ANÁLISIS DE RIESGOS DE CENTRO DE DATOS BASADO EN LA HERRAMIENTA PILAR DE MAGERIT

María Fernanda Molina-Miranda
Facultad de Ciencias Matemáticas y Física, Universidad de Guayaquil
maria.molinam@ug.edu.ec

***Resumen*— Los riesgos están presentes en todo ámbito laboral y pueden provocar muchas pérdidas en el negocio si no son controladas a tiempo y de forma adecuada. Para ello existen procesos como es el caso de la gestión de los riesgos tecnológicos cuya finalidad es la protección de la información, conociendo las fortalezas y debilidades que pudiesen afectar durante todo el ciclo de vida del servicio. Es de vital importancia que una organización dedicada a brindar servicios tecnológicos y de mantener respaldada mucha información confidencial de forma segura, realice un análisis de riesgos para saber cómo garantizar la continuidad del negocio.**

Se ha desarrollado un análisis de riesgo tecnológico de orden cualitativo aplicado en el centro que administra y brinda los servicios de red y sistemas de una universidad siguiendo la metodología MAGERIT.

Para la evaluación se ha considerado la herramienta PILAR, la cual soporta el análisis y gestión de los riesgos de sistemas de información siguiendo la metodología MAGERIT. Los resultados muestran los gráficos que reflejan los niveles de riesgo e impacto potencial, actual y objetivo.

Finalmente, la aportación de este estudio es identificar el nivel de riesgo en que se encuentran los activos mediante el nivel de madurez de la seguridad implementada y sobre todo incentivar al personal a seguir las respectivas normas y procedimientos referentes a la seguridad de la información y recursos.

***Palabras Claves*— *amenazas, MAGERIT, metodología, PILAR, riesgos, salvaguardas, tecnológica*.**

***Abstract*— The risks exist in any workplace and can cause considerable losses in business if they are not controlled at time and in a properly way. For this reason, there are processes such as technological risk management whose purpose is the information protection, knowing the strengths and weaknesses that might affect the entire service lifecycle.**

This paper describes the concepts related to information security risk management, standards, methodologies and tools that provide the guides to reduce the vulnerability level of the assets against a threat. It is important that an organization, dedicated to provide technology services and backup a lot of confidential information in a secure way, has a risk management plan to ensure business continuity.

For this reason, it has been necessary to develop a qualitative technological risk analysis applied at the area that manages and provides network services and systems, insidean university following the MAGERIT methodology. The first step consists on describing the current situation of the organization, then identifying the assets with their threats, performing the measurement of risks and suggesting the necessary safeguards that could be part of the implementation plan.

PILAR tool was considered for the evaluation, which supports the analysis and information system risk management following the MAGERIT methodology. The results reflects the risk levels and potential, current and target impact using graphs.

Finally, the contribution of this study is identifying the risk level for the assets, comparing the maturity level of security implemented and especially encouraging staff to follow the relevant rules and procedures concerning the security of information and resources.

***Keywords-- MAGERIT, methodology, PILAR, risk, safeguards, technological, threats,*.**

I. INTRODUCCIÓN

Se conoce a los riesgos de TI, como cualquier riesgo relacionado con la tecnología de la información. Si bien la información durante mucho tiempo ha sido considerada como un activo valioso e importante, el aumento de la economía del conocimiento ha llevado a las organizaciones a depender cada vez más en la información, procesamiento de la información y sobre todo de TI. Varios eventos o incidentes pueden comprometer de alguna manera, por lo tanto, pueden causar impactos adversos en los procesos de negocio de la organización o de su misión, que van desde intrascendente a catastrófica. [1]

Cuando se habla de tecnología y de mantener la seguridad sobre ésta, fácilmente se piensa en términos de protección física, lógica y protección sobre los sistemas y equipos. Solo al final se trata lo referente a medidas técnicas. Sin embargo, esta seguridad es limitada y debe ser respaldada por una gestión y procedimientos adecuados que garanticen la continuidad del negocio.

Existen varios estándares reconocidos a nivel mundial como son la serie ISO 27000 [2]que tratan sobre la gestión de riesgos en seguridad de la información proporcionando recomendaciones, lineamientos de métodos y técnicas de evaluación de riesgos de la seguridad en la información que conllevan a medir los niveles de riesgo por su impacto y

probabilidad; también existen metodologías y herramientas que ayudan a manipular grandes volúmenes de información generados para realizar un análisis completo en un mediana o grande empresa.

El presente artículo está compuesto de la siguiente manera: En la sección II se desarrolla el método referente a la gestión de riesgos, metodologías y herramientas a implementar. En la sección III se detalla el caso de estudio considerado para aplicar la metodología MAGERIT, además de los datos ingresados y obtenidos a través de la herramienta PILAR. Finalmente en la sección IV, las conclusiones, recomendaciones y trabajos futuros.

II. MÉTODO

Para fundamentar el presente estudio se ha definido el método descriptivo para dar a conocer diversos conceptos referentes a la importancia, gestión y análisis del riesgo, además de las metodologías y herramientas existentes que servirán para realizar el trabajo.

