Diseño del Sistema de Gestión de Riesgos de Seguridad de la Información para una Institución Militar en Colombia.

Nicolas B. Lugo, Jaiber E. Gómez y Fabio E. Sandoval. Estudiantes del curso Proyecto Final, Maestría Seguridad de la Información, Universidad de los Andes.

Resumen

Este proyecto tuvo como punto de partida un análisis de riesgos de seguridad de la información, que permitió cuantificar y comparar el estado general de la seguridad de la información con las salvaguardas implementadas para su cumplimiento y de acuerdo con las diferencias encontradas, se definió un Plan de Seguridad completo con salvaguardas y controles adicionales para el cumplimiento de todos los requisitos previamente definidos al interior de la institución Militar.

Es por ello, que este proyecto aborda la problemática asociada a la falta de un Sistema de Gestión de Riesgos de Seguridad de la Información para una Institución Militar en Colombia, lo cual genera una situación de posible compromiso y afectación a la infraestructura tecnológica de esta institución, al no poder tener un panorama claro acerca de la exposición ante los riesgos actuales e incluso ante los riesgos emergentes, los cuales en la última década han ido creciendo según el informe de amenazas 2022 de BlackBerry. (Informe de amenazas de Ciberseguridad 2022).

Para atender esta necesidad, se realizó un análisis inicial de la situación, apalancados con la metodología y marco de referencia de Magerit, apropiando las fases de implementación y los hitos propios de la metodología, así como de las mejores prácticas y recomendaciones descritas en la misma, teniendo en cuenta lo anterior, se realizó el diseño de un Sistema de Gestión de Riesgos de Seguridad de la Información, con el objetivo de gestionar y mantener adecuadamente la confidencialidad, integridad y disponibilidad de los activos de información de la institución, mediante una adecuada gestión y análisis de riesgos.

Dentro de la fase de implementación sugerida, y para poder brindar una solución dentro de los tiempos establecidos, se contemplaron cinco fases, dentro de las cuales se abordó la definición de la Metodología, elaboración de matriz de riesgos, método de análisis de riesgos, procesos de gestión de riesgos y como resultado se obtuvo el Plan de Seguridad. En la implementación parcial del mismo, se obtuvieron resultados satisfactorios al lograr implementar mejoras al control de accesos a través de contraseñas más robustas y se recibió una retroalimentación positiva por parte de la institución.

Finalmente, para el desarrollo e implementación de este proyecto, es importante que sea organizado de acuerdo con las cinco fases proyectadas, así mismo, con las principales activades que en cada una de ellas se establecen.

Palabras clave: Magerit, Riesgos, Gestión de Riesgos, SGR, Institución Militar.

Abstract

This project had as its starting point an analysis of initial information security risks, which allowed quantifying and comparing the general state of information security with the safeguards implemented for its compliance and, according to the differences found, a Complete Security Plan with additional safeguards and controls to comply with all previously defined requirements within the Military institution.

That is why this project addresses the problems associated with the lack of an Information Security Risk Management System for a Military Institution in Colombia, which generates a situation of possible compromise and affectation of the technological infrastructure of this institution. , by not being able to have a clear picture about the exposure to current risks and even to emerging risks, which in the last decade have been growing according to the BlackBerry 2022 threat report. (2022 Cybersecurity Threat Report).

To meet this need, an initial analysis of the situation was carried out, leveraged with Magerit's methodology and reference framework, appropriating the implementation phases and milestones of the methodology, as well as the best practices and recommendations described therein. Considering the above, the design of an Information Security Risk Management System was carried out, with the objective of adequately managing and maintaining the confidentiality, integrity, and availability of the institution's information assets, through an adequate risk management and analysis.

Within the suggested implementation phase, and in order to provide a solution within the established times, five phases were contemplated, within which the definition of the Methodology, preparation of the risk matrix, risk analysis method, processes risk management and as a result the Safety Plan was obtained. In its partial implementation, satisfactory results were obtained by implementing improvements to access control through more robust passwords and positive feedback was received from the institution.

Finally, for the development and implementation of this project, it is important that it be organized according to the five projected phases, likewise, with the main activities that are established in each of them.

Keywords: Magerit, Risks, Risk Management, SGR, Military Institution.

I. DESCRIPCIÓN DEL PROBLEMA

Los ataques cibernéticos crecen en número y sofisticación, poniendo en riesgo la información, es por ello, que las amenazas se perciben cada vez más como un problema de seguridad Nacional e Internacional, haciendo que las Organizaciones sean vulnerables a innumerables amenazas que afectan la confidencialidad, integridad y disponibilidad de la información, razón por la cual se requiere de herramientas para anticipar, disminuir y contrarrestar el impacto de eventos inesperados que pueden afectar el cumplimiento de la misión y visión de las instituciones Militares.

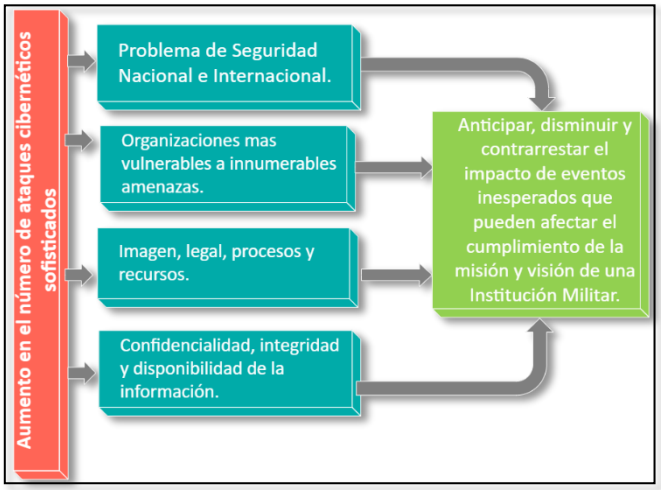


Ilustración 1. Descripción del problema.

De acuerdo con lo anterior, es imperativo establecer un análisis de riesgos que permita identificar, clasificar y valorar los eventos que pueden afectar la infraestructura tecnológica de la institución, y de esta forma poder establecer las salvaguardas necesarias para reducir el impacto hasta un nivel tolerable.

Todas las Instituciones necesitan establecer un Sistema de Gestión de Riesgo de Seguridad de la Información, debido a la situación actual en el área de ciberataques. “En 93 por ciento de los casos, un atacante externo puede penetrar la red de una Institución y obtener acceso a los recursos de esta” (Brooks, 2022).

Teniendo esto en cuenta, cada vez se vuelve más apremiante, que las Instituciones que no tienen un Sistema de Gestión de Riesgos de Seguridad de la Información queden expuestas tanto a ataques que lleven a filtración de datos por parte de atacantes como a fuga de información por parte de funcionarios de la institución hasta obtener permisos de comando y control de la infraestructura misma.

