Universidad Politécnica de Madrid

Escuela Técnica Superior de Ingenieros de Telecomunicación


# PROPUESTA DE UN PLAN DE GESTIÓN DE RIESGOS DE TECNOLOGÍA APLICADO EN LA ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

**TRABAJO FIN DE MÁSTER**

**María Fernanda Molina Miranda**

2015

Universidad Politécnica de Madrid

Escuela Técnica Superior de Ingenieros de Telecomunicación

**Máster Universitario en**
**Ingeniería de Redes y Servicios Telemáticos**

**TRABAJO FIN DE MÁSTER**

# PROPUESTA DE UN PLAN DE GESTIÓN DE RIESGOS DE TECNOLOGÍA APLICADO EN LA ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Autor

**María Fernanda Molina Miranda**

Director

**Víctor A. Villagrá González**

Departamento de Ingeniería de Sistemas Telemáticos

2015

## 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.

En el presente trabajo se han descrito los conceptos relacionados con la gestión de los riesgos de la seguridad de la información, estándares, metodologías y herramientas que proporcionan las guías necesarias para reducir el nivel de vulnerabilidad que tienen los activos ante una amenaza. Es de vital importancia que una organización, dedicada a brindar servicios tecnológicos y mantener respaldada mucha información confidencial de forma segura, cuente con un plan de gestión de riesgos para garantizar la continuidad del negocio.

Por este motivo, se ha visto la necesidad de desarrollar un análisis de riesgo tecnológico de orden cualitativo aplicado en el centro que administra y brinda los servicios de red y sistemas de la Escuela Superior Politécnica del Litoral siguiendo la metodología MAGERIT. Primero se procede a describir la situación actual de la organización, luego a identificar los activos con sus respectivas amenazas, para proseguir a realizar la medición de riesgos existentes y sugerir las salvaguardas necesarias que podrían formar parte del plan de implantación.

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.

## 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, inside the Escuela Superior Politecnica del Litoral, 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.

# Índice General

# Índice de figuras

# Índice de Tablas

## Siglas

| | |
|---|---|
| BRP | *Perfil de riesgos comerciales* |
| BS | *Estándar Británico* |
| CLUSIF | *Club de Seguridad de la Información Francesa* |
| CRAMM | *Método de Gestión y Análisis de Riesgo CCTA* |
| EEUU | *Estados Unidos de América* |
| ESPOL | *Escuela Superior Politécnica del Litoral* |
| GTSI | *Gerencia de Tecnologías Y Sistemas De Información* |
| IEC | *Comisión Electrotécnica Internacional* |
| ISO | *Organización Internacional de Estandarización* |
| NIST | *Instituto Nacional de Estándar y Tecnología* |
| OCTAVE | *Evaluación de Amenazas Operacionalmente Críticas, Activos y Vulnerabilidades* |
| PDCA | *Planificar, Hacer, Revisar y Actuar* |
| PILAR | *Procedimiento Informático Lógico para el Análisis de Riesgos* |
| RTF | *Formato de texto enriquecido* |
| SP | *Publicaciones Especiales* |
| TI | *Tecnología de la Información* |
| UML | *Lenguaje de Modelado Unificado* |
| UPS | *Sistemas de alimentación ininterrumpida* |
| VPN | *Red privada virtual* |
| XML | *Lenguaje de Marcado Extensible* |

# 1 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.

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 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.

## 1.1 Objetivos

El presente trabajo tiene por objetivo general:

- Desarrollar un plan de gestión de riesgos tecnológicos aplicado al centro que administra y brinda los servicios de red y sistemas a la Escuela Superior Politécnica del Litoral siguiendo la metodología MAGERIT.

Considerando la situación actual del centro de tecnología, los principales servicios y actividades que se realizan a diario con la finalidad de mitigar las fallas y amenazas que atentan contra la seguridad de los equipos y de la información, ya que aún no se han definido una política de seguridad ni procesos que aseguren la continuidad de los servicios.

Para la consecución del objetivo principal se han definido los siguientes objetivos específicos:

- Determinar el alcance del plan de riesgos propuesto, ya que no se cuenta con toda la documentación necesaria como pueden ser datos estadísticos de incidentes, entrevistas al personal, entre otros que permitan conocer más de cerca la situación de riesgo; el trabajo propuesto considerará los principales aspectos que puedan afectar a la pérdida o deterioro de la información.
- Definir los principales activos que forman parte del modelo de negocio del centro de tecnología, como son los equipos, lugares y aplicaciones de software que en conjunto permiten una buena administración de la institución para fines administrativos, académicos y financieros.
- Identificar las principales amenazas que afectan a los activos anteriormente considerados, pudiendo afectar la integridad, disponibilidad y confiabilidad de la información que estos almacenan o transfieren.
- Proponer salvaguardas para minimizar los riesgos que pudiesen materializarse tras las amenazas definidas anteriormente; determinando el nivel de las salvaguardas ya implementadas y de las nuevas salvaguardas.
- Contrastar los riesgos e impactos actuales con los residuales tras realizar el análisis cualitativo en la herramienta PILAR.

## 1.2 Estructura General

El contenido del presente trabajo de Fin de Máster está estructurado por seis capítulos distribuidos de la siguiente manera: el Capítulo 2 contiene la importancia y descripción de los conceptos generales relacionados al análisis y la gestión de riesgos del área TI. En el Capítulo 3 se encuentran descritos los estándares, metodologías y herramientas existentes en la industria que hacen posible la gestión de los riesgos. En el Capítulo 4 se describen las tareas y el plan de actividades que sigue una de las metodologías más aplicadas a nivel mundial como es la metodología MAGERIT. En el Capítulo 5 se exponen el alcance, objetivo y situación actual del caso de estudio a realizar; mientras que en el último capítulo se realiza el análisis de riesgos del caso de estudio planteado, el cual consiste en aplicar los conocimientos adquiridos respecto a la evaluación de activos, amenazas y los riesgos, sirviendo de apoyo la herramienta PILAR, resultando un plan para contrarrestar los riesgos actuales.

Finalmente se presentan las conclusiones y los futuros trabajos que pudieran desarrollarse para extender el análisis y conceptos expuestos en el presente trabajo.

# 2 Gestión de Riesgos

## 2.1 Importancia de la Gestión del Riesgo

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 ocurre en EEUU, "La probabilidad de un fuerte terremoto en California es cada vez mayor, según un estudio"[1], este es el titular de una noticia que se propagó en el mes de marzo del presente año, informando que los expertos han obtenido mayores porcentajes de riesgo de un terremoto de magnitud 8 en la escala de Richter debido a la falla de San Andrés.

De igual manera Ecuador se encuentra en las zonas de peligro de colisión de placas tectónicas, y además se presentan otros fenómenos hidrometeorológicos como son las inundaciones, erupciones volcánicas, deslizamientos 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.

## 2.2 Gestión del Riesgo

El riesgo se originó en el siglo 17 con las matemáticas asociadas con los juego 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

[1] 20 minutos. Disponible en: http://www.20minutos.com/noticia/21834/0/aumenta-riesgo-terremoto/magnitud-8-richter/california-estados-unidos/

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. [1]

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". [2]

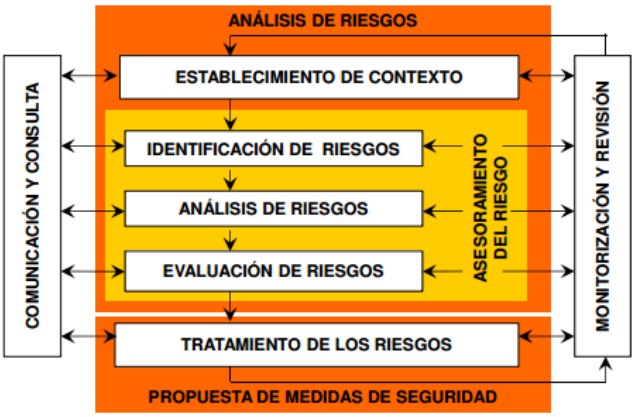



Figura 1 Esquema de Gestión del Riesgo

La gestión del riesgo consiste en seis procesos: establecimiento del contexto, evaluación del riesgo, tratamiento del riesgo, aceptación de riesgos, comunicación y consulta de riesgos, y revisión y seguimiento del riesgo. Ver figura 1.

