual importancia, la casilla recibe un valor de 1.0.
2. Si el criterio que identifica la columna es de mayor importancia para el proyecto frente al criterio que identifica la fila, la casilla recibe un valor de 2.0 a 4.0 de acuerdo con el nivel de importancia definido por el equipo.
3. Si el criterio que identifica la columna es de menor importancia frente al criterio que identifica la fila, la casilla queda en blanco temporalmente.
4. Para aquellas casillas que habían quedado en blanco, si el criterio que identifica la fila es de mayor importancia que el criterio que identifica la columna, la casilla recibe un valor 2.0 a 4.0 de acuerdo con el nivel de importancia definido por el equipo. De lo contrario, el valor de la casilla es calculado dividiendo 1 sobre el valor de la casilla contrapuesta. De esta manera la matriz queda completamente diligenciada.

La tabla 1 permite observar la distribución de pesos asignados a cada uno de los criterios de acuerdo con este paso del proceso

Matriz Inicial	*C.1 Facilidad de Implementación*	*C.2 Documentación Suplementaria*	*C.3 Cobertura de Controles*	*C.4 Autonomía de Implementación*	*C.5 Pertinencia Frente al Alcance*	*C.6 Entregables Sintetizados*	*C.7 Flexibilidad de Aplicación*	*C.8 Acceso Abierto*
C.1 Facilidad de Implementación	**1.0**	1.0	0.3	4.0	2.0	1.0	1.0	4.0
C.2 Documentación Suplementaria	1.0	**1.0**	0.5	0.5	3.0	1.0	0.5	2.0
C.3 Cobertura de Controles	3.0	2.0	**1.0**	2.0	0.3	1.0	1.0	3.0
C.4 Autonomía de Implementación	0.3	2.0	0.5	**1.0**	0.5	0.5	1.0	1.0
C.5 Pertinencia Frente al Alcance	0.5	0.3	3.0	2.0	**1.0**	0.3	0.5	1.0
C.6 Entregables Sintetizados	1.0	1.0	1.0	2.0	3.0	**1.0**	3.0	3.0
C.7 Flexibilidad de Aplicación	1.0	2.0	1.0	1.0	2.0	0.3	**1.0**	4.0
C.8 Acceso Abierto	0.3	0.5	0.3	1.0	1.0	0.3	0.3	**1.0**

Tabla 1: Matriz Inicial de Criterios

El segundo paso consiste en la normalización de la matriz, para luego calcular la media aritmética de cada una de las filas y de esta manera conseguir el Vector de Prioridad y el peso de cada uno de los criterios en la decisión final.

En la tabla 2 se observan los valores ya normalizados de los criterios

Matriz Normalizada	*C.1 Facilidad de Implementación*	*C.2 Documentación Suplementaria*	*C.3 Cobertura de Controles*	*C.4 Autonomía de Implementación*	*C.5 Pertinencia Frente al Alcance*	*C.6 Entregables Sintetizados*	*C.7 Flexibilidad de Aplicación*	*C.8 Acceso Abierto*	*Vector Prioridad*	
C.1 Facilidad de Implementación	0.1	0.1	0.0	0.3	0.2	0.2	0.1	0.2	0.154	15.4%
C.2 Documentación Suplementaria	0.1	0.1	0.1	0.0	0.2	0.2	0.1	0.1	0.114	11.4%
C.3 Cobertura de Controles	0.4	0.2	0.1	0.1	0.0	0.2	0.1	0.2	0.168	16.8%
C.4 Autonomía de Implementación	0.0	0.2	0.1	0.1	0.0	0.1	0.1	0.1	0.085	8.5%
C.5 Pertinencia Frente al Alcance	0.1	0.0	0.4	0.1	0.1	0.1	0.1	0.1	0.111	11.1%
C.6 Entregables Sintetizados	0.1	0.1	0.1	0.1	0.2	0.2	0.4	0.2	0.180	18.0%
C.7 Flexibilidad de Aplicación	0.1	0.2	0.1	0.1	0.2	0.1	0.1	0.2	0.135	13.5%
C.8 Acceso Abierto	0.0	0.1	0.0	0.1	0.1	0.1	0.0	0.1	0.053	5.3%