A. Gestión de Riesgos

En la compleja economía mundial de hoy, las compañías se enfrentan a riesgos ambientales, riesgos inherentes a los procesos y riesgos relacionados a las malas decisiones que se dan dentro de los procesos. Las noticias relacionadas con todo tipo de desastres naturales suelen ser uno de los temas más frecuentes y de mayor impacto mediático en los medios de comunicación, debido a sus efectos devastadores sobre la salud de las personas, edificaciones y millones de pérdidas económicas.

Las empresas se pueden enfrentar a cambios sismológicos como el terremoto que afrontó la provincia de Manabí, Ecuador el 16 de abril del año 2016; debido a los procesos tectónicos comunes en la zona del Cinturón de Fuego del Pacífico. [3]

Además en Ecuador se presentan otros fenómenos hidrometeorológicos como son las inundaciones, erupciones volcánicas, deslizamientos [4] y estos deberían ser motivos por los cuales las empresas y organizaciones deberían implementar planes para gestionar los riesgos, y al tratarse de los riesgos que afectan a los sistemas de TI, también se consideran las amenazas a los cuales se encuentran expuestos los elementos que manejan la información como son los ataques dirigidos al software que afectan la disponibilidad e integridad de la información almacenada o transportada a través de los equipos de comunicación.

Por esta razón hay que estar preparados para prevenir todo tipo de ataques o desastres, ya que cuando el costo de recuperación supera al costo de prevención es preferible tener implementados planes de gestión de riesgos que permitan la continuidad del negocio tras sufrir alguna pérdida o daño.

B. Gestión del Riesgo

El riesgo se originó en el siglo 17 con las matemáticas asociadas con los juegos de azar, actualmente se refiere a la combinación de la probabilidad y la magnitud de pérdidas y ganancias potenciales. Durante el siglo 18, el riesgo, fue visto como un concepto neutral, considerando las pérdidas y ganancias y fue empleado en la marina. En el siglo 19, el riesgo surgió en el estudio de la economía. En el siglo 20 se hizo una connotación negativa al referirse a los peligros en la ciencia y tecnología. [5]

La definición estandarizada de riesgo proviene de la Organización Internacional de Normalización (ISO), definiéndolo como "la posibilidad de que una amenaza determinada explote las vulnerabilidades de un activo o grupo de activos y por lo tanto causa daño a la organización". [6]

C. Análisis del Riesgo

El análisis de riesgos es conocido como el proceso sistemático para estimar la magnitud de los riesgos a que está expuesta una organización, éste permite determinar cómo es, cuánto vale y cómo de protegido se encuentra un sistema, siguiendo los objetivos, estrategia y política de la organización para elaborar un plan de seguridad. Al implantar y operar este plan debe satisfacer los objetivos propuestos con el nivel de riesgo aceptado por la Dirección de la organización. Al conjunto de estas actividades se le denomina Proceso de Gestión de Riesgos. [7]

El análisis de riesgo se realiza ya sea cuantitativa o cualitativamente. El análisis cualitativo es recomendable hacerlo en primer lugar y utiliza una escala de calificación de atributos para describir la magnitud de las consecuencias potenciales ya sea bajo, medio o alto; y la probabilidad de que se produzcan estas consecuencias. Un análisis cualitativo permite:

- Identificar los activos más significativos.
- Identificar el valor relativo de los activos.
- Identificar las amenazas más relevantes.
- Identificar las salvaguardas presentes en el sistema.
- Establecer claramente los activos críticos, aquellos sujetos a un riesgo máximo.

En cambio, el análisis cuantitativo es más detallado y utiliza una escala con valores numéricos para las consecuencias y probabilidad, permitiendo:

- Detallar las consecuencias económicas de la materialización de una amenaza en un activo.
- Estimar la tasa anual de ocurrencia de amenazas.
- Detallar el coste de despliegue y mantenimiento de las salvaguardas.
- Permitir ser más precisos en la planificación de gastos de cara a un plan de mejora de seguridad.

Los sistemas de gestión de la seguridad de la información formalizan cuatro etapas cíclicas donde el análisis de riesgos

es parte de las actividades de planificación, se toman decisiones de tratamiento, estas decisiones se materializan en la etapa de implantación, en el cual se despliegan elementos que permiten la monitorización de las medidas tomadas para poder evaluar la efectividad de las mismas y actuar dependiendo a éstas, dentro de un círculo de excelencia o mejora continua. Ver Figura 3. [8]

El riesgo es una función de la probabilidad y el impacto.

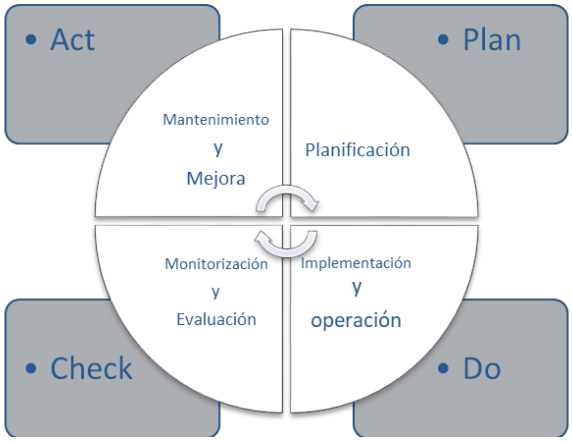

Figura 3 Ciclo PDCA

D. *Metodología*

Una metodología se materializa por un conjunto de métodos, técnicas y herramientas. No contiene métodos específicos; sin embargo, lo especifica por procesos que conforman el marco de gestión de riesgo.