- Establecimiento del Contexto

El proceso de establecimiento de contexto recibe como entrada toda la información relevante acerca de la organización, determinando el alcance y los límites del proceso. La salida del proceso es la especificación de estos parámetros.

- Evaluación del Riesgo

Este proceso consta de tres subprocesos: identificación de riesgos, análisis de riesgo y evaluación de riesgos. El proceso recibe como entrada la salida del proceso de establecimiento de contexto. Identifica de forma cuantitativa o cualitativa los riesgos y les da prioridad a los criterios de evaluación que dependen de los objetivos de la organización.

Al identificar los riesgos se busca determinar lo que podría causar una pérdida potencial y comprender cómo, dónde y por qué puede ocurrir dicha pérdida; identificando los activos, amenazas, medidas de seguridad, vulnerabilidades y sus consecuencias.

El análisis de riesgo se lo explica ampliamente en el apartado 2.4.

Por último, el proceso de evaluación de riesgos recibe como entrada la salida del proceso de análisis de riesgos. Se comparan los niveles de riesgo con los criterios de evaluación de riesgos y los criterios de aceptación del riesgo. El resultado del proceso es una lista de los riesgos priorizados de acuerdo a los criterios de evaluación de riesgo.

- Tratamiento del Riesgo

Tiene como objetivo seleccionar las medidas de seguridad para reducir o evitar los riesgos y definir un plan de tratamiento de riesgo. El proceso recibe como entrada la salida del proceso de evaluación de riesgos y produce como salida el plan de tratamiento de riesgos.

Después de que se han tomado las decisiones del tratamiento de riesgos, siempre habrá riesgo restante, llamados riesgos residuales. Estos riesgos pueden ser difíciles de evaluar, pero por lo menos se debe hacer una estimación para asegurar la suficiente protección. Si el riesgo residual es inaceptable, el proceso del tratamiento del riesgo se debe repetir. En el tratamiento del riesgo debe identificarse los factores limitantes y dependientes, prioridades, plazos, recursos, incluyendo las aprobaciones necesarias para su asignación.

- Consulta y Comunicación del Riesgo

Es un proceso horizontal que interactúa de forma bidireccional con todos los demás procesos de gestión de riesgos. Su propósito es establecer un entendimiento común de todos los aspectos de riesgo entre todas las parte interesadas de la organización.

- Monitoreo y Revisión del Riesgo

La gestión de riesgos es un proceso continuo, donde las medidas de seguridad implementadas son monitoreadas y revisadas para asegurar que funcionan correctamente de forman efectiva. El mantenimiento de las medidas de seguridad debe ser planeado y realizado sobre una base programada regularmente. Por último, se deben realizar auditorías internas de forma regular por parte de un tercero y tener una documentación completa, accesible y con procesos controlados para apoyar al SGSI. [3]

## 2.3 Conceptos Relacionados al Riesgo

El riesgo se genera por la interrelación de algunos elementos como se visualiza en la figura 2.

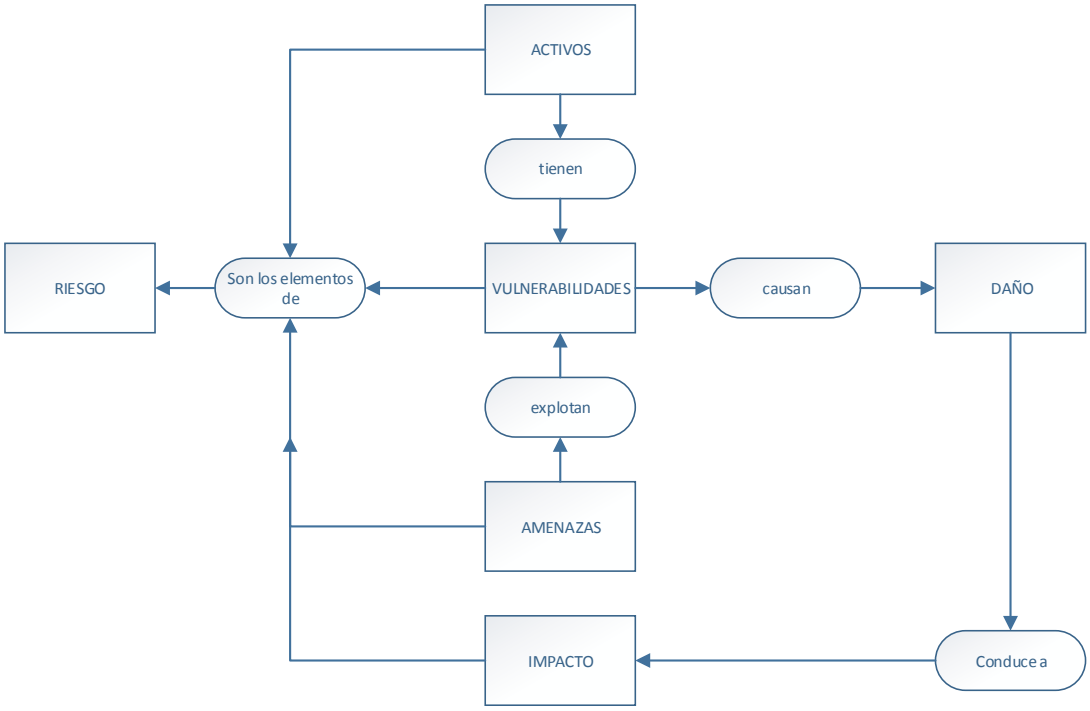



**Figura 2 Riesgo y sus conceptos relacionados**

### 2.3.1 Activo

Es cualquier cosa que tenga valor en la organización, sus operaciones comerciales y su continuidad, incluido los recursos de información que apoyan la misión de la organización.

Se pueden distinguir dos clases de activos: los activos primarios que incluyen a los procesos del negocio, actividades e información; y los activos de apoyo, que incluyen hardware (equipos de procesamiento de datos, periféricos y medios de comunicación), software (sistema operativo, servicio, software de aplicación), red, personal (directores, usuarios, personal de operación y desarrolladores), lugar y estructura de la organización (proveedores y fabricantes).

La información es un activo que, como otros activos comerciales importantes, tiene valor para la organización y, en consecuencia, necesita ser protegido adecuadamente. La seguridad informática protege la información de un amplio rango de amenazas con el objetivo de asegurar la continuidad de los negocios, minimizar el daño comercial y maximizar el reembolso de las inversiones y oportunidades comerciales.

La información puede existir en muchas formas; puede ser de forma escrita, impresa, electrónica, transmitida por correo o usando medios electrónicos o hablado en una conversación.

La seguridad de la información es evaluada por tres pilares fundamentales: Disponibilidad, Integridad y Confidencialidad.

- Confidencialidad: asegura que solo los usuarios con acceso autorizado puedan acceder a la información.

- Integridad: proteger la exactitud, totalidad de los datos y métodos de procesamiento de la información que los usuarios autorizados gestionan.

- Disponibilidad: los recursos deben estar disponibles cuando sean requeridos en cualquier instante de tiempo. [4]

### 2.3.2 Amenaza

Es una vulnerabilidad de un activo que puede ser explotado por una o más causas potenciales de un incidente, que puede resultar en daño al sistema u organización.