La filtración de datos por parte de los atacantes ocurre porque las Instituciones Militares tienen información confidencial privilegiada tanto de la misma institución como de sus proveedores. La filtración ocurre a través del uso de un programa malicioso, ingeniería social y/o vulnerabilidades en los sistemas para obtener permisos y acceso a estos. (UpGuard, 2022). Una vez que el atacante tiene acceso a la información, puede publicarlas o cifrar de forma que las Instituciones no puedan acceder a ella y pedir un dinero por devolverla.

En el caso de las Instituciones Militares en Colombia, poseen una gran cantidad de información clasificada como reservada sobre actividades operacionales que se relacionan directamente con la Seguridad Nacional. Tener una filtración de datos podría ocasionar efectos devastadores para las actividades y operaciones realizadas por cada una de ellas. Adicionalmente, podría estar expuesta a ejecución de Ransomware, teniendo un efecto negativo en el cumplimiento de la misión y visión Institucional. (Ries, 2022).

Otro problema que puede sufrir una Institución Militar sucede cuando un atacante logra tener acceso a los sistemas de información y realiza modificaciones a los archivos que contienen información confidencial para obtener un beneficio personal, causando una gran afectación para la institución. (Sutcliffe, 2022). En el caso de las Instituciones Militares en Colombia, esto podría tener repercusiones en la toma de decisiones a nivel Operacional, táctica y/o Actividades Militares.

Todas las organizaciones son blanco de estos tipos de ataques y riesgos de seguridad de la información, pero dependiendo qué tan bien preparados estén se puede minimizar el impacto y reducir la afectación que se sufran. (Team, 2022). En esto radica la urgencia e importancia de la implementación de un Sistema de gestión de riesgos de Seguridad de la Información, permitiendo a las Instituciones Militares establecer protocolos de respuesta a las diferentes amenazas y riesgos, de forma que estén preparadas tanto preventiva como reactivamente.

Finalmente, las Instituciones Militares deben contar con una gestión integral de riesgos de Seguridad de la Información, basada en una estrategia de carácter preventivo y reactivo, de manera que, al comprender el concepto de riesgo, se desarrollen acciones que mitiguen la afectación al cumplimiento de la misión y visión Institucional, y en caso de materialización se contemplen estrategias para la identificación, análisis, tratamiento, evolución y monitoreo de dichos riesgos con una mayor objetividad. (Emerald Insight, 2022).

Teniendo presente lo anterior, se plantea realizar el diseño del Sistema de Gestión de Riesgos de Seguridad de la Información para una Institución Militar en Colombia, con el objetivo de

evaluar los activos de información, las amenazas que existen y las salvaguardas que se deben implementar consolidando de esta forma el Plan de Seguridad, con el fin de asegurar el cumplimiento de la Misión y Visión de las Instituciones Militares, y de esta forma proteger y prevenir de forma efectiva la información de cada una de ellas.

II. MARCO TEÓRICO

A continuación, se define cada uno de los componentes esenciales que hacen parte del marco de referencia, permitiendo de esta forma dar sustento para el desarrollo del diseño del Sistema de Gestión de Riesgos de Seguridad de la Información para una Institución Militar en Colombia.

Así mismo se realiza la descripción de los principales modelos y metodologías de análisis de riesgos de seguridad de la Información, definiendo por separado cada una de ellas.

A. Análisis de riesgos de seguridad de la información

Actualmente, el análisis de riesgos de seguridad de la información está orientado, por una parte; a la identificación de los activos de información a proteger, y por otra; a identificar las amenazas que pueden producir pérdidas sobre estos activos, una vez se logra identificar estas amenazas es importante establecer las salvaguardas que permitirán proteger los activos de posibles amenazas latentes. De acuerdo con lo anterior, la cuantificación de estos elementos hace parte del análisis de riesgos proyectado en el diseño del Sistema de Gestión de Riesgos de Seguridad de la Información para una Institución Militar en Colombia.

De la misma forma, es importante dar a conocer que el ejercicio de análisis de riesgos no debe estar aislado de las demás estrategias para incrementar el nivel de seguridad, dicho lo anterior, el poder establecer una línea base que conforme un esquema de medidas básicas de seguridad, que a la vez deben ser cumplidas a nivel transversal por toda la Institución, permitiendo de esta forma mitigar los niveles de riesgo a que pueda estar expuesta.

Dentro de la fase de Análisis de Riesgos, se tuvieron en cuenta varios aspectos, donde principalmente se contemplaron las definiciones y buenas prácticas de la metodología Magerit, pero también las sugerencias realizadas por el equipo académico que acompañó al proyecto durante todo su desarrollo.

De acuerdo con el análisis realizado en otras instituciones colombianas, el sistema de gestión es bastante similar al planteado para la Institución Militar en Colombia, teniendo presente que son implementados de acuerdo con lo establecido por la metodología de Magerit, donde se evalúan los diferentes escenarios y se establecen salvaguardas para mitigar posibles riesgos que se pueden presentar a la infraestructura tecnológica.

En el caso de Instituciones Militares de Estados Unidos, tienen un sistema de gestión llamado Operational Risk Management (ORM) donde establecen procedimientos para el manejo de riesgos y amenazas. Este sistema de gestión se basa en 4 principios: Aceptar el riesgo cuando el beneficio es mayor que el costo, no aceptar riesgos innecesarios, Anticipar y manejar riesgos al tener planes y hacer decisiones sobre el riesgo a los niveles correctos. Teniendo estos principios en cuenta, se establecen tres indicadores para la medición de los protocolos. El primero es monitoreo de la efectividad de los protocolos, con el propósito de revisar cuantos riesgos han sido gestionados por este medio. A partir de ese análisis se establece el indicador que necesita mayor evaluación. En caso de que el protocolo no este gestionando correctamente los riesgos, es necesario realizar una evaluación detallada de los riesgos y qué cambios causan que no se esté gestionando el riesgo correcto. El último de los indicadores es establecer un procedimiento que registra todos los aprendizajes.

Por último, en el caso del ejército de Estados Unidos, esta Institución tiene un sistema de gestión propio que se basa en cinco principios:

1. Incorporar los sistemas de gestión de riesgo y sus principios a todos los integrantes de la organización.
2. Integrar los requerimientos de seguridad en todos los procesos de la organización.
3. Establecer límites de los grupos de la Institución para manejar el acceso a la información correctamente.
4. Categorizar los riesgos.
5. Planear para el manejo de riesgo.

Teniendo en cuenta estos principios se estableció unos protocolos de seguridad.
Para el monitoreo de estos protocolos se establecen 2 procedimientos:

1. Revisar la disponibilidad de los procedimientos de los riesgos y que tan efectivos son.
2. Monitorear los protocolos en intervalos establecidos para que ningún riesgo efectivo.