Tabla 2: Matriz de Criterios Normalizada

2.2.4. Evaluación de las Opciones

Una vez definidos los pesos de cada uno de los criterios, se agendó y realizó una reunión entre los integrantes del grupo de trabajo y el sponsor del proyecto a fin de realizar un juicio de expertos en donde se estimó el nivel de cumplimiento de cada una de las metodologías frente a cada uno de los criterios.

Cada uno de los participantes del equipo recibió bibliografía inicial para cada una de las metodologías a evaluar y, adicionalmente, tomó un tiempo prudencial para investigar recursos adicionales que le permitieran reconocer las características generales de cada una de las metodologías, así como algunas de sus ventajas y desventajas.

El ejercicio de estimación se llevó a cabo en una reunión de evaluación. Se hizo uso de una técnica de estimación ágil en la que se evalúan, uno por uno, todos los criterios para cada metodología.

Para dicha evaluación, cada uno de los participantes arroja un puntaje de cumplimiento del criterio por parte de cada metodología; este puntaje corresponde a la siguiente escala basada en puntos Fibonacci:

1. La metodología no cumple el criterio.
2. La metodología cumple mínimamente el criterio.
3. La metodología aporta ciertos elementos de cumplimiento, pero no cumple completamente el criterio.
4. La metodología cumple completamente el criterio.

Una vez cada participante ha asignado este puntaje, se compara la estimación de todos los participantes alrededor del criterio en busca de una mayoría. Aquellos participantes que difieren más notablemente de los demás tienen la oportunidad de justificar su estimación con el fin de llegar a un consenso y acercar estas diferencias hacia el punto medio sin salirse de la escala definida.

Para este ejercicio se utilizó la herramienta Planit Poker (https://www.planitpoker.com/), que permite su uso gratuito en reuniones de estimación para metodologías ágiles tanto en equipos presenciales como reunidos a través de video conferencia. Esta técnica es muy utilizada, por ejemplo, para definir la complejidad de un requerimiento en proyectos de desarrollo de software (Radigan, s.f.).

Una vez se completó la estimación, se realizó el cálculo de un puntaje final para cada metodología a través de la multiplicación del puntaje recibido por el peso el criterio en cuestión para, finalmente sumar el puntaje a fin de arrojar una nota definitiva.

Criterios	Peso %	ISO 27005	Magerit	Mehari	Microsoft	NIST 800-30	ISO 27005	Magerit	Mehari	Microsoft	NIST 800-30
C.1 Facilidad de Implementación	15.4%	1	5	3	3	2	0.2	0.8	0.5	0.5	0.3
C.2 Documentación Suplementaria	11.4%	5	5	2	3	3	0.8	0.8	0.3	0.5	0.5
C.3 Cobertura de Controles	16.8%	5	1	1	1	5	0.8	0.2	0.2	0.2	0.8
C.4 Autonomía de Implementación	8.5%	1	5	5	3	2	0.2	0.8	0.8	0.5	0.3
C.5 Pertinencia Frente al Alcance	11.1%	1	5	5	2	2	0.2	0.8	0.8	0.3	0.3
C.6 Entregables Sintetizados	18.0%	2	5	5	5	3	0.3	0.8	0.8	0.8	0.5
C.7 Flexibilidad de Aplicación	13.5%	1	5	5	3	3	0.2	0.8	0.8	0.5	0.5
C.8 Acceso Abierto	5.3%	1	5	5	5	5	0.2	0.8	0.8	0.8	0.8
							2.6	3.2	2.5	1.9	2.2

Tabla 3: Evaluación de las Metodologías

Finalmente, a través de este proceso se pudo determinar que Magerit es la metodología que más se ajusta a las necesidades del proyecto propuesto y que cuenta con las características requeridas de acuerdo con los criterios seleccionados.