Las amenazas podrían presentarse de varios tipos:

- De origen natural

Incendio, inundación, tormenta eléctrica, terremoto, siniestros mayores que afectan la disponibilidad de los activos como son los equipos informáticos, infraestructura física y medios de soporte de información.

- Del entorno
  - Incendio, inundación, polvo, sobrecarga eléctrica, corte de suministro eléctrico, condiciones inadecuadas de temperatura o humedad afectan la disponibilidad de los activos como son los equipos informáticos, infraestructura física y medios de soporte de información.
  - El fallo de los servicios de comunicaciones afecta la disponibilidad de las redes de comunicaciones.
  - La degradación de los soportes de almacenamiento de la información afecta la disponibilidad de los medios de soporte de información como son las cintas de respaldo.
  - Las emanaciones electromagnéticas afectan la confidencialidad de los equipos informáticos, medios de soporte de información.

- Defecto de aplicaciones

Aquellos problemas que se producen en el equipo por defectos de fábrica o en la implementación, se denominan vulnerabilidades técnicas. Por lo general, la recuperación de este tipo de problemas se la obtiene por parte del proveedor o siguiendo una guía de configuración; para ello se debe tener respaldada la información para restaurarla cuando sea necesario.

- Causadas por las personas de forma accidental.

- Los errores de los usuarios que usan el servicio afectan la integridad, confidencialidad y disponibilidad de los datos, servicios, claves criptográficas, soportes de información y aplicaciones.
- Los errores del administrador responsable de la instalación y operación afectan la disponibilidad, integridad y confidencialidad de los datos, claves criptográficas, servicios, aplicaciones, equipos informáticos, redes de comunicación y soportes de información.
- Los errores de monitorización afectan la trazabilidad de los registros de actividad, por la falta de registros, registros incompletos, registros incorrectamente fechados o registros incorrectamente atribuidos.
- Los errores de configuración afectan la integridad de los datos de configuración.
- Los errores de encaminamiento afectan la confidencialidad de los servicios, aplicaciones y las redes de comunicaciones.

- Causadas por las personas de formas deliberada
  - La manipulación de los registros de actividad afectan la integridad y por lo tanto la trazabilidad de los registros de actividad.
  - La manipulación de la configuración afecta la integridad, confidencialidad y disponibilidad de los registros de actividad.
  - La suplantación de la identidad del usuario, abuso de privilegios de acceso y acceso no autorizado afectan la confidencialidad, autenticidad e integridad de la información, claves criptográficas, servicios, aplicaciones y redes de comunicaciones.
  - La monitorización no autorizada del tráfico y la intercepción de información afecta la confidencialidad de las redes de comunicaciones.
  - El robo y ataque destructivo de los activos afectan la disponibilidad y confidencialidad.
  - La propagación de virus, spyware, gusanos, troyanos, bombas lógicas afectan la disponibilidad, integridad y confidencialidad de las aplicaciones. [5]

### 2.3.3 Vulnerabilidad

Los activos se ven influidos por una serie de amenazas; la probabilidad de que se materialice una de dichas amenazas y la degradación que le supone a un activo es lo que se conoce como vulnerabilidad según MAGERIT.

Se clasifican de acuerdo a la clase de activos, es decir: hardware (susceptibilidad a la humedad, polvo, suciedad, almacenamiento sin protección), software (sin pruebas de software, falta de seguimiento de auditoría), red (líneas inadecuadas, falta de seguridad),

sitio (ubicación en un área susceptible a inundaciones, red de energía inestable), y organización (falta de auditorías periódicas, falta de planes de continuidad).

### 2.3.4 Impacto

Es un indicador de qué puede suceder cuando ocurren las amenazas, siendo la medida del daño causado por una amenaza cuando se materializa sobre un activo. El impacto se estima, conociendo el valor de los activos y la degradación causa por las amenazas.

| Impacto = Valor * Degradación |
|---|

## 2.4 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. 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. [6]

El análisis de riesgo se realiza ya sea cuantitativa o cualitativamente. El análisis cualitativo es recomendable hacerlo en primer lugar, 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.

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. [7]

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

Riesgo = Probabilidad * Impacto

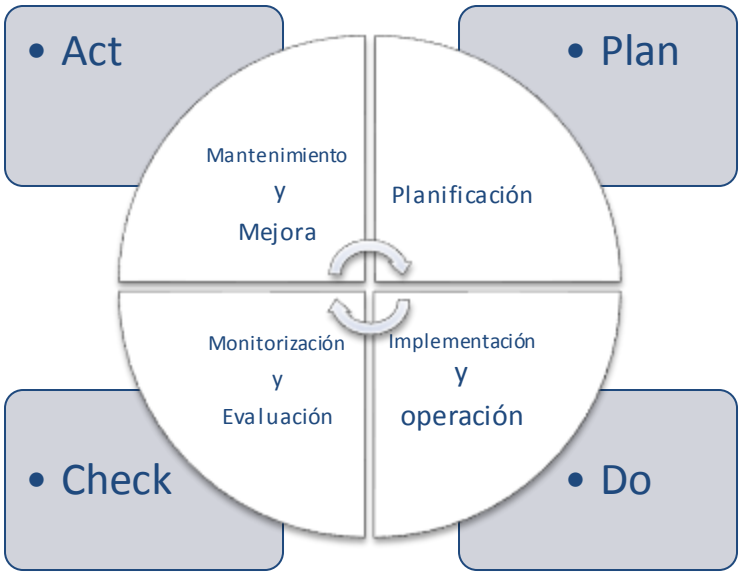



Figura 3 Ciclo PDCA

# 3 Estándares y Metodologías de Gestión del Riesgo

## 3.1 Estándares de Gestión del Riesgo

Existen varios estándares internacionales que están relacionados, directa o indirectamente con la gestión de riesgos de sistemas de información. Las normas internaciones más importantes son:

BS 7799 es un norma publicada por el British Standard Institute que tiene como objetivo dar efectiva seguridad de la información a través de un programa permanente de actividades de gestión de riesgos, además incluye la identificación y evaluación del riesgo mediante la implementación y mejora continua del sistema basado en el control del riesgo.

La serie ISO/IEC 27000 es una familia de estándares sobre gestión de la seguridad de la información derivados de la norma británica BS 7799, varias normas dentro de las series ya han sido publicadas; otros se encuentran en desarrollo. Dentro de esta serie están ISO/IEC 27001:2013 - Requisitos de la Gestión de la Seguridad de la Información, estándar diseñado para asegurar la selección de las medidas adecuadas de seguridad que protegen los activos de información y brindan confianza a las partes interesadas. La norma abarca todo tipo de organizaciones como pueden ser: empresas comerciales, agencias gubernamentales y organizaciones sin fines de lucro; y especifica los requisitos para establecer, implementar, operar, monitorear, revisar, mantener y mejorar un sistema de gestión de la seguridad de la información en el contexto de la organización. Además se especifican los requisitos para la aplicación de medidas de seguridad adaptados a las necesidades de las organizaciones.

La ISO/IEC 27002:2013 define qué debe hacerse en términos de controles de seguridad de la información, proporciona las directrices para las normas de seguridad de la información de la organización y las prácticas de gestión de seguridad de la información, incluyendo la selección, implementación y gestión de controles, teniendo en cuenta el entorno de riesgo en la seguridad de la información.

La norma ISO/IEC 27005:2011 - Gestión de riesgos en seguridad de la información, esta norma proporciona recomendaciones y lineamientos de métodos y técnicas de evaluación de riesgos de Seguridad en la Información. Es compatible con los conceptos generales especificados en la norma ISO/IEC 27001 y está diseñado para guiar en la implementación de seguridad de la información basado en el enfoque de gestión de riesgos.