Teniendo en cuenta los diferentes indicadores se establecen los siguientes:

1. Monitoreo en intervalos establecidos por la Institución que permitan manejar la efectividad de los protocolos y su disponibilidad.
2. Establecer evaluaciones periódicas para los protocolos en caso de que sea necesario una evaluación detallada y revisar cuantos necesitan esta evaluación.
3. Registrar todos los incidentes para no repetir errores pasados.

III. METODOLOGÍAS DE ANÁLISIS Y GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

En la revisión realizada sobre varias fuentes y estándares encontramos los siguientes como los más representativos: Octave, Magerit, ISO31000, Mehari y NIST 800-30.

1. **OCTAVE** (Operationally Critical Threat, Asset and Vulnerability Evaluation): Desarrollado en la Universidad de Carnegie Mellon, es una metodología para recoger y analizar información de manera que se pueda diseñar una estrategia de

protección y planes de mitigación de riesgo basados en los riesgos operacionales de seguridad de la organización. Hay dos versiones, una para grandes organizaciones y otra para pequeñas, de menos de 100 colaboradores. (Análisis Comparativo: Metodologías de análisis de Riesgos, 2022).

2. **MAGERIT**: Metodología de análisis y gestión de riesgos de TI desarrollado por el Consejo Superior de Administración Electrónica y publicado por la Institución de administraciones públicas español, es una metodología de análisis de riesgos que describe los pasos para realizar un análisis del estado de riesgo y para gestionar su mitigación, detalla las tareas para llevarlo a cabo de manera que el proceso esté bajo control en todo momento y contempla aspectos prácticos para la realización de un análisis y una gestión realmente efectivos. (Introducción al análisis de riesgos – Metodologías, 2022).

3. **ISO 31000:** Es una norma internacional que ofrece las directrices y principios para gestionar el riesgo de las organizaciones. Esta norma fue publicada en 2018 por la Institución Internacional de Normalización (ISO) en colaboración con IEC, y tiene por objetivo que organizaciones de todos los tipos y tamaños puedan gestionar los riesgos en la empresa de forma efectiva, por lo que recomienda que las organizaciones desarrollen, implanten y mejoren continuamente un marco de trabajo cuyo objetivo es integrar el proceso de gestión de riesgos en cada una de sus actividades.

   El propósito del marco de referencia de la gestión del riesgo es asistir a la Institución en integrar la gestión del riesgo en todas sus actividades y funciones significativas. La eficacia de la gestión del riesgo dependerá de su integración en la gobernanza de la organización, incluyendo la toma de decisiones. Esto requiere el apoyo de las partes interesadas, particularmente de la alta dirección.

   El desarrollo del marco de referencia implica integrar, diseñar, implementar, valorar y mejorar la gestión del riesgo a lo largo de toda la organización. (ISO 31000:2018 Gestión del riesgo, 2022).

4. **MEHARI**: Desarrollada por la CLUSIF (CLUb de la Sécurité de l'Information Français) en 1995 y deriva de las metodologías previas Melissa y Marion; es una Metodología de análisis de riesgo que cuenta con un modelo de evaluación de riesgos y módulos de componentes y procesos. Con MEHARI se detectan vulnerabilidades mediante auditorías y se analizan situaciones de riesgo. (Introducción al análisis de riesgos – Metodologías, 2022).

5. **NIST 800-30**: hace parte de los estándares de la serie SP-800 dedicada a la seguridad de la información y desarrollada por el NIST (National Institute of Standards and Techonogy); La publicación de esta guía se realizó en julio de 2002, tiene como principios: suministrar una base para el desarrollo de la gestión del riesgo y suministrar información acerca de controles de seguridad en función de la rentabilidad del negocio. (Análisis Comparativo: Metodologías de análisis de Riesgos, 2022).

IV. PLANIFICACIÓN DEL PROYECTO

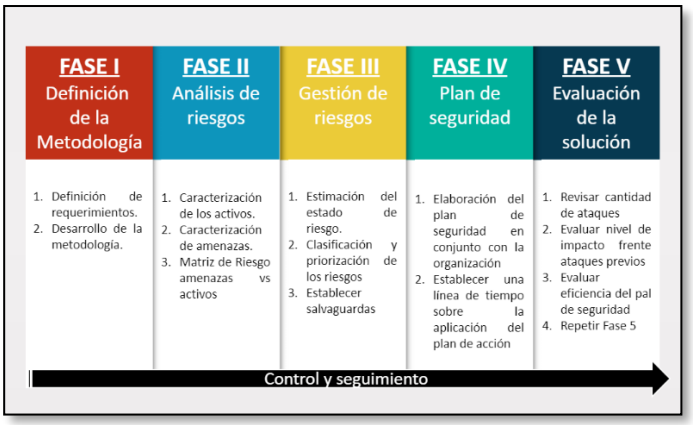


Ilustración 2. Fases del proyecto.

El desarrollo del presente proyecto se ha estructurado en cinco fases, las cuales se dan a conocer a continuación, junto con las actividades que se deben desarrollar en cada una de ellas.

El objetivo de cada fase es el siguiente:

- **FASE I: Definición de la Metodología**
  Se define la metodología a implementar, tomando como punto de partida las metodologías identificadas para la gestión de riesgos y se adapta a los requerimientos específicos para la Institución.

- **FASE II: Análisis de riesgos**
  Se utiliza la metodología y la matriz de riesgos para realizar el análisis de riesgos que soportara la implementación del Sistema de gestión de riesgos de seguridad de la información.

- **FASE III: Gestión de riesgos**
  Con base a la información obtenida de la fase anterior, se deben clasificar los riesgos

identificados dependiendo del impacto que puede tener de diferentes formas en la organización.

- **FASE IV: Plan de seguridad**
  En esta fase, se realiza la elaboración del plan de seguridad con el objetivo de mejorar la implantación de una serie de salvaguardas que lleven impacto y riesgo a los niveles residuales previamente establecidos.

- **FASE V: Evaluación de la Solución**
  En esta fase, se realiza se realiza evaluación y monitoreo de los cambios realizados de forma que se pueda evaluar la efectividad de estos.

V. IMPLEMENTACIÓN DEL PROYECTO

A. FASE I: Selección de la Metodología

La primera fase se concentró en la selección de la metodología, al hacer la revisión de cada metodología, se concluye que no todas son "metodologías", es decir, Magerit, Mehari y Octave son metodologías, pero ISO 31000 y NIST 800-32 son solo marcos de referencia, Frameworks o buenas prácticas. Octave inicialmente fue desarrollada para el sector militar y luego liberada para aplicaciones civiles, dividiéndose para grandes y pequeñas empresas; Magerit, por otra parte, está totalmente orientada a costos. También es la opción más efectiva y completa porque se enfoca en la gestión del riesgo de la información en cuanto a integridad, confidencialidad, disponibilidad y otras características importantes para garantizar la seguridad de los sistemas y procesos de la organización. Por estas razones se tomó la decisión de seleccionar Magerit como la metodología a utilizar para realizar el Sistema de Gestión de Riesgos de seguridad de la información para una Institución Militar en Colombia. (Análisis de riesgos en seguridad de la información, 2022).