3. Metodología Magerit Para el Análisis e Identificación de Riesgos en Seguridad de la Información

Se trata de una metodología concebida por la Comisión Estratégica de las Tecnologías de la Información y las Comunicaciones del gobierno español, en respuesta a la percepción de que la administración estatal, las entidades y en general toda la sociedad dependen cada vez más de las tecnologías de la información para su funcionamiento y el cumplimiento de sus objetivos. (Secrtetaría de Administración Digital, 2012)

Algunas de las características y ventajas de la metodología Magerit incluyen:

- Determina los riesgos presentes con respecto a la información y propende por su control.
- Permite determinar y recomendar las medidas apropiadas que deberían ser puestas en marcha.
- Facilita la implementación de un sistema de gestión de seguridad de la información.
- Proporciona los principios y requerimientos para la protección de la información.

Adicionalmente, la misión de la metodología se enmarca en los siguientes objetivos:

- Poner en conocimiento a los responsables de los sistemas de información la existencia de riesgos a fin de establecer un tratamiento idóneo y documentado de estos.
- Ofrecer un método ordenado para analizar dichos riesgos.
- Planificar las medidas oportunas para mantener los riesgos bajo control.
- Apalancar procesos de auditoría y certificación.

3.1. Análisis y Gestión de Riesgos

Una de las principales dificultades al abordar las problemáticas asociadas a la seguridad de la información en la mayoría de las organizaciones es dar comienzo a los esfuerzos de protección desde la definición de un mapa de riesgos. Es común encontrar escenarios en los que la organización y sus líderes van directo a las medidas con la convicción de que es necesario proteger todos los sistemas y plataformas, implementar todas las soluciones, pero sin una hoja de ruta que dicte prioridades o recomendaciones y que, en la mayoría de las oportunidades, tampoco permite medir la efectividad de los esfuerzos.

Sopesar esta resistencia al uso de una metodología organizada y basada en el estudio de los riesgos requirió dos esfuerzos importantes:

1. Presentar las metodologías de gestión del riesgo, y en especial Magerit, al equipo de trabajo; ofreciendo claridad sobre las ventajas y las fortalezas que ofrece abordar estas metodologías como un punto de inicio para la protección de los activos de información.
2. Evidenciar los retos que suponen las tareas de endurecimiento y adopción de sistemas y plataformas en cuanto a seguridad de la información sin los pasos previos que ayuden a identificar las necesidades inmediatos, los requerimientos delimitados y sin una cobertura definida que permita medir la efectividad y eficiencia de las medidas adoptadas.

Una vez superada esta dificultad se abordó la metodología como un conjunto de pasos y técnicas orientados, no solamente a mitigar los riesgos inherentes a la seguridad de la información sino también, a poder identificar los activos de información decisivos y su contribución a los objetivos organizacionales desde el punto de vista de la información. Magerit parte entonces del ideal de proteger la misión de la organización, teniendo en cuenta las diferentes dimensiones de seguridad de la información:

- Disponibilidad
- Integridad
- Confidencialidad
- Autenticidad
- No repudio

Para que un activo de seguridad se considere seguro, pueden cumplirse todas o solo algunas de estas características según las necesidades de cada sistema y cada organización. Para conseguir el cumplimiento de estas características se requiere disponer de los medios y esfuerzos idóneos para este fin.

El análisis de riesgos es un método para determinar los impedimentos internos o externos para el conseguir una o varias de estas características. Los pasos de los que se compone este método son:

3.2. Determinar los activos relevantes para la organización

Los recursos del sistema de información o aquellos que se relacionan con este, necesarios para que la organización funcione correctamente y alcance los objetivos propuestos por su dirección (Huggins, 2020).