La metodología cualitativa es el más utilizado para el análisis de riesgos y cumple con los requisitos de ISO 27001. El nivel de riesgo se basa en niveles de probabilidad e impacto. Ver Tabla I.

TABLA I NIVEL DE RIESGO

Nivel de Riesgo	Acción requerida para tratamiento del riesgo
Muy Alto	Inaceptable: acciones deben tomarse inmediatamente.
Alto	Inaceptable: acciones deben tomarse lo antes posible.
Medio	Acciones requeridas y que deben tomarse en plazo razonable.
Bajo	Aceptable: no se requieren acciones como resultado de la evaluación de riesgos
Muy Bajo	Aceptable: ninguna acción requerida.

La salida de la ecuación del riesgo se puede representar mediante una escala de 3 niveles refiriéndose al impacto de un evento producido a una probabilidad de ocurrencia. Ver tabla II.

Probabilidad				
	ALTA	Riesgo medio	Riesgo Alto	Riesgo Muy Alto
	MEDIA	Riesgo Bajo	Riesgo Medio	Riesgo Alto
	BAJA	Riesgo muy bajo	Riesgo bajo	Riesgo medio
		BAJO	MEDIA	ALTO
		Impacto		

TABLA II
MATRIZ DE 3 NIVELES DE RIESGO

Entre las metodologías más reconocidas se encuentran:

MAGERIT, OCTAVE, Metolodogía NIST SP800-30, CRAMM, MEHARI, CORAS.

E. *MAGERIT*

Es una de las metodologías más utilizadas que permite el análisis de gestión de riesgos de los Sistemas de Información; fue creada por el Consejo Superior de Administración Electrónica para minimizar los riesgos de la implantación y uso de las Tecnologías de la Información siguiendo la terminología de la norma ISO 31000. En el año 2012 se actualizó a la versión 3.

La metodología se puede resumir en:

1. Determinar los activos relevantes para la organización, su interrelación y su valor, en el sentido de qué perjuicio o coste supondría su degradación.
2. Determinar a qué amenazas están expuestos aquellos activos.
3. Determinar qué salvaguardas hay dispuestas y cuán eficaces son frente al riesgo.
4. Estimar el impacto, definido como el daño sobre el activo derivado de la materialización de la amenaza.
5. Estimar el riesgo, definido como el impacto ponderado con la tasa de ocurrencia de la amenaza.

MAGERIT consiste en 3 libros en versiones inglés, español e italiano:

- Libro I: Método
- Libro II: Catálogo de Elementos
- Libro III: Guía de Técnicas [9]

F. *Herramientas*

Por lo general los análisis de riesgo conlleva considerar una gran cantidad de activos, y a cada uno de estos les corresponde un sinnúmero de amenazas y salvaguardas, por ello resulta un arduo trabajo manipular tal magnitud de información y es por esta razón que se han desarrollado herramientas de apoyo de análisis de riesgos que cumplen ciertos requisitos:

- Permiten trabajar con un conjunto amplio de activos, amenazas y salvaguardas.
- Permiten un tratamiento flexible del conjunto de activos para asemejar al modelo real de la organización.

- Demostrar resultados cercanos a la realidad.

G. PILAR

"Procedimiento Informático Lógico para el Análisis de Riesgos" es una herramienta desarrollada para soportar el análisis y la gestión de riesgos de sistemas de información siguiendo la metodología MAGERIT [10]. Creado por el Centro Nacional de Inteligencia, actualmente se encuentra disponible la versión 6.2.6.

Analiza los riesgos en varias dimensiones: confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad. Para tratar el riesgo se proponen: salvaguardas o contramedidas, normas y procedimientos de seguridad.

Esta herramienta soporta las fases del método MAGERIT:

•Caracterización de los activos: identificación, clasificación, dependencias y valoración

•Caracterización de las amenazas

•Evaluación de las salvaguardas

Evalúa el impacto y el riesgo, acumulado y repercutido, potencial y residual, presentándolo de forma que permita el análisis de por qué se da cierto impacto o cierto riesgo.

Las salvaguardas se califican por fases, permitiendo la incorporación a un mismo modelo de diferentes situaciones temporales. Se puede incorporar el resultado de los diferentes proyectos de seguridad a lo largo de la ejecución del plan de seguridad, monitorizando la mejora del sistema.

PILAR presenta los resultados en varias formas, ya sea en informes RTF, gráficas o tablas que se pueden agregar a una hoja de cálculo, logrando elaborar diferentes tipos de informes y presentaciones de los resultados.

Finalmente, la herramienta calcula calificaciones de seguridad respecto a normas ampliamente conocidas, como son UNE-ISO/IEC 27002:2009: sistemas de gestión de seguridad, RD 1720/2007: datos de carácter personal y RD 3/2010: Esquema Nacional de Seguridad.

Cabe destacar que esta herramienta incorpora tanto los modelos cualitativos como cuantitativos, logrando alternarse entre estos para extraer el máximo beneficio de las posibilidades teóricas de cada uno de ellos. [11]

III. ANÁLISIS DE RESULTADOS

H. Caso de estudio

Alcance

El presente caso de estudio consistirá en identificar los principales riesgos a los cuales se encuentran expuestos los activos involucrados en las funciones que presta el centro de IT de una universidad siguiendo la metodología MAGERIT.