Adicionalmente, se encuentra implementado en una variedad de sectores, desde organizaciones propias de TI, sector financiero, hasta la industria de petróleo y gas.

Ofrece características propias como: Base de activos bien estructurada, establece un gobierno de riesgo de TI bien definido, genera una disciplina y cultura de conciencia relacionada con el riesgo.

Presenta técnicas generales para el desarrollo de la gestión del riesgo entre las que encontramos:

- Análisis costo – beneficio.
- Diagramas de flujo de datos (DFD)
- Diagramas de procesos (SADT)
- Técnicas gráficas: GANTT, histogramas, diagramas de Pareto y Pie.
- Técnicas de planificación y gestión de proyectos (PERT)
- Sesiones de trabajo: entrevistas, reuniones y presentaciones.
- Valoraciones Delphi.

Magerit, como metodología, está orientada a manera de proyecto, donde se cuenta con un circuito de retroalimentación y mejora continua, contando con la posibilidad de abordar riesgos emergentes en el futuro e ir afinando cada vez más el sistema según las necesidades y los cambios organizacionales que se presenten.

Finalmente, la versión 3 de Magerit cuenta con una mejor alineación con ISO 31000, integrando las tareas de análisis de riesgos dentro de un marco organizacional de gestión de riesgos dirigido desde los órganos de gobierno de TI.

B. FASE II: Análisis de Riesgos

En la segunda fase se tuvo presente el análisis de riesgos, donde primero se identificaron los riesgos a los activos y amenazas futuras. Después de eso se debe establecer el impacto que tienen cada uno de los riesgos y amenazas. Por último, se deben establecer salvaguardas y formas de gestionar el impacto. Para esto es necesario un análisis de que partes de la Institución se van a cubrir con el procedimiento y quienes son los responsables en el manejo y tratamiento de los riesgos.

Luego se generó un entregable que se basa en 2 matrices de riesgo. En la primera matriz, uno de los ejes debe establecer todos los riesgos y amenazas que se identificaron para la Institución y que procesos son afectados por esos riesgos en el otro eje. En la segunda matriz se mantiene el eje de riesgo y se hace el cruce con los procesos establecidos. De esta manera se pueden identificar las áreas críticas de la organización, así como cuáles son los procesos más vulnerables a ataques.

	Activo 1	Activo 2	Activo 3
Riesgo 1	X	X	
Riesgo 2		X	X

Ilustración 3. Ejemplo matriz riesgo-activos

	Proceso 1	Proceso 2	Proceso 3
Riesgo 1	X	X	
Riesgo 2		X	X

Ilustración 4. Ejemplo matriz riesgo-procesos

Teniendo en cuenta el plan de acción establecido para la fase 2, el equipo se puso en contacto con el personal de la Institución para poder empezar a evaluar los riesgos y vulnerabilidades que se tienen frente al proceso seleccionado por el personal de la Institución al que se debió aplicar el análisis. Frente a esta comunicación, la Institución nos da a conocer los protocolos que hacen parte de la Institución y los activos que maneja. Y como cubre una gran parte horizontal de los procesos que ocurren dentro de la

Institución. Al tener mayor conocimiento del macroproceso que se iba a evaluar, se estableció que procesos hacían parte de este, así como que partes de la Institución se veían relacionadas.

- **Dimensiones de valoración**
  Las dimensiones que se tuvieron en cuenta para la valoración de la consecuencia de la materialización de una amenaza están relacionadas con las características o propiedades que hacen valioso un activo, las cuales se relacionan a continuación:
  - **Disponibilidad**
    Propiedad o característica de los activos consistente en que las entidades o procesos autorizados tienen acceso a los mismos cuando lo requieren. (UNE 71504:2008).

    De acuerdo con lo anterior, la disponibilidad es una característica que afecta a todo tipo de activo, debido a su gran valor desde el punto de vista de disponibilidad, si una amenaza afectara esta propiedad las consecuencias serían graves.

  - **Integridad de los datos**
    Propiedad o característica consistente en que el activo de información no ha sido alterado de manera no autorizada. (ISO/IEC 13335-1:2004).

    De acuerdo con lo anterior, los datos reciben una alta valoración desde el punto de vista de integridad, su alteración voluntaria o intencional, causaría daños a la Institución.

  - **Confidencialidad de la información**
    Propiedad o característica consistente en que la información ni se pone a disposición, ni se revela a individuos, entidades o procesos no autorizados. (ISO/IEC 27001:2007).

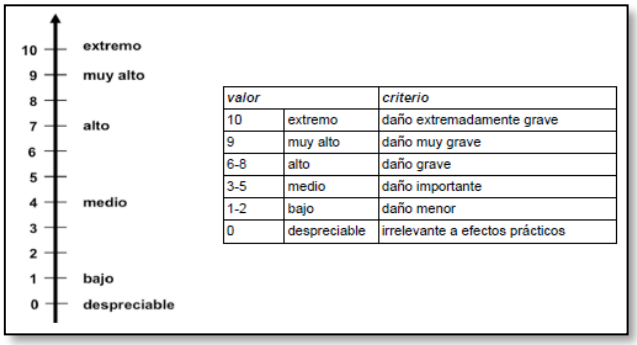
    De acuerdo con lo anterior, los datos reciben una alta valoración desde el punto de vista de confidencialidad, su revelación podría causar graves daños a la Institución.

  - **Autenticidad**
    Propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos. (UNE 71504:2008).

    De acuerdo con lo anterior, los datos reciben una elevada valoración desde el punto de vista de autenticidad del origen cuando un defecto de imputación podría causar graves daños en la Institución.

  - **Trazabilidad**
    Propiedad o característica consistente en que las actuaciones de una entidad pueden ser imputadas exclusivamente a dicha entidad. (UNE 71504:2008)

- **Criterios de valoración**
  Los criterios utilizados en el proyecto fueron seleccionados determinando una escala de 10 valores, donde 0 corresponde a un valor despreciable o sin efecto, y 10 corresponde a extremo o daño extremadamente grave.



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

Ilustración 5. Criterios de valoración - Magerit version3.

- **Valoración de Activos**
  La institución tuvo una variedad de activos que hacen parte del proceso al que se le realiza el análisis de riesgos y que necesitan ser evaluados para clasificar su nivel de prioridad e impacto.