El estándar ISO/IEC 31000:2009 – Principios y directrices de gestión de riesgos, se puede aplicar a cualquier tipo de riesgo, cualquiera que sea su naturaleza, tanto si tiene

consecuencias positivas o negativas. Esta norma no es específicamente sobre la seguridad de la información o para los riesgos de TI. Proporciona un enfoque común en apoyo a las normas de control de riesgos.

La guía ISO 73:2009 proporciona las definiciones de los términos relaciones con la gestión de riesgos. Su objetivo es fomentar una comprensión y enfoque coherente, la descripción de las actividades relacionadas con la gestión del riesgo y el uso de la terminología uniforme a los procesos y marcos que se ocupan de esta gestión. [8]

La "Guía de gestión de riesgos para los sistemas de tecnología de la información" de EEUU, SP 800-53 proporciona una base común para el personal con y sin experiencia, técnicos y no técnicos que usan el proceso de gestión de riesgos en sus sistemas de TI. Las directrices de NIST son para las organizaciones federales que procesan información sensible, pero también puede ser utilizado por empresas no gubernamentales. [9]

## 3.2 Metodologías

Un método es un procedimiento o proceso sistemático y ordenada para alcanzar algún objetivo. 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:

**Tabla 1 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.

Tabla 2 Matriz de 3 Niveles de Riesgo

| | | | | |
|---|---|---|---|---|
| **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** | | |

A continuación una breve descripción de las metodologías más reconocidas:

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

### 3.2.1 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.

Los objetivos que busca alcanzar son:

- Hacer que los responsables de los sistemas de información sean conscientes de la existencia de riesgos y de la necesidad de tratarla a tiempo.
- Ofrecer un método sistemático para el análisis de riesgos.
- Ayudar en la descripción y planificación de las medidas adecuadas para mantener los riesgos bajo control.
- De forma indirecta, preparar la organización de los procesos de evaluación, auditoría, certificación o acreditación, según corresponda en cada caso.

La metodología se puede resumir en el siguiente gráfico. Ver figura 4.

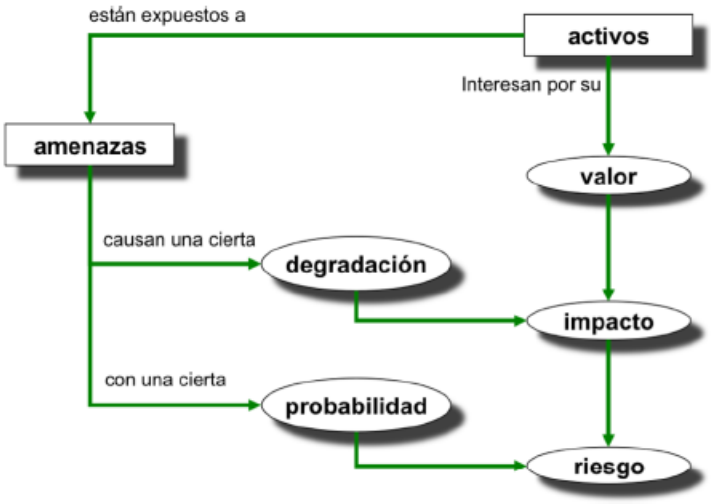



Figura 4 Modelo MAGERIT

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 [10]

### 3.2.2 OCTAVE

OCTAVE es la metodología de Evaluación de Amenazas Operacionalmente Críticas, Activos y Vulnerabilidades para agilizar y optimizar el proceso de evaluación de riesgos de seguridad de la información alineados a los objetivos y metas de la organización.

Existen tres metodologías publicadas: OCTAVE aplicable en organizaciones con más de 300 empleados, OCTAVE-S aplicable en organizaciones de hasta 100 empleados y OCTAVE Allegro que permite una amplia evaluación del entorno del riesgo operativo sin la necesidad de un amplio conocimiento de evaluación de riesgos y requiere menos tiempo de implementación.

Los dos objetivos específicos de OCTAVE son:

- Desmitificar la falsa creencia: la seguridad informática es un solamente un asunto técnico.

- Presentar los principios básicos y la estructura de las mejores prácticas internacionales que guían los asuntos no técnicos.

OCTAVE divide los activos en dos tipos: sistemas y personas. En el primer grupo se consideran el hardware, software y los datos.

La metodología OCTAVE está compuesta por tres fases:

1. Visión de la Organización: donde se definen los elementos como los activos, vulnerabilidad de la organización, amenazas, exigencias de seguridad y normas existentes.
2. Visión Tecnológica: se clasifican en dos componentes, las claves y vulnerabilidades técnicas.
3. Planificación de las medidas y reducción de riesgos: se clasifican los elementos como la evaluación de riesgos, estrategia de protección, ponderación de los riesgos y plano de reducción de riesgos.

El método OCTAVE ofrece un proceso simplificado enfocado en los activos de la información, que pretende ayudar a una organización a:

- Desarrollar criterios de evaluación de riesgos cualitativos que describen el riesgo operacional de la organización.
- Identificar los activos que son importantes para la misión de la organización.
- Identificar las vulnerabilidades y amenazas de los activos.
- Determinar y evaluar las consecuencias potenciales para la organización tras una amenaza.

La metodología de OCTAVE Allegro consiste en 8 pasos organizados en 4 etapas, ilustrado en la figura 5. [11]

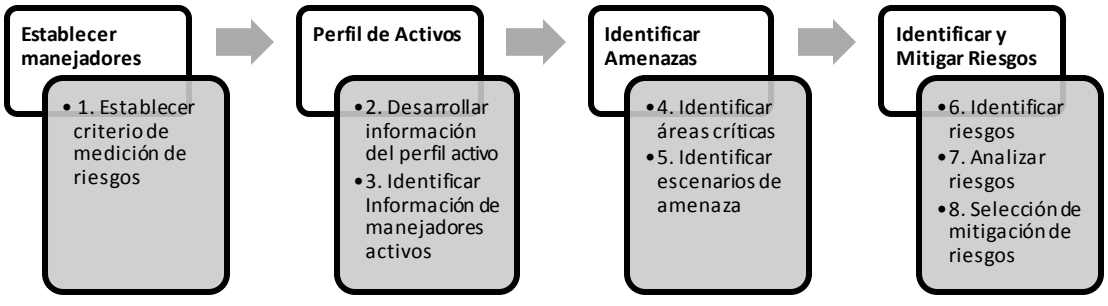



**Figura 5 Procesos de OCTAVE Allegro**

- Establecer manejadores, donde la organización desarrolla los criterios de medición de riesgos que sean coherentes con los manejadores de la organización.

- Perfil de activos, donde los activos que son el foco de evaluación de riesgos se identifican y se perfilan.
- Identificar las amenazas, donde las amenazas de los activos, dentro del contexto de los contenedores, son identificadas y documentadas a través de un proceso estructurado.
- Identificar y mitigar riesgos, donde se identifican y analizan los riesgos que se basan en la información sobre amenazas, y se desarrollan las estrategias de mitigación para manejar los riesgos.

Las salidas de cada paso en el proceso son documentadas en una serie de hojas de trabajos que son usadas como entradas del siguiente paso en el proceso.

### 3.2.3 Metodología NIST SP 800-30

El Instituto Nacional de Estándares y Tecnología (NIST) fundado en 1901 es parte del Ministerio de Comercio de Estados Unidos. Los estándares de NIST deben ser cumplidos por todos los productos y servicios que de alguna forma dependen de alguna tecnología, desde los dispositivos creados a nano escala hasta por una red eléctrica inteligente. [9]

La Ley de Gestión de la Seguridad de la Información Federal (FISMA) requiere a las agencias federales seguir un conjunto de estándares de seguridad. Estos estándares son provistos por NIST y son conocidos como Estándares Federales de Procesamiento de Información (FIPS).