Los análisis a realizar será de orden cualitativo, en el cual los niveles de medición serán en orden probabilístico; la detección de los activos y amenazas en la organización se realizará de forma general considerando los equipos prioritarios para el buen funcionamiento de actividades del departamento; y las salvaguardas se definirán sin considerar el costo económico; ya que no se cuenta con datos estadísticos, financieros, ni registros oficiales para realizar los cálculos correspondientes; por lo tanto sólo servirá de guía para que la institución y un grupo de personas encargadas de la seguridad de la misma lo evalué antes de implementarlo o mejorarlo.

Cabe mencionar que se utilizará la herramienta PILAR en modo de evaluación, por lo cual no se contarán con todas las funcionalidades como son los informes escritos y detalle de salvaguardas.

El conjunto de actividades que conllevan una gestión son los siguientes:

1. Levantar un modelo del valor del sistema, identificando y valorando los activos relevantes.
2. Levantar un mapa de riesgos del sistema, identificando y valorando las amenazas sobre aquellos activos.
3. Levantar un conocimiento de la situación actual de salvaguardas.
4. Evaluar el impacto posible sobre el sistema en estudio.
5. Evaluar el riesgo del sistema en estudio.
6. Informar a las áreas del sistema con mayor impacto o riesgo a fin de que se puedan tomar las decisiones de tratamiento con motivo justificado.

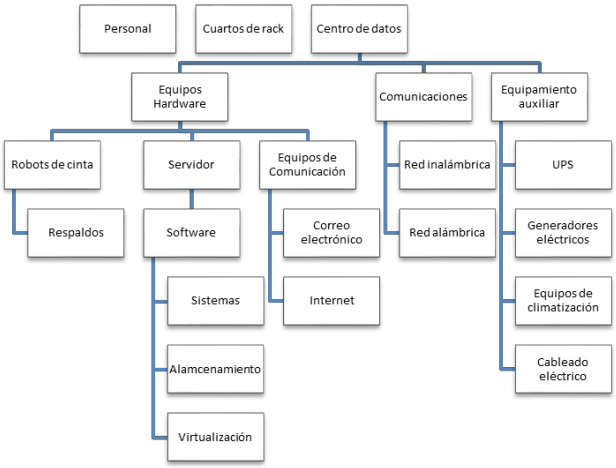

Figura 4. Árbol de dependencia de activos

En el árbol de dependencias de la figura 4 se encuentran desplegados de forma jerárquica los activos de acuerdo al nivel de dependencia que existe entre estos.

En el primer nivel se ha considerado al centro de datos, que es el lugar donde se concentran los servidores y equipos de comunicación, mientras estos se encuentran en el segundo nivel al igual que el equipamiento auxiliar. En el tercer nivel se encuentran los servicios y aplicaciones que corren sobre los equipos basados en hardware. Además,b se han considerado a los equipos que generan electricidad y la climatización en el centro de datos que son de suma importancia para el normal funcionamiento de los equipos.

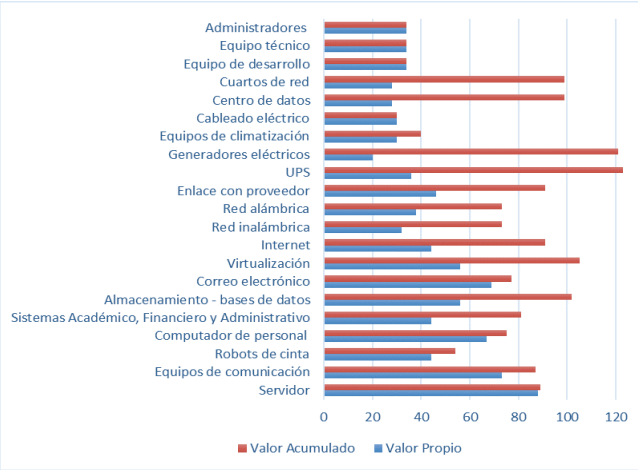

Figura 5. Valor propio y acumulativo de activos

En la gráfica de la figura 5 se ha representado la valoración propia y acumulada de cada uno de los activos, en la cual se ha considerado la relación de dependencia de la figura 4; de esta forma sobresalen a simple vista los activos, tales como: las instalaciones, equipamiento auxiliar y entre los principales servicios ofrecidos están internet y almacenamiento de información.

Respecto a la estructura de red, en la figura 6 se presenta la topología de red, la cual está conformada por un router principal, un switch de backbone, un analizador de red y dos cortafuegos: uno de borde y otro para proteger los servidores internos. En el primer cortafuego se filtran las reglas para la DMZ, redes inalámbricas y acceso al internet. Los servidores con sistema operativo Windows se protegen mediante antivirus que se actualiza diariamente, mientras que los servidores Linux mantienen listas de acceso.

PILAR también permite obtener la valoración de las amenazas de forma automática considerando la frecuencia de materialización y el impacto que tendrían en la organización según las dimensiones.