Este paso consiste en identificar y documentar los activos de información de la organización, así como su interrelación y su valor, en el sentido de qué perjuicios o costos supondría su degradación. Para llevar a cabo esta labor se debe tener en cuenta:

i. El activo esencial es la información que maneja el sistema, es decir los datos que se capturan, se alojan, se procesan y se transmiten a través de este.
ii. Los servicios que se prestan con base a los datos, así como aquellos servicios de soporte y gestión.
iii. El software que permite procesar los datos y desplegarlos para su empleo por parte de los servicios y sistemas de información.
iv. Los equipos informáticos y el hardware que permite hospedar datos, aplicaciones y servicios.
v. Los soportes de información como dispositivos de almacenamiento de datos, de back-up y de respaldo.
vi. El equipamiento auxiliar, que complementa el material informático.
vii. Las redes de comunicaciones que proporcionan el intercambio de información.
viii. Las instalaciones físicas en donde se alojan tanto equipos informáticos y de comunicaciones como las personas y las actividades productivas de la organización.
ix. Finalmente, las personas que operan e interactúan con todos los elementos anteriormente citados.

En esta fase, una de las dificultades radica en la identificación de la misión de la organización, teniendo en cuenta que se delimitó el alcance a la Dirección de Tecnología y Sistemas de Información, para posteriormente identificar aquellos activos de información y comunicaciones que aportan en mayor medida a este objetivo al interior de la DSTI y cómo desde el punto de vista de la DTSI existen potestad y dominio de la información necesaria para reunir la información para los pasos siguientes, así como para eventualmente poner en marcha las medidas y recomendaciones pertinentes.

3.3. Determinar a qué amenazas están expuestos aquellos activos

Este paso consiste en determinar las amenazas a las que está expuesto cada uno de los activos identificados.

Las amenazas son eventos desastrosos intencionales o no intencionales que podrían ocurrir y conllevar un impacto directo sobre los activos, causando un daño o afectación a los intereses de la organización. (Centro Criptológico Nacional de España, n.d.)

Pueden existir eventos desastrosos que son generados por la naturaleza como terremotos e inundaciones o desastres de tipo industrial como contaminación o fallos eléctricos, entre muchos otros, ante los cuales el sistema de información es víctima pasiva. Sin embargo, ser pasivos no significa permanecer indefensos; se requiere contar con las medidas de mitigación, detección y reacción que pueden contribuir a evadir completamente el impacto de un desastre, a contener sus consecuencias o a erradicarlas definitivamente para luego seguir con una recuperación oportuna.

Por otro lado, existen también amenazas o ataques intencionales por parte de terceros que pueden beneficiarse de los daños causados a la organización; o que simplemente tienen como objetivo afectar a la organización por intereses como el lucro, la competencia o el espionaje.

Durante la realización de este trabajo fue necesario establecer la claridad de que no todas las amenazas afectan a todos los activos, en contraste a esta idea, existe una relación entre los diferentes tipos de activos y las amenazas que pueden materializarse en torno a ellos. Por ejemplo, las instalaciones físicas podrían ser afectadas por inundaciones o daños eléctricos, mientras que las personas podrían ser objeto de tácticas de engaño o de coacción; por su parte las aplicaciones de software podrían ser atacadas por virus informáticos o intrusiones de software espía.

Para el desarrollo de este paso fue necesario realizar también un trabajo de sensibilización en el que se ayudó al equipo de la DSTI a reconocer objetivamente las amenazas sobre los activos, combatiendo la idea de que todos los ataques son posibles sobre todos los activos y de que todas las consecuencias podrían ser igualmente graves sin distinguir los atributos de seguridad que han sido afectados o en qué medida.

3.3.1. Valoración de las Amenazas

Cuando una amenaza se materializa, no todos los activos se ven afectados en las mismas dimensiones ni en la misma cuantía.