FIPS es una serie de publicaciones especiales de la serie SP 800 sobre la seguridad de la información. Esta serie incluye una metodología para el análisis y gestión de riesgos de la seguridad de la información, alineada y complementaria con el resto de documentos de la serie.

La metodología NIST SP 800-30 está compuesta por 9 pasos básicos para el análisis de riesgo. Ver figura 6.

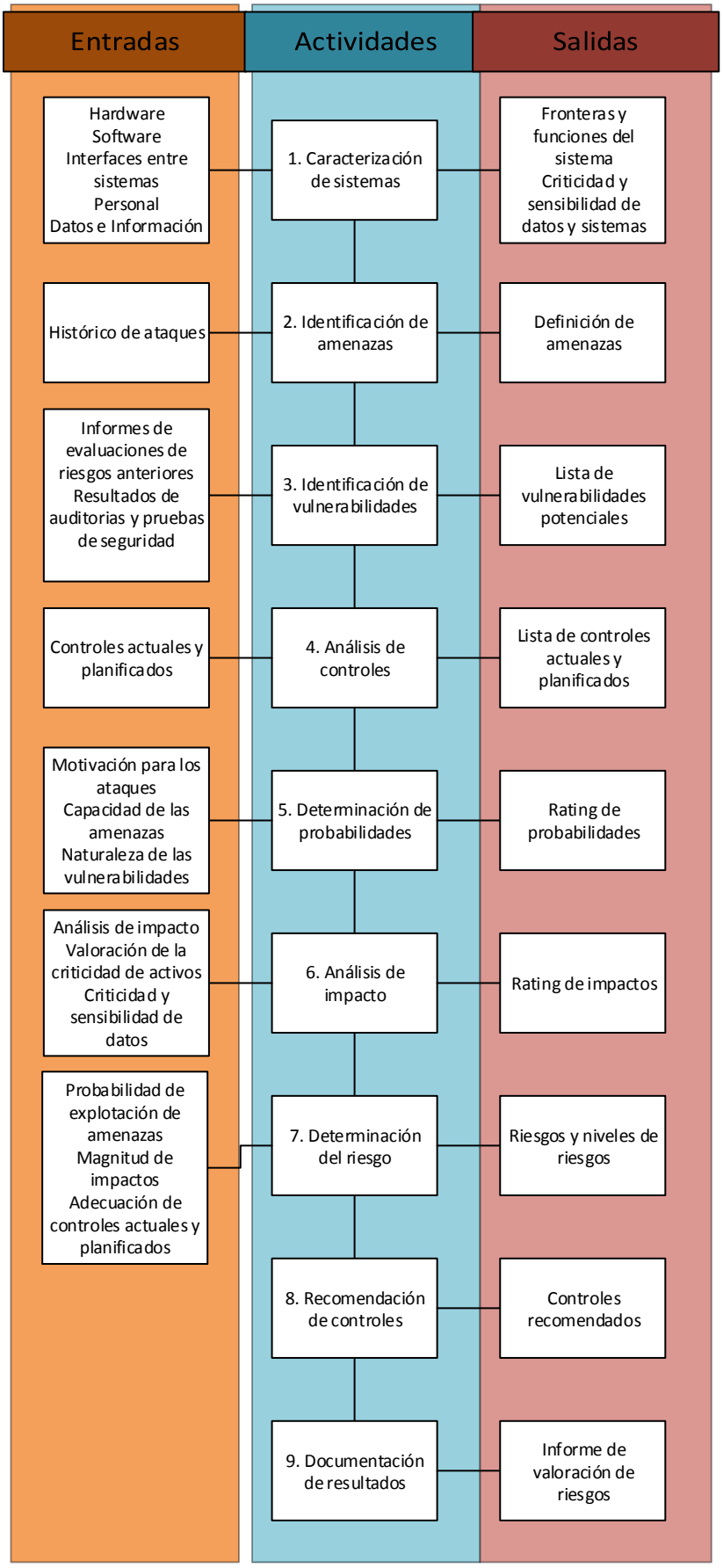



Figura 6 Metodología NIST SP 800-30

El proceso de gestión de riesgos definido en la metodología NIST SP800-30 puede resumirse en el siguiente gráfico. Ver figura 7.

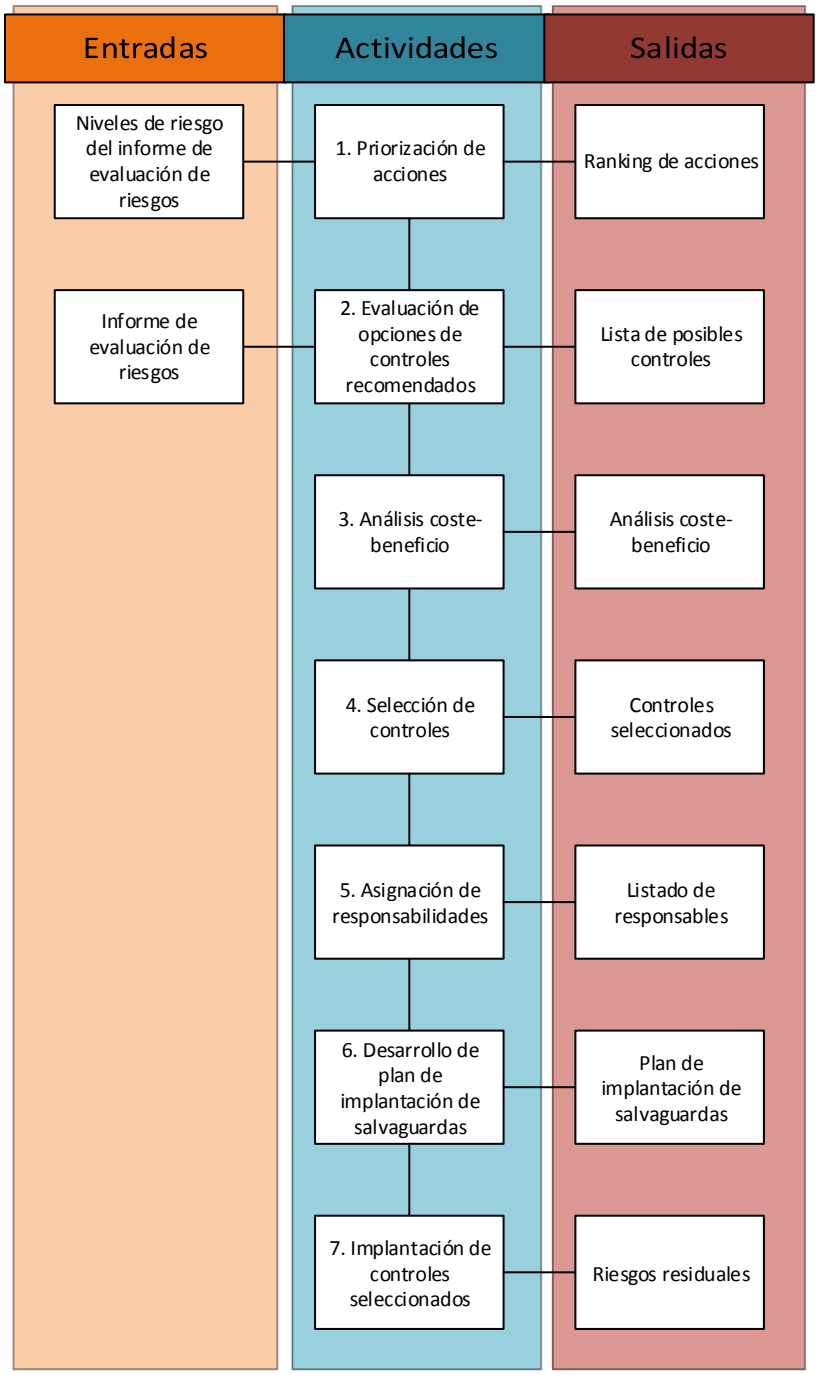



Figura 7 Proceso de Gestión - NIST SP800-30

### 3.2.4 CRAMM

Es una metodología desarrollada en el Reino Unido por la Agencia Central de Cómputo y Telecomunicaciones CCTA. Es el método de análisis de riesgo preferido en los organismos de administración pública. Se compone de tres etapas, cada una apoyada por cuestionarios, objetivos y directrices. Las dos primeras se encargan de identificar y

analizar los riesgos para el sistema, y la tercera recomienda la manera en que estos riesgos deben ser gestionados. CRAMM sigue el siguiente proceso:

- Utiliza reuniones, entrevistas y cuestionarios para la recolección de datos.
- Identifica y clasifica los activos de TI en tres categorías; datos, software y activos físicos.
- Requiere que se consideren el impacto de la pérdida de confidencialidad, integridad y disponibilidad del activo.
- Mide la vulnerabilidad por niveles: muy alto, alto, medio, bajo o muy bajo.
- Mide el riesgo por niveles: alta, media o baja. [12]

### 3.2.5 MEHARI

Es la metodología de análisis y gestión de riesgos desarrollada por la CLUSIF (CLUb de la Sécurité de l'Information Français) en 1995 y se deriva de las metodologías previas Melissa y Marion.

El primer objetivo de MEHARI es proporcionar un método para la evaluación y gestión de los riesgos, concretamente en el dominio de la seguridad de la información, conforme a los requerimientos de la ISO/IEC 27005, proporcionando el conjunto de herramientas y elementos necesarios para su implementación:

Otros objetivos adicionales son:

- Permitir un análisis directo e individual de situaciones de riesgos descritas en los escenarios.
- Proporcionar un completo conjunto de herramientas específicamente diseñadas para la gestión de la seguridad a corto, medio y largo plazo, adaptables a diferentes niveles de madurez y tipos de acciones consideradas.[13]

### 3.2.6 CORAS

Desarrollado a partir de 2001 por SINTEF, un grupo de investigación noruego financiado por organizaciones del sector público y privado. Se desarrolló en el marco del Proyecto CORAS financiado por la Unión Europea.

El método CORAS proporciona:

- Una metodología de análisis de riesgos basado en la elaboración de modelos, que consta de siete pasos, basados fundamentalmente en entrevistas con los expertos.
- Un lenguaje gráfico basado en UML para la definición de los modelos (activos, amenazas, riesgos y salvaguardas), y guías para su utilización a lo largo del proceso. El lenguaje se ha definido como un perfil UML.

- Un editor gráfico para soportar la elaboración de los modelos, basado en Microsoft Visio.
- Una biblioteca de casos reutilizables.
- Una herramienta de gestión de casos, que permite su gestión y reutilización.
- Representación textual basada en XML del lenguaje gráfico.
- Un formato estándar de informe para facilitar la comunicación de distintas partes en el proceso de análisis de riesgos. [14]

Los ocho pasos del método CORAS pueden representarse gráficamente de la siguiente forma, ver la figura 8.


Figura 8 Los ocho pasos de la metodología CORAS

## 3.3 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.

A continuación una breve descripción de tres herramientas útiles para el análisis de riesgo:

- MSAT
- RISICARE
- PILAR

### 3.3.1 Herramienta de Evaluación de Seguridad de Microsoft (MSAT)

Esta herramienta gratuita de Microsoft emplea un enfoque integral para la medición de la seguridad para temas que abarcan tanto personas, procesos y tecnología; ofreciendo información y recomendaciones para la seguridad del ambiente informático de empresa con menos de 1000 empleados, a fin de ayudarles a comprender los riesgos potenciales que afrontan y el nivel de madurez de seguridad de la organización.

Utiliza el concepto de defensa en profundidad para implementar capas de defensa que incluyen controles técnicos, estándares organizativos y operativos, basándose en las mejores prácticas aceptas para reducir el riesgo en ambientes de TI como son ISO 17799 y NIST -800.x.

MSAT proporciona:

- Conocimiento constante, complejo y fácil de utilizar acerca del nivel de seguridad.
- Marco de defensa de profundidad con análisis comparativos del sector.
- Informes detallados y actuales comparando el plan inicial con los avances obtenidos.
- Recomendaciones comprobadas y actividades prioritarias para mejorar la seguridad.
- Consejos estructurados de Microsoft y de la industria.

La evaluación de riesgos consiste en dos partes:

- Un perfil de los riesgos comerciales (BRP).- Consta de alrededor 200 preguntas distribuidas sobre el modelo de la empresa para calcular el riesgo.
- Una evaluación para determinar las medidas de seguridad formadas por capas de defensa compuesta por cuatro áreas de análisis: infraestructura, aplicaciones, operaciones y usuarios.[15]

### 3.3.2 RISICARE

Es una herramienta basada en el método MEHARI que mejora la productividad y la precisión de un enfoque de gestión de riesgos especialmente en contexto de empresas

medianas. RISICARE define un perímetro de procesos claves para optimizar el proceso y los recursos sean internos o externos; apoyado en los siguientes parámetros:

- Utilizar el método MEHARI desarrollado dentro de CLUSIF.
- Personalizar la base de conocimientos e incluso construir sus propias base de conocimiento.
- Relacionar la cuantificación de los escenarios de riesgo con una posible auditoría.
- Desarrollar planes coherentes para optimizar la reducción de riesgos generales.
- Ser una herramienta potente y de fácil uso integrándose con Windows.

RISICARE consta de 4 fases:

1. Establecimiento del contexto.- Primero se identifican y se clasifican los activos, luego se establece un vínculo entre los procesos del negocio y finalmente se cuantifican las vulnerabilidades de los activos.
2. Análisis de lo Existente.- Se mide el nivel de madurez de la empresa en función de la taxonomía de temas de auditoría de CLUSIF 2010.
3. Tratamiento de Riesgos.- Se garantiza el cumplimiento de la norma ISO 27005, realizando planes de acción destinados a reducir la gravedad de los riesgos.
4. Aceptación del Riesgo.- Definir medios para evitar, transferir y reducir el riesgo. [16]

### 3.3.3 PILAR

PILAR es una herramienta desarrollada para soportar el análisis y la gestión de riesgos de sistemas de información siguiendo la metodología MAGERIT. Las siglas de PILAR provienen de "Procedimiento Informático Lógico para el Análisis de Riesgos" creado por el Centro Nacional de Inteligencia, actualmente se encuentra disponible la versión 5.4.

Analiza los riesgos en varias dimensiones: confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad. Para tratar el riesgo se proponen: salvaguarda 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. [17]

# 4 Metodología MAGERIT

## 4.1 Pasos a seguir

Paso 1: Definir Activos

Llevar a cabo un inventario de equipo de cómputo, software y mobiliario, para determinar cuál es la información crítica que se tiene que resguardas, adicionalmente levantar un inventario de los servicios de cómputo, telecomunicaciones, internet, etc., que son requeridos para que los usuarios estén en posibilidad de llevar a cabo sus actividades normales.

Paso 2: Determinar Amenazas

Al determinar la amenaza que perjudica a un activo, hay que valorar su influencia en el valor del activo, en dos sentidos: Degradación, es decir conocer cuán perjudicado resultaría el activo y por la probabilidad, es decir cuán probable o improbable es que se materialice la amenaza.

La probabilidad de ocurrencia se modela de forma cualitativa y cuantitativa. Ver tabla 3.