En la tabla II se han considerado las salvaguardas más importantes que se consideran necesarias aplicar en el presente análisis de riesgos; las valoraciones actuales se encuentran entre nivel 0 y 4, siendo 0 el nivel de riesgo muy alto y es necesaria la implementación de salvaguardas.

En el nivel L0 se consideran a los procedimientos inexistentes y que no han sido evaluados como son:

- Desarrollo de un plan de contingencias ante desastres.
- Realizar simulacros de forma periódica, adoptando procesos estructurados de planificación de capacidad TI, desarrollo seguro, pruebas de seguridad siguiendo los estándares de seguridad anteriormente descritos.
- Coordinar una revisión periódica de las directivas de las copias de seguridad y de las reglas de acceso aplicadas a los cortafuegos para verificar que éstas se encuentren configuradas correctamente.
- Iniciar el uso de cables de seguridad para los computadores y portátiles.
- La instalación de antimalware en los servidores y equipos del personal.
- La implementación de un sistema de detección de intrusos.
- Agregar seguridad al acceso remoto utilizando autenticación multifactor.
- Implementar control de cuarentena en VPN
- La contratación de personal responsable de la seguridad, encargado de documentar los procedimientos, normas y directrices de seguridad de la información, identificar los roles y responsabilidades que deben asignarse al personal administrativo; reflejando los cambios en la política de seguridad, la cual debe someterse a una revisión periódica en participación conjunta con la Gerencia.

En cambio, en el nivel 4 se indica que aún faltan definir procesos para mejorar la protección de la información; el objetivo es mejorar estos procesos hasta que sean gestionables y medibles, llegando al nivel de máxima seguridad e ideal, nivel 5.

Entre las salvaguardas referentes a la parte lógica se tienen:

•Adquirir la buena práctica de realizar pruebas de las actualizaciones previas a su instalación en los servidores, haciendo un seguimiento continuo de los parches de seguridad mediante herramientas de gestión de vulnerabilidades o actualizaciones automáticas.

•Analizar las directivas de cortafuegos con regularidad asegurando el nivel de protección equilibrado entre los controles de seguridad de la red perimetral e interna.

•Asignar cuentas dedicadas a la administración con contraseñas complejas y que sean cambiadas de forma regular para reducir el riesgo de acceso no autorizado.

•Para evitar la fuga de información sería recomendable conocer un poco más sobre el nuevo personal a contratar solicitando un historial, trabajando de forma conjunta con el personal de Talento Humano para verificar los antecedentes de forma proporcional a la clasificación de seguridad de aquella información a la que va a acceder el empleado a contratar, ya que los accesos para un administrador serian diferentes del de un administrativo.

•Implementar el cifrado de los datos almacenados y en tránsito.

•Dar charlas al personal referente a la seguridad.

En la tabla III se han evaluado el impacto y riesgo de cada amenaza que afectan a los activos por niveles, definiendo como el nivel 10 como más crítico y nivel 1 como menos crítico. En la evaluación del impacto potencial se refleja la criticidad de los elementos sin la debida salvaguarda, por ello se encuentran entre nivel 9 y 10, en la columna de impacto actual se refleja la situación actual y finalmente el impacto objetivo resulta aplicando las salvaguardas sugeridas.