Una vez se ha determinado que una amenaza puede afectar un activo es necesario estimar qué tan vulnerable es dicho activo ante esta amenaza en dos sentidos:

- **Degradación**: mide el daño causado por un incidente. Se puede expresar como una fracción del valor del activo, de manera que se puede llegar a definir si un activo se ha visto degradado en un porcentaje de su valor o en su totalidad (Centro Criptológico Nacional, 2010).
- **Frecuencia**: Ayuda a determinar cada cuanto tiempo se materializa una amenaza (Centro Criptológico Nacional, 2010).

De esta manera se hace posible la identificación y agrupamiento de amenazas por el nivel de degradación causado y la frecuencia estimada. Luego de este análisis podrían existir, por lo tanto, amenazas de muy altas consecuencias, pero de muy improbable materialización; así como amenazas que se pueden presentar frecuentemente, pero generar un impacto de muy baja degradación. También puede darse el caso de amenazas que degradan levemente los activos pero que, acumulando esta degradación con otras amenazas o con nuevas materializaciones de la misma amenaza, pueden llegar a generar una degradación de mayor importancia.

La frecuencia se modela como una tasa anual de ocurrencia. Es posible asignar una escala arbitraria de acuerdo con las necesidades del caso, pero a continuación de presenta el ejemplo de una escala de 4 niveles:

- **100**, muy frecuente. Podría llegar, inclusive, a hablarse de incidentes diarios
- **10,** frecuente. Sucede al menos una vez al mes.
- **1,** normal. Puede presentarse por lo menos una vez al año.
- **0.1,** muy poco frecuente. Puede presentarse una vez en el lapso de varios años.

3.4. Determinar Medidas y Salvaguardas

Este paso comprende la definición de los procedimientos, mecanismos de control y medios tecnológicos que reducen o bien la frecuencia de las amenazas o, por otro lado, el nivel de degradación de los activos ante la materialización de las amenazas. Existen amenazas que pueden evitarse simplemente organizando adecuadamente los activos y los procesos de la organización. Sin embargo, otras requieren elementos técnicos como aplicaciones de software o equipos especializados. También existen otras que requieren seguridad física, más allá de las herramientas tecnológicas y, por último, también se encuentran las políticas del personal y los protocolos para la realización de las actividades propias de la organización.

Las medidas y salvaguardas influyen en el cálculo del riesgo de dos maneras:

- **Reducir la frecuencia de ocurrencia de una amenaza**, de manera que se les puede llegar a llamar Salvaguardas Preventivas. Aquellas salvaguardas preventivas ideales son aquellas que llegan a impedir completamente la ocurrencia de una amenaza.

- **Limitar la afectación generada al o los activos involucrados**, puede tratarse de salvaguardas que reducen o impiden la degradación de los activos ante la ocurrencia de una amenaza; o aquellas que detectan la materialización de una amenaza a fin de permitir una reacción oportuna impidiendo que la misma avance y degrade aún más los activos afectados. También existen salvaguardas que permiten una recuperación efectiva y óptima cuando los activos son degradados hasta un punto grave o crítico. De cualquier forma, estas salvaguardas están orientadas a reducir las consecuencias, mas no a impedir que las amenazas de materialicen.

Las salvaguardas se caracterizan por ser acciones, mecanismos o herramientas que se han puesto en marcha para mitigar o anular una amenaza. No puede considerarse salvaguarda a elementos, personas o definiciones

que no deben su existencia a este propósito. Además, las salvaguardas se miden por su eficacia para mitigar la amenaza que se pretende controlar.

Una salvaguarda ideal sería aquella que es 100% eficaz en la reducción de la degradación de los activos o en la materialización de una amenaza particular. Esto implica que la salvaguarda debería ser en teoría idónea, es correctamente desplegada, configurada y mantenida, se emplea siempre y existen procedimientos claros de uso bajo condiciones normales y uso bajo afectación por una incidencia.

Los usuarios, por su parte, deben ser informados y entrenados en el uso de las salvaguardas y deben existir controles que permitan alertar acerca de posibles fallos.