**Tabla 3 Modelación de la probabilidad de ocurrencia**

| | Cualitativamente | | | Cuantitativamente | | |
|---|---|---|---|---|---|---|
| **MA** | Muy alta | Casi seguro | Fácil | 100 | Muy frecuente | A diario |
| **A** | Alta | Muy alto | Medio | 10 | Frecuente | Mensualmente |
| **M** | Media | Posible | Difícil | 1 | Normal | Una vez al año |
| **B** | Baja | Poco probable | Muy difícil | 1/10 | Poco frecuente | Cada varios años |
| **MB** | Muy baja | Muy raro | Extremadamente difícil | 1/100 | Muy poco frecuente | siglos |

Paso 3. Determinar Salvaguardas

Son aquellos procedimientos o mecanismos tecnológicos que reducen el riesgo. Revisar la seguridad, controles físicos y ambientales existentes, evaluando si son adecuados respecto a las posibles amenazas. Se debe estar preparado para cualquier percance, verificando que dentro de la organización se cuente con los elementos necesarios para salvaguardar sus activos.

Existen diversos tipos de protección prestados por las salvaguardas:

- Prevención.- Cuando reduce oportunidades que ocurra un incidente.

- Disuasión.- Aquellas salvaguardas que actúan antes del incidente y los atacantes no se atreven a atacar.
- Eliminación.- Cuando es eliminado un incidente y no ocurre.
- Minimización del impacto.- Cuando se el impacto es limitado y se acotan las consecuencias de un incidente.
- Corrección.- Tras producirse el daño, la salvaguarda lo repara.
- Recuperación.- La salvaguarda permite volver al estado anterior luego de ocurrido el incidente.
- Monitorización.- Salvaguardas que monitorean lo que ocurre.
- Detección.- Detecta un ataque cuando informa de que el ataque está ocurriendo.
- Concienciación.- Actividades de formación de las personas anexas al sistema que pueden tener una influencia sobre él.
- Administración.- Relacionadas con los componentes de seguridad del sistema.

Para medir los aspectos organizativos, se puede emplear una escala de madurez de eficacia. Ver tabla 4.

**Tabla 4 Eficacia y Madurez de salvaguardas**

| FACTOR | NIVEL | SIGNIFICADO |
|---|---|---|
| **0%** | L0 | Inexistente |
| | L1 | Inicial / ad hoc |
| | L2 | Reproducible, pero intuitivo |
| | L3 | Proceso definido |
| | L4 | Gestionado y medible |
| **100%** | L5 | Optimizado |

Paso 4: Impacto Residual

El sistema queda en una situación de posible impacto cuando en su proceso de gestión existe un conjunto de salvaguardas desplegadas y una medida de madurez. El impacto residual puede calcularse acumulado sobre los activos inferiores, o repercutido sobre los activos superiores.

Paso 5. Riesgo Residual

El sistema queda en una situación de posible riesgo cuando en su proceso de gestión existe un conjunto de salvaguardas desplegadas y una medida de madurez.

## 4.2 Plan de Actividades

El análisis de los riesgos se realiza a través de tareas según la metodología MAGERIT.

**Tareas del Método de Análisis de Riesgos**

4.2.1 – Caracterización de los activos

1.1 – Identificación de los activos
1.2 – Dependencias entre activos
1.3 – Valoración de los activos

4.2.2 – Caracterización de las amenazas

2.1 – Identificación de las amenazas
2.2 – Valoración de las amenazas

4.2.3 – Caracterización de las salvaguardas

3.1 – Identificación de las salvaguardas pertinentes
3.2 – Valoración de las salvaguardas

4.2.4 – Estimación del estado del riesgo

4.1 – Estimación del impacto
4.2 – Estimación del riesgo

### 4.2.1 Tarea 1: Caracterización de los Activos

Esta actividad busca identificar los activos relevantes dentro del sistema a analizar, caracterizándolos por el tipo de activo, identificando las relaciones entre los diferentes activos, determinando en qué dimensiones de seguridad son importantes y valorando esta importancia. Se compone de 3 sub-tareas:

#### 4.2.1.1 Identificación de los Activos

Esta actividad se basa en recolectar la información necesaria para identificar los activos, mediante entrevistas al personal, solicitando diagramas de proceso y de flujos de datos. De esta manera, se puede medir el alcance del proyecto y obtener las relaciones entre los activos.

#### 4.2.1.2 Dependencias entre Activos

El objetivo de esta tarea es identificar y valorar las dependencias entre activos, es decir, conocer la medida en que un activo de orden superior se puede ver perjudicado por una amenaza sobre un activo de orden inferior; resultando diagramas de dependencia.

#### 4.2.1.3 Valoración de los Activos

El objetivo es identificar en qué dimensión es valioso el activo, para lo cual a la organización significara una pérdida en caso de que fuese afectado. El resultado de esta actividad es el informe denominado "modelo de valor".

### 4.2.2 Tarea 2: Caracterización de las Amenazas

Esta actividad busca identificar las amenazas relevantes sobre el sistema a analizar, caracterizándolas por las estimaciones de ocurrencia o probabilidad y daño causado o degradación. Se compone de 2 sub-tareas:

#### 4.2.2.1 Identificación de las amenazas

Se debe identificar las amenazas más relevantes sobre cada activo, se lo consigue analizando los informes y registros de incidentes y vulnerabilidades. Además realizando árboles de ataque, los cuales permiten estudiar y analizar cómo se puede atacar un objetivo permitiendo identificar qué salvaguardas se necesitan desplegar para impedirlo.

#### 4.2.2.2 Valoración de las amenazas

El objetivo es estimar la frecuencia de ocurrencia de cada amenaza sobre cada activo, estimando la degradación que causaría la amenaza en cada dimensión del activo si llegara a materializarse. El resultado de esta actividad es el informe denominado "mapa de riesgos".

### 4.2.3 Tarea 3: Caracterización de las Salvaguardas

Esta actividad busca identificar las salvaguardas desplegadas en el sistema a analizar, calificándolas por su eficacia frente a las amenazas que pretenden mitigar. Se compone de 2 sub-tareas:

#### 4.2.3.1 Identificación de las salvaguardas pertinentes

Esto se logra analizando los informes de productos y servicios, indicadores de impacto y riesgo residual y los modelos de activos y amenazas del sistema.

#### 4.2.3.2 Valoración de las salvaguardas

Luego de tener el listado de salvaguardas, conviene determinar la eficacia sobre los activos considerando:

- La idoneidad de la salvaguarda para el fin perseguido
- Calidad de implantación
- Formación de los responsables de su configuración y operación
- Existencia de controles de medida de su efectividad.

El resultado de esta actividad se concreta en varios informes: declaración de aplicabilidad, evaluación de salvaguardas, y de insuficiencias o vulnerabilidades del sistema de protección.

### 4.2.4 Tarea 4: Estimación del Estado del Riesgo

Esta actividad procesa todos los datos recopilados en las actividades anteriores para:

- Realizar un informe del estado de riesgo: estimación de impacto y riesgo.
- Realizar un informe de insuficiencias: deficiencias o debilidades en el sistema de salvaguardas.

Esta actividad consta de dos tareas:

#### 4.2.4.1 Estimación del Impacto

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

- Impacto potencial.- Al que se encuentra expuesto el sistema teniendo en cuenta el valor de los activos y la valoración de las amenazas; pero no las salvaguardas actualmente desplegadas.
- Impacto residual.- Al que se encuentra expuesto el sistema teniendo en cuenta el valor de los activos y la valoración de las amenazas, así como la eficacia de las salvaguardas actualmente desplegadas.