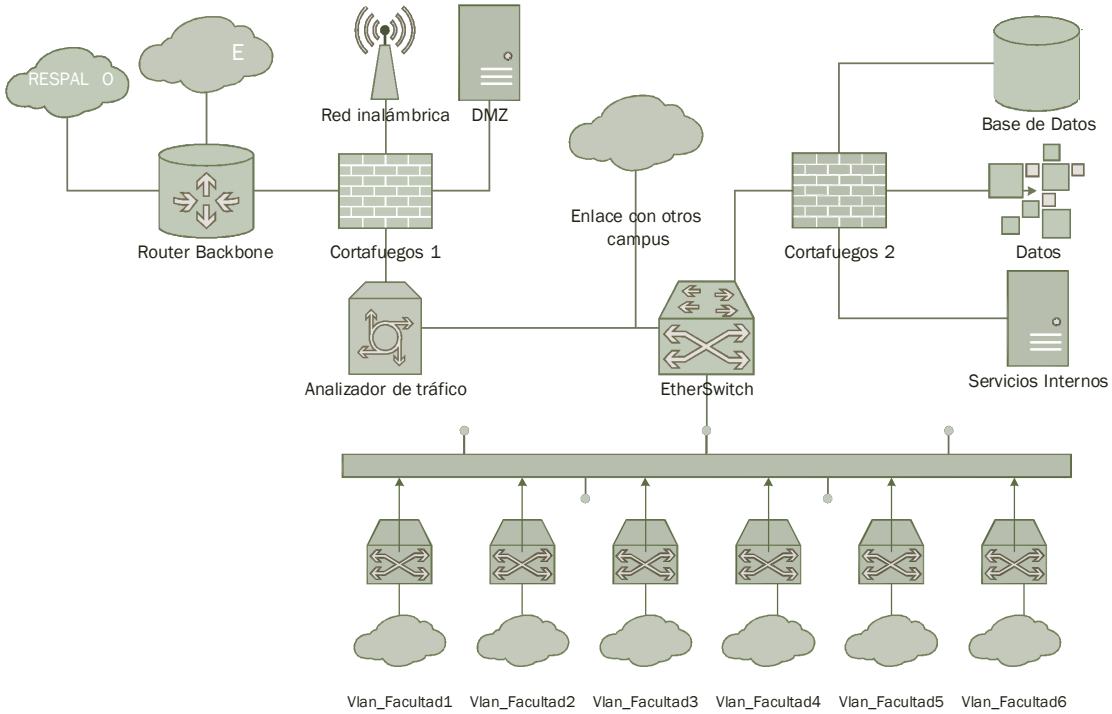

Figura 6 Topología de red

TABLA II

EVALUACIÓN DE SALVAGUARDAS

Riesgos	Salvaguardas	Actual	Objetivo
Incendio y Terremoto	Instalación de sistemas contra incendio	L3	L4
	Instalación de alarmas contra incendio	L3	L4
	Uso y mantenimiento de extintores	L4	L5
	Desarrollo de plan de emergencia ante incendios	L2	L3
	Desarrollo de plan de contingencia ante desastres	L0	L3
	Realizar simulacros de forma periódica	L0	L3
	Almacenar las cintas de respaldo en otra oficina	L3	L3
Falla de generador eléctrico	Mantenimiento semanal de generador eléctrico	L4	L5
Falla de equipos de climatización	Mantenimiento de equipos de climatización	L4	L5
	Adquirir nuevos equipos de climatización	L1	L3
Agotamiento de recursos	Mantenimiento preventivo de servidores y robot de cinta	L3	L4
	Revisión de directiva de copias de seguridad de forma regular	L0	L3
	Monitoreo de recursos de los equipos críticos	L3	L4
Desconexión Física o lógica	Asegurar los equipos de comunicaciones y servidores en armarios cerrados	L1	L3
Robo	Uso de cables de seguridad para computadores de personal y portátiles	L0	L3
Virus	Instalación de antivirus en servidores	L3	L4
	Instalación de antivirus en equipos de personal	L4	L4
	Actualizar periódicamente las firmas del antivirus	L4	L4
Malware	Instalación de antimalware en servidores	L0	L3
	Instalación de antimalware en equipos de personal	L0	L3
Errores de configuración	Realizar pruebas de actualizaciones previo a la instalación	L1	L3
	Pruebas periódicas de los cortafuegos	L0	L3
Acceso no autorizado	Establecer controles de acceso físico	L3	L4

	Analizar directivas de cortafuegos con regularidad	L1	L3
	Implementación de sistema de detección de intrusos	L0	L3
	Asignar cuentas para la administración de sistemas	L1	L3
	Utilizar autenticación multifactor para conexión remota	L0	L3
	Implementar control de cuarentena en VPN	L0	L3
	Implementar directivas de contraseñas complejas	L2	L4
	Implementar controles avanzados de gestión de cuentas	L2	L4
Fuga de información	Implementar cifrado de datos	L2	L3
	Contratar personal responsable de la seguridad	L0	L4
	Solicitar historial de personal antes de ser contratado	L2	L3
	Dar charlas al personal referente a la seguridad	L1	L3

TABLA III
RIESGOS E IMPACTO DE CADA AMENAZA

Activos	Amenaza	Impacto Potencial	Impacto Actual	Impacto Objetivo	Riesgo Potencial	Riesgo Actual	Riesgo Objetivo
Servidores	Incendio	10	7	5	4	4	2
	Terremoto	10	7	5	4	4	2
	Robo	9	6	3	4	4	2
	Acceso no autorizado	9	6	3	6	5	4
	Falla de generador eléctrico	9	5	3	6	5	4
Equipos de comunicaciones	Incendio	10	7	5	4	4	2
	Terremoto	10	7	5	4	4	2
	Robo	9	6	3	4	4	2
	Acceso no autorizado	9	6	3	6	5	2
	Desconexión Física o lógica	9	6	3	6	4	2
	Falla de generador eléctrico	9	5	3	6	4	2
Robot de cintas	Incendio	10	7	5	4	4	2
	Terremoto	10	7	5	4	4	2
	Robo	9	6	3	6	4	2
Computador de personal	Incendio	10	7	5	4	4	2
	Terremoto	10	7	5	4	4	2
	Robo	9	6	3	6	4	2
	Malware	9	8	3	7	6	4
Sistemas académicos, financieros y administrativos	Incendio	10	7	5	4	4	2
	Terremoto	10	7	5	4	4	2
	Acceso no autorizado	9	6	3	6	6	2
Almacenamiento – bases de datos	Acceso no autorizado	9	6	3	6	6	2
	Desconexión física o lógica	9	6	3	6	4	2
	Agotamiento de recursos	9	6	3	7	5	2
Correo electrónico	Incendio	10	7	5	4	4	2
	Terremoto	10	7	5	4	4	2
	Acceso no autorizado	9	6	3	6	6	2
	Desconexión física o lógica	9	6	3	6	6	2
Virtualización	Incendio	10	7	5	4	4	2
	Terremoto	10	7	5	4	4	2
	Acceso no autorizado	9	6	3	6	6	2
	Desconexión física o lógica	9	6	3	6	6	2
Internet	Incendio	10	7	5	4	4	2
	Terremoto	10	7	5	4	4	2

De igual manera se obtienen las evaluaciones respecto al riesgo, finalmente se puede observar la columna de riesgo objetivo se encuentra en nivel 2, lo cual indica que mediante las salvaguardas aplicada es posible mejorar la seguridad de los equipos. La valoración residual debe ser considerada como parte de un nuevo análisis de riesgo.