  Estos activos se pueden clasificar en 3 categorías: organizacionales, elementos y lugares físicos. De acuerdo con el alcance establecido se clasificaron de la siguiente forma: departamento de TI y los colaboradores de todo tipo. En los elementos físicos encontramos: computadores de los colaboradores, computadores de alto nivel, (sea de usuarios de alto nivel en la Institución o que tienen una gran cantidad de permisos) las bases de datos y los sistemas de red que se utilizan en la Institución.

  Por último, se tienen los lugares físicos como las oficinas e instalaciones de las bases de datos. Entre todos estos activos existen unos que tienen más precedencia sobre los demás y requieren una mayor protección y evaluación sobre los riesgos que se pueden tener.

- **Valoración de Vulnerabilidades**
  Por parte de la Institución se realizó levantamiento de información, que permitió identificar posibles vulnerabilidades y amenazas (85 en total).

  Estas fueron clasificadas en 6 categorías: Hardware, Software, Red, Personal, Lugar y organización. Teniendo en cuenta la gran cantidad de vulnerabilidades, se decidió realizar un filtrado de estas para encontrar las

que requieren una mayor prioridad y para agrupar las que se evalúan temas iguales.

Para las categorías de Hardware y Software se tomó en cuenta que son elementos importantes de uso cotidiano. Estos son sistemas que requieren mantenerse actualizados y en constante monitoreo por las fallas que se pueden encontrar y como permiten puntos vulnerables para la organización. Teniendo esto en cuenta, las diferentes vulnerabilidades de estas categorías se tendrán en cuenta con prioridad para la gestión de riesgos.

- **Valoración de Amenazas**

Como se mencionó anteriormente en este documento se puede encontrar las posibles vulnerabilidades y amenazas que se pueden presentar en la infraestructura tecnológica de la Institución.

Dentro del documento se pueden ver que hay amenazas humanas (a través de acciones humanas) y las otras amenazas, 38 en total. En la sección de las otras amenazas, se observa que existen clasificaciones para las amenazas y en algunas se puede ver si son deliberadas, accidentales o naturales. Todas estas amenazas, al ser un número más reducido, se decidió que todas serían agregadas a la lista de vulnerabilidades y amenazas a evaluar. Teniendo en cuenta que aquí cada una de las amenazas requiere una evaluación individual, no se pueden hacer evaluaciones categóricas sobre la prioridad, y es necesario que se evalúe cada una para ver cuales pueden tener un mayor impacto frente a la organización.

- **Valoración de Salvaguardas**

Las salvaguardas propuestas fueron evaluadas por la Institución con el objetivo de mitigar posibles riesgos a la infraestructura tecnológica, permitiendo de esta forma disminuir o reducir el impacto en la materialización de uno de estos.

La valoración de las salvaguardas varias de acuerdo con las siguientes características:

- Nuevas tecnologías.
- Eliminación de tecnologías antiguas.
- Cambios en los tipos de activos a proteger.
- Evolución de las brechas de ataques.
- Cambio en el catálogo de salvaguardas.

Para poder establecer el porcentaje de reducción en la probabilidad e impacto de una amenaza se debe determinar las siguientes características, así:

- Capacidad de la salvaguarda para mitigar el riesgo.
- Capacidad de la salvaguarda para prevenir y detectar la amenaza.
- Configuración de la salvaguarda (Automáticas / Manuales).
- Criterios en la implantación, configuración y mantenimiento de la salvaguarda.
- Efectividad de la salvaguarda en la mitigación del riesgo.
- Dependencia entre salvaguardas.
- Control y seguimiento en el funcionamiento de la salvaguardia.

De acuerdo con lo anterior, la efectividad en la valoración de las salvaguardas se determina de la siguiente forma:

- Sin impacto sobre la amenaza: La salvaguarda no tiene ningún impacto sobre la amenaza.
- Poca efectividad sobre la amenaza: La efectividad de la salvaguarda no tiene impacto directo sobre la amenaza.
- Efectivo: La salvaguarda cumple con la reducción de la frecuencia e impacto de la amenaza.
- Muy efectivo: La salvaguarda se configuró específicamente para una amenaza.

- **Matrices de Riesgo**

Una vez se identificaron los componentes de TI de la Institución, se contactó para que por parte de ellos nos presentaran una lista de los riesgos y vulnerabilidades que han registrado en los últimos meses para tener una línea base de riesgos. Una vez se tiene la información se generaron las dos matrices de riesgo en las que se pueden establecer la conexión entre los riesgos y vulnerabilidades y los componentes y procesos.

	Nivel de Riesgo	Probabilidad de que ocurra	Categoría	Afectación Económica	Afectación Reputacional
Piratería	Media	Alta	Tecnología	Moderada	Catastrofica
Ingeniería Social	Alta	Media	Tecnología	Mayor	Mayor
Intrusión, accesos forzados al sistema	Alta	Alta	Tecnología	Mayor	Moderada
Acceso no autorizado	Alta	Media	Social	Menor	Moderada
Crimen por computador	Media	Media	Tecnología	Moderada	Moderada
Acto fraudulento	Alta	Baja	Social	Moderada	Menor
Soborno de la información	Media	Baja	Social	Leve	leve
Suplantación de identidad	Alta	Media	Tecnología	Leve	Leve
Intrusión en el sistema	Alta	Muy Baja	Social	Menor	Menor
Bomba/Terrorismo	Alta	Muy Alta	Tecnología	Mayor	Mayor
Guerra de la información	Media	Media	Tecnología	Moderada	Menor
Ataques contra el sistema DDoS	Alta	Alta	Tecnología	Moderada	Moderada
Penetración en el sistema	Alta	Media	Social	Moderada	Moderada
Manipulación en el sistema	Media	Alta	Tecnología	Menor	Mayor
Explotación económica	Media	Baja	Social/Tecnología	Moderada	Moderada
Hurto de información	Alta	Media	Tecnología	Menor	Moderada

Ilustración 6. Matriz de riesgos

Con relación a la ilustración anterior, los umbrales de afectación se establecieron de acuerdo con el impacto económico que puede llegar a causar dicha afectación (por ejemplo: valor del activo + tiempo de afectación + valor de recuperación + posible afectación reputacional + posibles sanciones), estos umbrales fueron revisados con la Institución y de la misma forma se establecieron los umbrales de aceptación de controles versus riesgos residuales. Por ejemplo, para “Piratería” tenemos que el nivel de riesgo es medio, combinado con una probabilidad alta, la afectación puede llegar a ser moderada y la afectación reputacional sería catastrófica.

En la Fase III: Gestión de Riesgos, se presenta de manera más detallada las escalas aplicadas relacionadas con probabilidad versus impacto.

- **Evaluación de Escenarios**

Al tener las matrices de riesgo se empezó a evaluar diferentes escenarios a los que la Institución puede verse afectada. Teniendo en cuenta que existen una gran cantidad de posibles escenarios, se plantearon dos escenarios optimistas, dos escenarios Normales, dos escenarios pesimistas y un escenario catastrófico. Para cada uno de los escenarios se presentaron las amenazas y vulnerabilidades que serán explotadas y como estos en conjunto tendrían efectos en la Institución.