Para cada salvaguarda se debe calcular su nivel de eficacia, que debería ir desde un 0% para aquellas que no son eficaces en lo absoluto, hasta un 100% para aquellas que cuentan con una eficacia perfecta. Sin embargo, esta medida debe ser realista y derivada de análisis y estadísticas apropiadas y corroborabas.

3.5. Estimación del Impacto

El impacto se define por el daño causado a un activo, derivado de la materialización de una amenaza. Usualmente la valoración de un sistema de información está dada por la información que este maneja y por los servicios que presta. Al conocer el valor de los activos y la degradación que eventualmente podría causar una amenaza sobre los mismos, se puede establecer cuál será el impacto de dichas amenazas sobre el sistema. Podría ser necesario, sin embargo, tener en cuenta la dependencia entre los diferentes activos, ya que la degradación de uno podría implicar también la degradación de otros que dependen de él y, de esta manera, se multiplica el impacto de la amenaza.

Para recabar esta información el trabajo se basó en la experiencia de los colaboradores de la Dirección de Tecnología y Sistemas de Información a través de diferentes reuniones y entrevistas con el equipo de trabajo. También se indagó por información histórica referente a los incidentes conocidos de los últimos meses con el fin de tabular los aspectos de seguridad que fueron comprometidos, así como naturaleza y gravedad de los incidentes.

3.6. Estimación del Riesgo

Usualmente el riesgo se calcula como el impacto ponderado por la tasa de ocurrencia de la amenaza. Así, un riesgo es la medida del daño probable sobre un sistema.

Al conocer el impacto de las amenazas sobre los activos y la frecuencia de ocurrencia de las amenazas, se calcula directamente el riesgo a través de la combinación de estos dos valores.

$$Valor\ del\ Riesgo = Impacto\ Ponderado\ *\ Tasa\ de\ Ocurrencia$$

Además del riesgo estimado, también existen otras medidas del riesgo que es necesario tener en cuenta:

- **Riesgo acumulado**: se calcula sobre los activos teniendo en cuenta el impacto sobre un activo y otros activos que dependen del primero, causado por la materialización de una amenaza (Centro Criptológico Nacional de España, n.d.). El cual es multiplicado por la frecuencia o probabilidad de ocurrencia de dicha amenaza. Este debe ser calculado para cada activo y para cada una de las amenazas, de manera que existe un valor de riesgo acumulado para cada activo en conjunto con cada una de las amenazas que le pueden llegar a impactar. (Centro criptológico Nacional de España, 2012)

$$Riesgo\ Acumulado = Impacto\ Acumulado\ *\ Tasa\ de\ Ocurrencia$$

- **Riesgo repercutido**: este se calcula tomando en cuenta el impacto sobre un activo a causa de la degradación de otros activos de los que este depende causada por la materialización de una amenaza (Centro Criptológico Nacional de España, n.d.). De manera que un activo que se degrada a causa de la degradación de un activo del que este depende genera una repercusión más alta dentro de la organización. El riesgo repercutido estima, entonces, el daño a la organización propiamente a través del cálculo del daño en los activos explícitamente valorados. (Centro criptológico Nacional de España, 2012)

$$Riesgo\ Repercutido = Impacto\ Repercutido\ *\ Tasa\ de\ Ocurrencia$$

- **Riesgo Residual**: El riesgo residual es el riesgo remanente después de que se ha puesto en marcha una contramedida (Centro criptológico Nacional de España, 2012)

Posterior al análisis de los riesgos, se procedería con la etapa de gestión de riesgos, en la cual se establece un tratamiento para los riesgos identificados, acorde con el apetito de riesgos de la organización y en sintonía con sus objetivos y sus operaciones.

Para aquellos riesgos que son aceptados o transferidos se toman las acciones de documentación, negociación y sensibilización de los interesados. Mientras que para los riesgos que son rechazados se requiere una estrategia de replanteamiento de los procesos y operaciones de manera que el riesgo pueda ser evitado definitivamente.