Informes

En PILAR se han obtenido los resultados parciales de las evaluaciones realizadas. La figura 7 presenta los parámetros de seguridad que se afectan en algunos de los activos, como son: disponibilidad en color rojo, la integridad en color azul y la confidencialidad en color verde; prevaleciendo la confiabilidad en la mayoría de activos.

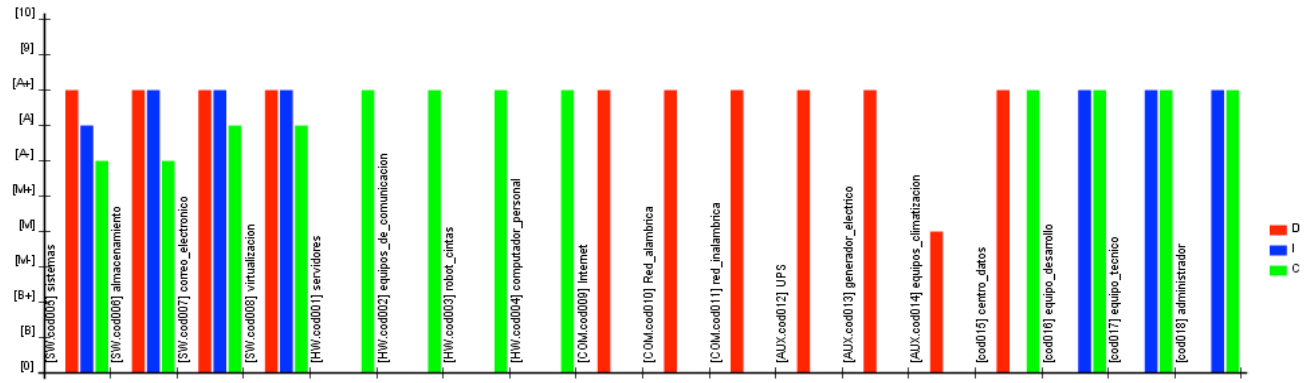

Figura 7. Valor de Activo

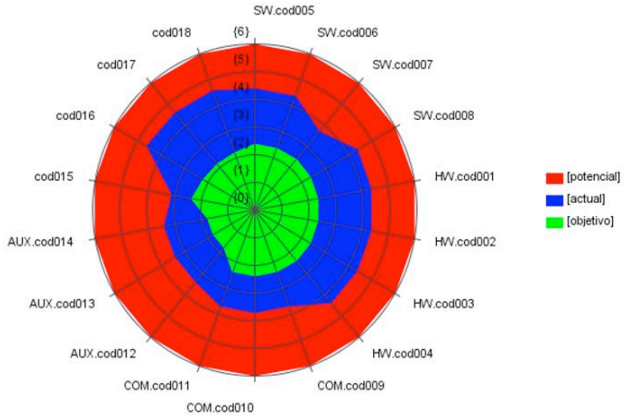

Figura 8 Impacto Acumulado

En la figura 8 es una gráfica radial obtenida en PILAR, en la cual se reflejan algunos activos con su respectiva codificación y los valores obtenidos en la tabla II respecto al impacto potencial, actual y objetivo; pudiendo diferenciarlos mediante los 3 colores: el impacto potencial se encuentra en color rojo, impacto actual en color azul e impacto objetivo en color verde.

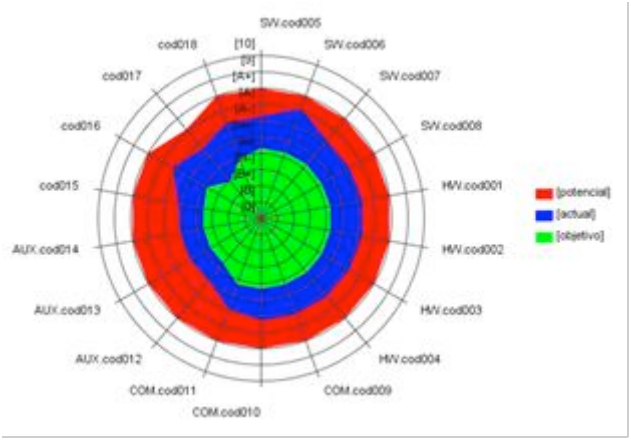

Figura 9 Riesgo Acumulado

De igual forma se reflejan los riesgos acumulados sobre cada uno de los activos definidos en la figura 9, en el cual se consideran la implementación de las salvaguardas que permiten que estos valores disminuyan los parámetros de vulnerabilidad de los activos hasta el nivel objetivo.

Finalmente se ha desarrollado el plan de seguridad que consta de una política de seguridad y un plan de ejecución que conlleva la participación del personal de varias áreas e implementación y mejora de procesos aplicando medidas preventivas y correctoras para reducir los niveles de riesgo existentes, además de reconocer el nivel de riesgo residual al cual aún se encuentran expuestos los sistemas y procesos de la organización.