Escenario Optimista 1:

• Amenazas/Vulnerabilidades:
1. Mal funcionamiento del equipo
2. Datos provenientes de fuentes no confiables
3. Asalto a un Empleado
4. Soborno de la información

Escenario Optimista 2:

• Amenazas/Vulnerabilidades:
1. Destrucción de equipos o información
2. Suplantación de Identidad
3. Agua
4. Fallo en el sistema de suministro de agua
5. Robo de equipos

Escenario Pesimista 1:

• Amenazas/Vulnerabilidades:
1. Ataques contra el sistema DDoS
2. Crimen por computadora
3. Interceptación
4. Inundación
5. Mantenimiento insuficiente/Instalación fallida de los medios de almacenamiento
6. Ausencia de control de cambios eficaz

Escenario Pesimista 2:

• Amenazas/Vulnerabilidades:
1. Ataques contra el sistema DDoS
2. Crimen por computadora
3. Interceptación
4. Código Malicioso
5. Sabotaje del sistema
6. Saturación del sistema de información

C. FASE III: Gestión De Riesgos

En la fase de gestión de riesgo, se revisó cómo la Institución se enfrenta a los riesgos. Primero se interpretaron los impactos y posibilidad de cada uno de los riesgos y se estableció cuál forma de tratamiento se va a utilizar para tratarlo. Entre las formas de mitigar un riesgo se tienen: eliminación, mitigación, compartición o financiación. Se evaluó, en conjunto, cuál es la mejor dependiendo del estado, la Institución y el riesgo específico. Teniendo en cuenta esto se debe clasificó cada uno de los riesgos.

Para esto se construyó un documento que estableció para cada riesgo los siguientes criterios:

- Nivel de riesgo: {'muy baja'|'baja'|'media'|'alta'|'muy alta'}.
- Probabilidad de que se realice: {'muy baja'|'baja'|'media'|'alta'|'muy alta'}.
- Categoría: {'tecnología'|'Naturales'|'Sociales'}.
- Afectación económica: {'Leve'|'Menor'|'Moderada'|'Mayor'|'Catastrófica'}.
- Afectación reputacional: {'Leve'|'Menor'|'Moderada'|'Mayor'|'Catastrófica'}.

Teniendo en cuenta estos criterios se clasificaron los riesgos de mayor prioridad a menor prioridad. Fue muy importante establecer el porqué de cada uno de los criterios como las categorías que se tienen.

- **Definición de umbrales de Riesgos**

Este umbral se utilizó principalmente para priorizar que vulnerabilidades y amenazas, en el corto plazo, que se tiene para realizar el proyecto. Fue muy relevante tener en cuenta que el siguiente paso del plan de acción incluirá una ejecución a corto plazo acompañada de una a largo plazo.

- **Riesgo aceptable**

Los riesgos se evaluaron uno a uno, pero también se estableció una generalización sobre los riesgos aceptables. Para la aceptación del riesgo se evaluó el nivel de riesgo de este en conjunto con la probabilidad de qué ocurrencia del riesgo, los riesgos que tienen un nivel de riesgo 'baja' o ´muy baja' en conjunto con probabilidades de ocurrencia 'baja', 'muy baja' y en algunos casos hasta 'media'. Para estos casos especiales tomaron en cuenta los otros criterios de afectación económica y afectación reputacional.

En el caso de que la ocurrencia fuera media y se presenten afectaciones leves, la Institución definió que es mejor aceptar el riesgo y pagar los daños a invertir en la solución, ya que esta puede conllevar a gastos mayores. Para los casos en donde el riesgo sea 'medio' se tuvo que realizar una evaluación diferente, primero se revisó si tienen ocurrencia 'muy baja' o 'baja' se puede aplicar el razonamiento anterior, pero si tiene ocurrencia 'media' o mayor se debió evaluar la parte reputacional, si son leves se puede aceptar, pero en la mayoría de los casos fue necesario realizar validaciones puntuales.

- **Riesgo inaceptable**

Teniendo en cuenta los casos mencionados en el punto anterior, se evaluaron los casos donde el riesgo es 'medio', 'alta' o 'muy alta'. Para estos casos, todos los que pertenecen a estos riesgos y además tuvieron ocurrencias 'alta´ o 'muy alta' acompañados de efectos económicos o reputacionales mayores a 'medios´ no son riesgos aceptables y se tuvo que establecer un plan de

acción para que puedan tener un gran impacto en la imagen reputacional de la Institución.

- **Análisis de riesgos identificados**

Teniendo en cuenta lo anterior, y al debatir con los representantes del departamento de IT, fue posible establecer unos puntos de vulnerabilidad que se tiene en la Institución. Estos puntos se clasificaron en 3 grandes categorías: vulnerabilidades relacionadas con las contraseñas y su configuración por parte de los usuarios. Para identificar estas categorías se utilizó la matriz de riesgos identificados, filtrando por nivel de riesgo en 'alto' y 'muy alto' con repercusiones económicas o reputacionales entre 'moderadas' o 'mayor'.

De los riesgos identificados con clasificación alta y muy alta, 5 de 20 se relacionaron con contraseñas débiles establecidas por los colaboradores. La segunda categoría se concentró en el acceso a la red de la Institución y las conexiones de los colaboradores. De los 20 riesgos identificados se presentaron 7 riesgos de nivel alto o muy alto. La tercera categoría se concentró en la falta de conocimiento por parte de los colaboradores y esto se pudo validar dado que, de los 20 riesgos, 5 se concentraron en la falta de conocimiento en seguridad y procedimientos relacionados.

Después de esta identificación se priorizaron estos riesgos en el desarrollo del plan de seguridad. Los otros riesgos que no entraron en las categorías cubren temas de respaldo de los datos, identificación de ataques y problemas frente afectaciones generadas por causas naturales.

Determinación del impacto potencial

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

La única consideración que queda hacer es relativa a las dependencias entre activos. Es frecuente que el valor del sistema se centre en la información que maneja y los servicios que presta; pero las amenazas suelen materializarse en los medios. Para enlazar unos con otros recurriremos al grafo de dependencias.

Impacto acumulado

Es el calculado sobre un activo teniendo en cuenta:

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

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

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

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

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

Impacto repercutido

Es el calculado sobre un activo teniendo en cuenta:

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

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

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

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

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

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

Agregación de valores de impacto

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

• Puede agregarse el impacto repercutido sobre diferentes activos,
• Puede agregarse el impacto acumulado sobre activos que no sean dependientes entre sí, y no hereden valor de un activo superior común,
• No debe agregarse el impacto acumulado sobre activos que no sean independientes, pues ello supondría sobre ponderar el impacto al incluir varias veces el valor acumulado de activos superiores,

• Puede agregarse el impacto de diferentes amenazas sobre un mismo activo, aunque conviene considerar en qué medida las diferentes amenazas son independientes y pueden ser concurrentes,
• Puede agregarse el impacto de una amenaza en diferentes dimensiones.