Por otro lado, para aquellos riesgos que se decide controlar, se definen y se ponen en marcha los indicadores de control, los indicadores de compromiso, las salvaguardas y las medidas que se hayan definido a través de este proceso.

4. Conclusiones

- La metodología de ponderación de criterios nos permitió abordar y evaluar holísticamente diferentes opciones metodológicas que posibilitaban realizar el análisis de riesgos, cada una con sus ventajas y dificultades propias. Pudimos despejar y expresar claramente los criterios que condicionaban nuestro proyecto para posteriormente equiparar las diferentes opciones disponibles. Consiguientemente apreciar con mayor claridad y criterio la opción más efectiva en función de las condiciones planteadas.

- Magerit es una opción práctica, de rápida adopción y con una curva de aprendizaje que se extiende en el orden de semanas y que permite obtener avances en el corto plazo respecto a la evaluación de riesgos en seguridad de la información. Su uso permite valorar los riesgos en cuanto a dimensiones como costo, degradación, frecuencia e impacto; de manera que se pueden estimar de manera procedimental aspectos como el costo del impacto, la efectividad de las salvaguardas y la eficiencia de los controles con lo cual se posibilita que se presenten datos y hechos concretos que fundamentan la percepción de los riesgos y respaldan la efectividad de los controles. Este ejercicio adquiere mayor importancia ante aspectos como la justificación de los costos y esfuerzos asociados del análisis y gestión de los riesgos en seguridad de la información y para cuantificar los resultados de dichos esfuerzos.

- A pesar de las diferencias en cuanto a tamaño, funcionamiento, misión y visión; las instituciones de educación superior en Colombia comparten un conjunto de amenazas en cuanto a seguridad de la información que podrían ser percibidas como riesgos sectoriales y, por ende, este estudio y otros en el sector podrían aportar conocimiento útil para construir una base de conocimiento y un esfuerzo común de protección que apalanque la ciberdefensa del sistema de educación superior en el país.

- Algunos de los riesgos más severos se ubican en el extremo del espectro que corresponde al recurso humano, de manera que los controles, medidas y políticas, más allá de las restricciones tecnológicas, deben enfocarse en tareas de entrenamiento, concienciación, proactividad y compromiso de los colaboradores y usuarios de las instituciones.

- Una dificultad importante a sopesar en el desarrollo de este trabajo, así como en otros proyectos de análisis de riesgos, es la convicción por parte de las organizaciones y algunos de sus directivos de que la seguridad de la información reposa exclusivamente en la implementación apresurada de soluciones y configuraciones tecnológicas sin tener en cuenta un análisis de riesgos que priorice los

controles a implementar y que de origen a un sistema de gestión de seguridad de la información que incluya controles procedimentales y metodológicos más allá de las herramientas tecnológicas.

- Otra tendencia errada que pudimos identificar es la concepción de que los riesgos en seguridad se pueden mitigar completamente a través de la ejecución de pruebas de penetración sobre las plataformas y sistemas de la organización. A pesar de que esta práctica puede arrojar alguna noción sobre la idoneidad de las soluciones técnicas configuradas, sin un análisis de riesgos con sus consiguientes recomendaciones y mitigaciones, estas pruebas no acercan la organización hacia ningún objetivo ni permiten medir la efectividad de un conjunto concreto de medidas y controles. Es necesario encausar los esfuerzos primero hacia el análisis de riesgos, para luego establecer los controles más pertinentes y posteriormente determinar un plan de pruebas y verificaciones que ayude a obtener métricas de efectividad y evolución de las actividades de protección, procurando un entorno de trabajo cuantificable y medible.