IV. CONCLUSIONES

En el presente trabajo fueron descritos los conceptos e importancia de los términos relacionados con la gestión del riesgo presentes en la seguridad de la información que es administrada mediante los diversos equipos, servicios y personal del área de TI; además de conocer los estándares, metodologías y herramientas que posibilitan el desarrollo del análisis de riesgo en una organización.

MAGERIT fue la metodología implementada en el caso de estudio realizado, para conocer las vulnerabilidades a las cuales se encuentran expuestos los activos que forman parte del departamento de informática de una universidad, mediante un análisis de riesgos de orden cualitativo permitió conocer el nivel de madurez en la seguridad aplicada en la institución para finalmente sugerir las salvaguardas necesarias para reducir los niveles de riesgo e impacto.

La herramienta PILAR permitió ingresar las valoraciones para realizar las evaluaciones referentes a los activos, amenazas y salvaguardas para finalmente obtener los niveles de riesgo e impacto plasmados en gráficas radiales permitiendo identificar fácilmente la necesidad de implementar procedimientos y normas cuya finalidad sea la protección de los recursos e información.

La gestión de los riesgos en una empresa debería considerarse un proceso intrínseco, ya que si la empresa no conoce sobre el riesgo que corren sus activos de información difícilmente llegará a estar preparada para evitar una posible ocurrencia, de allí la importancia de conocerlo y crear controles para disminuir o eliminar la ocurrencia. Como es el caso del departamento de IT de la universidad, cuyos resultados del análisis reflejaron que las medidas de seguridad han ayudado a reducir los riesgos de amenazas físicas de manera oportuna y que solo requieren de implementar procesos para una mejor gestión; en cambio el nivel de seguridad a nivel de datos y aplicación es bajo debido a la carencia de procedimientos y normas que minimicen el acceso no autorizado, la fuga de información y ataques a los sistemas.[12]

Es importante mencionar, que las salvaguardas sugeridas permiten minimizar los riesgos, pero cada una tiene un costo, por lo que en cada caso en particular debe evaluarse el valor de la información a proteger y los costos que implicaría la pérdida o el sufrimiento de un ataque, y en este sentido planificar las acciones pertinentes para la protección de tal información.

Los resultados obtenidos ayudarán a la organización a reconocer la necesidad de iniciar a implementar un plan de gestión de riesgos que permita mitigar los riesgos más críticos, hasta que decidan desarrollar un Plan de Tratamiento de Riesgo en el que se considere la contratación de personal especializado en seguridad, análisis de documentos y registros de incidentes, resultados de entrevistas al personal.

I. Trabajos futuros

Entre los lineamientos de futuros trabajos a desarrollarse se debería considerar desarrollar un análisis de riesgos de tipo cuantitativo considerando varios aspectos, como son: las consecuencias económicas de la materialización de una amenaza en cada activo, el costo del despliegue y mantenimiento de las salvaguardas; y estimar la probabilidad de ocurrencia de amenazas basándose en registros reales. También considerar los períodos de tiempo de recuperación de los procesos antes que las pérdidas se conviertan en irreparables y un análisis de aplicaciones críticas para definir prioridades de procesos.

REFERENCIAS

[1] J. Webb, A. Ahmad, S. B. Maynard, and G. Shanks, "A situation awareness model for information security risk management," *Comput. Secur.*, vol. 44, pp. 1–15, Jul. 2014.

[2] "ISO 27001: RISK MANAGEMENT AND COMPLIANCE - ProQuest." [Online]. Available: https://search.proquest.com/docview/226993963?pq-origsite=gscholar. [Accessed: 31-Jul-2017].

[3] "M 7.8 - 27km SSE of Muisne, Ecuador." [Online]. Available: https://earthquake.usgs.gov/earthquakes/eventpage/us20005j32#executive. [Accessed: 30-Jul-2017].

[4] CIA and CIA, *Ecuador - Geografía - Libro Mundial de Hechos*. .

[5] E. C. Klüppelberg, D. Straub and I. Welpe, "Risk - A Multidisciplinary Introduction," *Springer*, 2014.

[6] "ISO/Guide 73:2009(en)," 2009.

[7] E. M. Amutio, J. Candau and J. Mañas, "MAGERIT – Versión 3.0. Metodología De Análisis y Gestión De Riesgos De Los Sistemas De Información," vol. Libro I-, p. 10, 2012.

[8] E. R. Johnson and M. Merkow, "Security Policies and Implementation Issues," pp. 3–19, 2010.

[9] E. M. Amutio, J. Candau and J. Mañas, "MAGERIT – Versión 3.0. Metodología De Análisis y Gestión De Riesgos De Los Sistemas De Información," vol. Libro I-, p. 8, 2012.

[10] "PILAR Análisis de Gestión de Riesgos," 2014. [Online]. Available: http://www.pilar-tools.com/doc/v54/help_es/cia/index.html.

[11] E. M. Amutio, J. Candau and J. Mañas, "MAGERIT – Versión 3.0. Metodología De Análisis y Gestión De Riesgos De Los Sistemas De Información," vol. Libro I-, p. 125, 2012.

[12] C. N. Cruz b, "Evalución de riesgos de los sistemas de información de Audtioauto S.A. utilizando MAGERIT V3.0 apoyados para el análisis de las dimensiones de seguridad en los objetivos de control de COBIT V4.1," 2014.