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

El riesgo crece con el impacto y con la probabilidad, pudiendo distinguirse una serie de zonas para tener en cuenta en el tratamiento del riesgo:

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

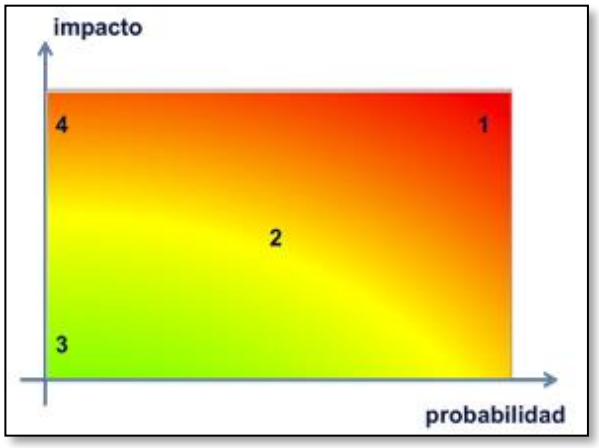


Ilustración 7. El riesgo en función del impacto y la probabilidad.

Riesgo acumulado
Es el calculado sobre un activo teniendo en cuenta

• El impacto acumulado sobre un activo debido a una amenaza y la probabilidad de la amenaza.

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

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

Riesgo repercutido
Es el calculado sobre un activo teniendo en cuenta

• El impacto repercutido sobre un activo debido a una amenaza y la probabilidad de la amenaza.

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

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

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

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

D. FASE IV: PLAN DE SEGURIDAD

La siguiente fase se concentró en desarrollar un Plan de Seguridad. Básicamente, se definió establecer una serie de pasos detallados para implementar los proyectos de seguridad dependiendo de los riesgos que mitigan, dando prioridad a los que solucionan los riesgos con mayor impacto. Teniendo en cuenta los riesgos que se identificaron en la sección anterior, se debe plantear un plan de acción a corto plazo y a largo plazo que ayude a cubrir las 3 categorías y los otros riesgos que tienen un gran riesgo y un efecto que entra en lo descrito en la sección del riesgo inaceptable.

Teniendo en cuenta el corto tiempo del que se dispuso para desarrollar este proyecto, como se comentó anteriormente, se planteó un plan de acción de corto plazo para ser realizado durante un mes. Una vez se trabajó en

la implementación del plan de corto plazo, se planteó uno a largo plazo, que se pueda implementar en un tiempo de 2 a 3 años. En el plan a corto plazo se plantearon 5 diferentes acciones que se pueden implementar rápidamente en la Institución para mejorar el estado de la seguridad de la organización. Por otro lado, en el plan a largo plazo, se plantearon procesos cuya implementación requiere de la preparación de personal y puesta en producción, Asimismo, estos procesos requerirán una gran inversión de capital para que se completen, por lo que es necesario llevarlos frente a los líderes de cada proceso y de esta forma obtener la aprobación de capital para realizarse.

- **Plan a corto plazo**

El plan a corto plazo se concentra en la implementación de recomendaciones en los protocolos de seguridad. Esto permitiría que la Institución pueda mejorar su nivel de seguridad, a través de diferentes pequeñas acciones. Este proceso ayuda a cubrir las categorías de seguridad de las contraseñas, del acceso de la red y el reconocimiento de los riesgos y ataques.

Acciones para realizar:

* Implementación de protocolos de seguridad en las cuentas Microsoft Outlook 365, de forma que se requiera doble autenticación, así como un vencimiento del acceso a la cuenta en un tiempo corto.

* Configuración de VPN institucional de forma que existen Zonas Rojas, Zona DMZ y Zona Verde para cada uno de los integrantes. Manejando el acceso externo a través de un firewall. Las normas del Firewall se deben discutir con el departamento de TI de la Institución.

* Establecer protocolo de notificación sobre fallas o problemas dentro de los sistemas de información, que permite el monitoreo del problema desde el inicio, durante la solución y una vez solucionado.

* Revisión del estado actual de los equipos de la organización.

* Establecer protocolos de revisión de fallas y vulnerabilidades identificadas para los sistemas de la Institución para poder estar al día con las actualizaciones y no generar puntos de vulnerabilidad.

- **Plan a largo plazo**

Actualmente, nos encontramos en comunicación con la Institución para la creación del plan a largo plazo. Teniendo en cuenta que para la implementación de protocolos de respaldos e implementaciones de nuevos software y hardware que ayuden a incrementar la seguridad tomaran tiempo y requieren una gran cantidad de capital para realizarse:

* Implementación de servidores de respaldo.

* Implementación de servidores con todos los protocolos de seguridad con generadores de energía de respaldo y ubicación diferente a la principal.

* Implementación de Firewall y antivirus para toda la compañía que incluya funciones de respaldo frente a Ransomware.

* Realizar cursos de seguridad para generar conciencia sobre los diferentes riesgos de seguridad que genera la ingeniería social.

E. FASE V: Evaluación de la Solución

La quinta fase se concentró en la evaluación y monitoreo de los cambios realizados de forma que pueda evaluar la efectividad y eficiencia de estos. Esta fase se debe medir a través de los indicadores identificados anteriormente, de forma que se pueda establecer qué tan efectivos son y realizar los cambios necesarios para que el sistema de gestión funcione correctamente para la Institución.

La Institución implementó los planes a corto plazo y se pudo notar una mejora en los niveles de seguridad dentro del ámbito de accesos relacionados con contraseñas. Estos procesos se están realizando manualmente y generan mucha carga operacional en sus inicios, sin embargo, mejoran la gestión de los riesgos de la organización. Teniendo el plan en acción es necesario evaluar los resultados a partir de los identificadores definidos en el proyecto.

En el primero de los indicadores se planteó un monitoreo constante de los riesgos y vulnerabilidades que ocurren dentro de los activos de la Institución. Esto se implementó en el corto plazo, de forma que, la Institución se encuentre preparada. Esto le permitirá a la Institución siempre reaccionar de manera eficaz y adecuada frente cualquier riesgo que ocurra. Este indicador se debe medir constantemente y debe evaluar que tan eficientemente la Institución identifica los riesgos internos y externos, y como gestionarlos.

En relación con el segundo indicador, se establecieron protocolos de monitoreo en los activos de la organización. Es importante tener en cuenta que los activos tecnológicos requieren estar actualizados para que no sean vulnerables a los ataques y riesgos emergentes. Para esto se planteó, en el plan a corto plazo, un monitoreo de los equipos y realización de actualizaciones. Este indicador se debe medir en intervalos de máximo 1 mes, revisando cuantos equipos se encuentran actualizados sobre la cantidad total de equipos de la organización.