5. Bibliografía

Betancourt, D. F. (24 de Noviembre de 2018). *Cómo hacer una matriz de priorización*. Obtenido de Ingenio Empresa: https://www.ingenioempresa.com/matriz-de-priorizacion/

Centro Criptológico Nacional. (2010). *Degradación causada por una amenaza* . Obtenido de EAR / PILAR: https://www.pilar-tools.com/es/glossary/index.html?n=DegradaciNCausadaPorUnaAmenaza.html

Centro Criptológico Nacional. (2010). *Frecuencia*. Obtenido de EAR / PILAR: https://www.pilar-tools.com/es/glossary/index.html?n=DegradaciNCausadaPorUnaAmenaza.html

Centro Criptológico Nacional de España. (s.f.). *Amenaza*. Obtenido de Guias Generales, Glosario de Abreviaturas: https://www.ccn-cert.cni.es/publico/seriesCCN-STIC/series/400-Guias_Generales/401-glosario_abreviaturas/topics/44.html

Centro Criptológico Nacional de España. (s.f.). *Riesgo*. Obtenido de Guias Generales, Glosario de Abreviaturas: https://www.ccn-cert.cni.es/publico/seriesCCN-STIC/series/400-Guias_Generales/401-glosario_abreviaturas/index.html?n=796.html

Centro Criptológico Nacional de España. (s.f.). *Riesgo Residual*. Obtenido de Guias Generales, Glosario de Abreviaturas: https://www.ccn-cert.cni.es/publico/seriesCCN-STIC/series/400-Guias_Generales/401-glosario_abreviaturas/index.html?n=797.html

Centro criptológico Nacional de España, n. (10 de 2012). *Magerit V3, Libro 1 - Metodo.* Obtenido de Administración electronica del gobierno español: https://administracionelectronica.gob.es/pae_Home/dam/jcr:fb373672-f804-4d05-8567-2d44b3020387/2012_Magerit_v3_libro1_metodo_es_NIPO_630-12-171-8.pdf

European Agency for Cybersecurity. (04 de Abril de 2018). *Mehari*. Obtenido de ENISA: https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-methods/m_mehari.html

Huggins, P. (14 de 04 de 2020). *What are Information Assets?* Obtenido de Black Swan Security: https://blog.blackswansecurity.com/2020/04/what-are-information-assets/

International Standard Organization. (Julio de 2018). *ISO/IEC 27005:2018*. Obtenido de International Standard Organization: https://www.iso.org/standard/75281.html

Microsoft. (27 de Agosto de 2021). *Risk management overview*. Obtenido de Microsoft Documentation: https://docs.microsoft.com/en-us/compliance/assurance/assurance-risk-management

National Institute of Standards and Technology. (Septiembre de 2012). *Guide for Conducting Risk Assessments*. Obtenido de Computer Security Resource Center: https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final

Radigan, D. (s.f.). *Puntos de historia y estimación*. Obtenido de Atlassian Agile Coach: https://www.atlassian.com/es/agile/project-management/estimation

Redacción Educación. (28 de 06 de 2021). *Universidad El Bosque sufre ataque informático*. Obtenido de El Tiempo: https://www.eltiempo.com/vida/educacion/universidad-el-bosque-sufre-ataque-informatico-599303

Redacción Universidad. (14 de 04 de 2021). *Ataque informático a la Universidad de los Andes ¿Qué hacer para protegerse?* Obtenido de Periódico Al Derecho: https://alderecho.org/2021/04/14/ataque-informatico-a-la-universidad-de-los-andes-que-hacer-para-protegerse/

Secretaría General de Administración Digital. (Octubre de 2012). *Cover of MAGERIT v.3: Analysis and risk Management information systems*. Obtenido de Portal de Administración Electrónica: https://administracionelectronica.gob.es/pae_Home/en/pae_Documentacion/pae_Metodolog/pae_Magerit.html?idioma=es

Secrtetaría de Administración Digital. (10 de 2012). *MAGERIT v.3 : Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información*. Obtenido de Portal de Administración Electrónica: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html

Vargas, R. V. (12 de 10 de 2010). *Using the analytic hierarchy process (ahp) to select and prioritize projects in a portfolio*. Obtenido de Project Management Institute: https://www.pmi.org/learning/library/analytic-hierarchy-process-prioritize-projects-6608