Para el tercer indicador, se plantea el registro de todos los incidentes, esta medida se debe evaluar trimestralmente, validando cuáles incidentes nuevos ocurrieron y cuáles no ocurrieron al estar registrados.

Es importante resaltar que para que estos procesos se mantengan y se simplifiquen para la Institución, es importante

la implantación de un servicio automatizado que permita monitorear, registrar y en casos específicos actualizar los sistemas. De forma que la Institución solo deba procesar los datos obtenidos y evaluar los resultados.

VI. CONCLUSIONES

El proyecto ha dado respuesta a la problemática y necesidad identificada al inicio del curso, definir e implementar un Sistema de Gestión de Riesgos de Seguridad de la información para una Institución Militar en Colombia, de acuerdo con el alcance y planificación establecido.

Como aporte desde la Maestría de Seguridad de la Información, se investigó sobre varios estándares y metodologías de Gestión de Riesgos, se propusieron varios escenarios, incluso se abordaron escenarios catastróficos, finalmente se escogió la que mejor se ajusta con la problemática planteada y se profundizó en los temas sugeridos en clase.

La creación de las diferentes matrices de riesgo permite visualizar el estado actual de la Institución y así mismo, establecer un precedente sobre la forma en que el Sistema de Gestión de Riesgo de Seguridad de la Información se va a implementar, acorde con las necesidades identificadas.

El establecimiento del plan de acción para la implementación del Sistema de Gestión de Riesgo permitió a la Institución, tener una iniciativa a seguir con objetivos claros. Realizando una implementación gradual de las recomendaciones y por ende, generando un panorama más seguro para toda la estructura organizacional de la Institución.

La gestión del riesgo de seguridad de la información permitirá a la Institución robustecer la estrategia de seguridad y privacidad de la información de forma clara y concisa, a través de la implementación y mejoramiento continuo del Sistema de Gestión de Riesgos de Seguridad de la Información, adaptándose a la evolución de los riesgos actuales y futuros.

El Sistema de Gestión de Riesgos de Seguridad de la Información permitirá mantener, operar, analizar y monitorear de forma cíclica la gestión del riesgo, y de esta forma establecer la toma de decisiones estratégicas para el cumplimiento de los objetivos de la Institución.

VII. REFERENCIAS

[1] https://www.blackberry.com/la/es/forms/enterprise/report-bb-2022-threat-report?utm_source=google&utm_medium=cpc&utm_campaign=smb_enterprise_es-co&_bt=605278076838&_bk=amenazas+ciberseguridad&_bm=b&_bn=g&_bg=138767645675&gclid=EAIaIQobChMIlqvSh8XY-wIVBI6GCh31fwEoEAAYAiAAEgJCWfD_BwE (Consultado: diciembre 1, 2022).

[2] https://es.wikipedia.org/wiki/Ministerio_de_Defensa_(Colombia) (Consultado el 15 de septiembre de 2022).

[3] Une.org. 2022. UNE-ISO GUIA 73:2010 IN Gestión del riesgo. Vocabulario. [en línea] Disponible en: <https://www.une.org/encuentra-tu-norma/busca-tu-norma/norma?c=N0045826> [Consultado el 15 de septiembre de 2022].

[4] Ccn-cert.cni.es. 2022. [en línea] Disponible en: <https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html> [Consultado el 20 de septiembre de 2022].

[5] Álvarez, m., 2022. Herramientas para análisis y gestión de riesgos " Análisis y Gestión de Riesgos" [en línea] Academia.edu. Disponible en: <https://www.academia.edu/35734661/Herramientas_para_an%C3%A1lisis_y_gesti%C3%B3n_de_riesgos_An%C3%A1lisis_y_Gesti%C3%B3n_de_Riesgos_> [Consultado el 20 de septiembre de 2022].

[6] Infostore.saiglobal.com. 2022. GUÍA UNE-ISO 73:2010 IN Gestión de riesgos. Vocabulario _ [en línea] Disponible en: <https://infostore.saiglobal.com/en-us/standards/une-iso-guia-73-2010-in-24830_saig_aenor_une_aenor_une_54564/> [Consultado el 20 de septiembre de 2022].

[7] ISO/IEC 18043:2006. [en línea] ISO. Disponible en: <https://www.iso.org/standard/35394.html> [Consultado el 20 de septiembre de 2022].

[8] Ccn-cert.cni.es. 2022. Glosario. [en línea] Disponible en: <https://www.ccn-cert.cni.es/publico/seriesCCN-STIC/series/400-Guias_Generales/401-glosario_abreviaturas/index.html?n=835.html> [Consultado el 20 septiembre 2022].

[9] UNE 71504:2008, 2022. [en línea] Disponible en: <https://es.slideshare.net/roberth.chavez/gestin-del-riesgos-de-seguridad-de-la-informacin> [Consultado el 20 de septiembre de 2022].

[10] Administracionelectronica.gob.es. 2022. PAe-MAGERIT v.3: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. [en línea] Disponible en: <https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html> [Consultado el 20 de septiembre de 2022].

[11] Iso.org. 2022. [en línea] Disponible en: <https://www.iso.org/obp/ui/#iso:std:iso:guide:73:ed-1:v1:en> [Consultado el 20 de septiembre de 2022].

[12] Seguridades7a.blogspot.com. 2022. MAGERIT. [en línea] Disponible en: <http://seguridades7a.blogspot.com/p/magerit.html> [Consultado el 24 de septiembre de 2022].

[13] Apuntesseguridadit.blogspot.com. 2022. Temas Seguridad Informática. [en línea] Disponible en: <http://apuntesseguridadit.blogspot.com/2014/03/octave-o-perationally-c-ritical-t-hreat.html> [Consultado el 24 de septiembre de 2022].

[14] Seguridades7a.blogspot.com. 2022. NIST SP 800-30. [en línea] Disponible en: <http://seguridades7a.blogspot.com/p/nist-sp-800-30.html> [Consultado el 24 de septiembre de 2022].

[15] Huerta, A., 2022. Introducción al análisis de riesgos – Metodologías (II) - Security Art Work. [en línea] Obra de Arte de Seguridad. Disponible en: <https://www.securityartwork.es/2012/04/02/introduccion

-al-analisis-de-riesgos-%E2%80%93-metodologias-ii/> [Consultado el 24 de septiembre de 2022].

[16] PMI Project Risk:2019. [en línea] PMI. Disponible en: <https://www.pmi.org/learning/library/es-desmitificando-el-enfoque-practico-de-la-planificacion-de-riesgos-7331#:~:text=Un%20riesgo%20en%20proyectos%20es,alcance%20o%20calidad%20(PMBOK).>

[17] MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Disponible en: < https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html>