#### 4.2.4.2 Estimación del Riesgo

En esta tarea se estima el riesgo al que están sometidos los activos del sistema:

- Riesgo Potencial.- Al que está sometido el sistema teniendo en cuenta el valor de los activos y la valoración de las amenazas, pero no las salvaguardas actualmente desplegadas.
- Riesgo Residual.- Al que está sometido el sistema teniendo en cuenta el valor de los activos y la valoración de las amenazas, así como la eficacia de las salvaguardas actualmente desplegadas. [18]

# 5 Caso de Estudio - Escenario

## 5.1 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 GTSI 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.

Finalmente lo que se desea demostrar con el caso de estudio es el nivel de madurez actual respecto a la seguridad y por lo tanto aceptar la necesidad de implementar un plan de gestión de riesgos en un ambiente donde las amenazas siempre están presentes y si no son debidamente controladas pueden ocasionar grandes pérdidas.

## 5.2 Objetivos

- Identificar el nivel de riesgo en que se encuentran los activos de GTSI y tratar de minimizarlos con las respectivas salvaguardas.
- Conocer el nivel de madurez de la seguridad actual.
- Incentivar al personal a seguir normas y procedimientos referentes a la seguridad de la información y recursos.

## 5.3 Situación Actual

ESPOL es una institución de educación superior de gran prestigio en la ciudad de Guayaquil, cuya misión es "Formar profesionales de excelencia, socialmente responsables, líderes, emprendedores, con principios y valores morales y éticos, que contribuyan al desarrollo científico, tecnológico, social, económico, ambiental y político del país; y, hacer investigación, innovación, transferencia de tecnología y extensión de calidad para servir a la sociedad". Y su visión es "Ser líder y referente de la Educación Superior de América Latina". [19]

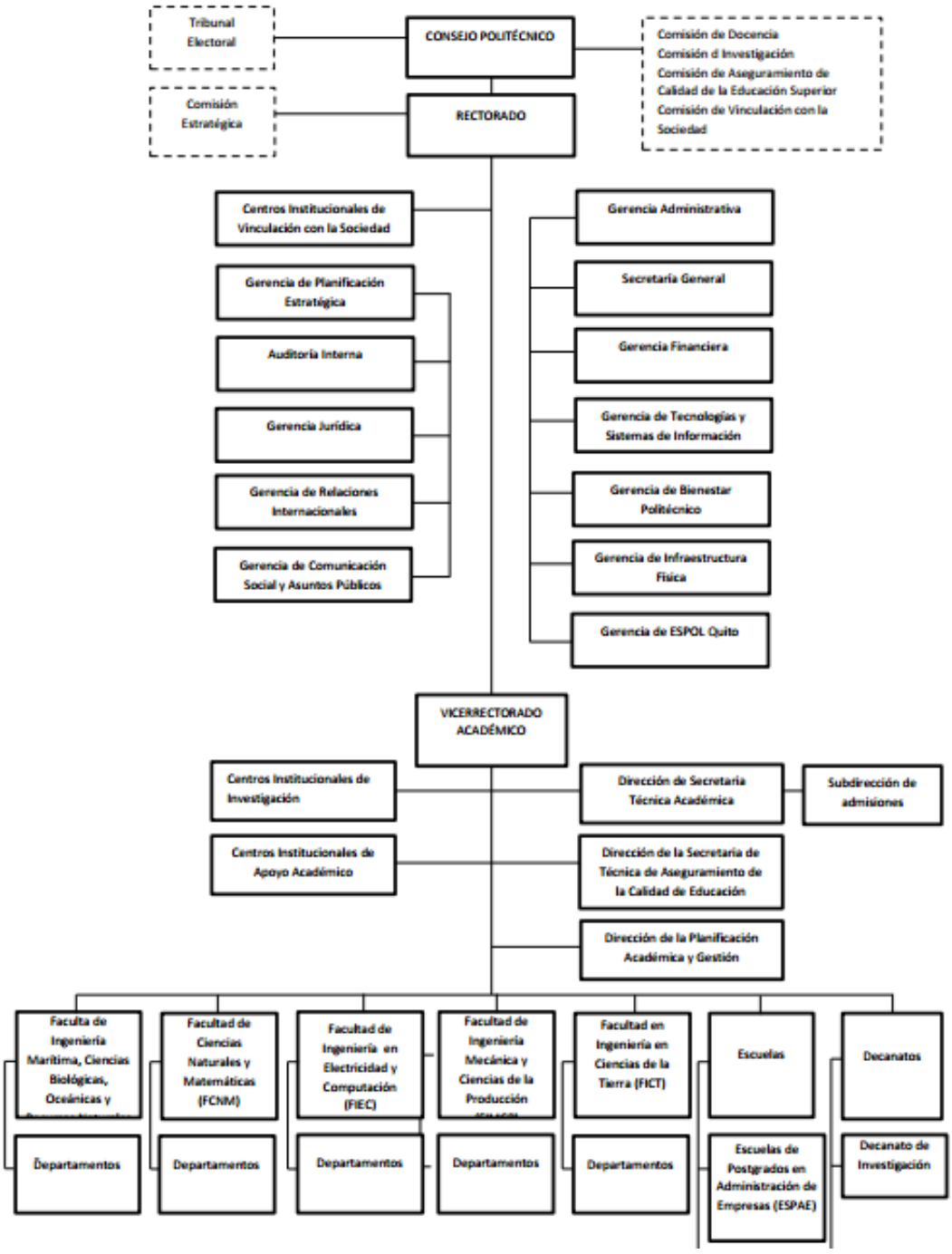



Figura 9 Organigrama ESPOL

En la figura 9 se presenta la estructura orgánica, en la cual constan centros de apoyos y entre estos se encuentra la Gerencia de Tecnologías Y Sistemas De Información (GTSI) que provee la infraestructura y procesos para brindar los servicios tecnológicos necesarios para cumplir las tareas académicas y administrativas de la institución. [20]

ESPOL se compone por 5 campus: dos ubicados en la ciudad de Guayaquil, que son Campus Prosperina y Peñas, los demás tienen el mismo nombre de la ciudad donde se localizan, Campus Quito, Campus Manglaralto y Campus Ancón; siendo el principal el campus Prosperina donde se están ubicados la mayor parte de las facultades y departamentos que conforman la institución, entre estos GTSI.

GTSI cuenta con una infraestructura de equipos muy variada, ya que se encuentra en una etapa de renovación de equipos que han estado en funcionamiento por más de 10 años, adquiriéndose equipos con última tecnología para almacenamiento, virtualización, nuevos cortafuegos y equipos de conmutación de red; lo cual ha conllevado a superar algunas dificultades de compatibilidad, configuración y administración.

Entorno físico

El edificio de GTSI es de una sola planta, su interior se divide en dos áreas, el área de oficinas y el área del centro de datos donde se encuentran los equipos de telecomunicaciones y servidores que conforman el núcleo de la infraestructura de TI. Ambas áreas cuentan con sistemas de climatización, extintores y detectores de humo. El edificio tiene conexión hacia un cuarto de generadores eléctricos que alimentan a los sistemas UPS que protegen a los equipos de sobrecargas eléctricas y apagones.

El control de acceso al edificio se resguarda por dos puertas, una tiene un detector de huellas; una persona en recepción se encarga de llevar un control de personal que ingresa y sale del edificio. Además hay cámaras de seguridad instaladas.

En el centro de datos se componen por cinco armarios: cuatro armarios son abiertos donde se encuentran los equipos de comunicaciones y servidores de tipo rack y un armario con puerta.

Infraestructura

La organización cuenta con una conexión permanente de Internet a través de enlace fibra óptica con el proveedor, protegido por un enlace de respaldo; y una red estrella de fibra óptica que conecta a los distintos edificios de las facultades hacia GTSI.

La red está conformada por segmentos de redes públicas y privadas que han sido distribuidas dependiendo de forma equitativa para cada facultad y servicios mediante vlans.

Cada uno de los campus tiene conexión con un proveedor para acceder al Internet y un enlace dedicado con el campus principal para acceder a los servicios internos.

Como se puede visualizar en la figura 10, la topología de red 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 cortafuegos 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.

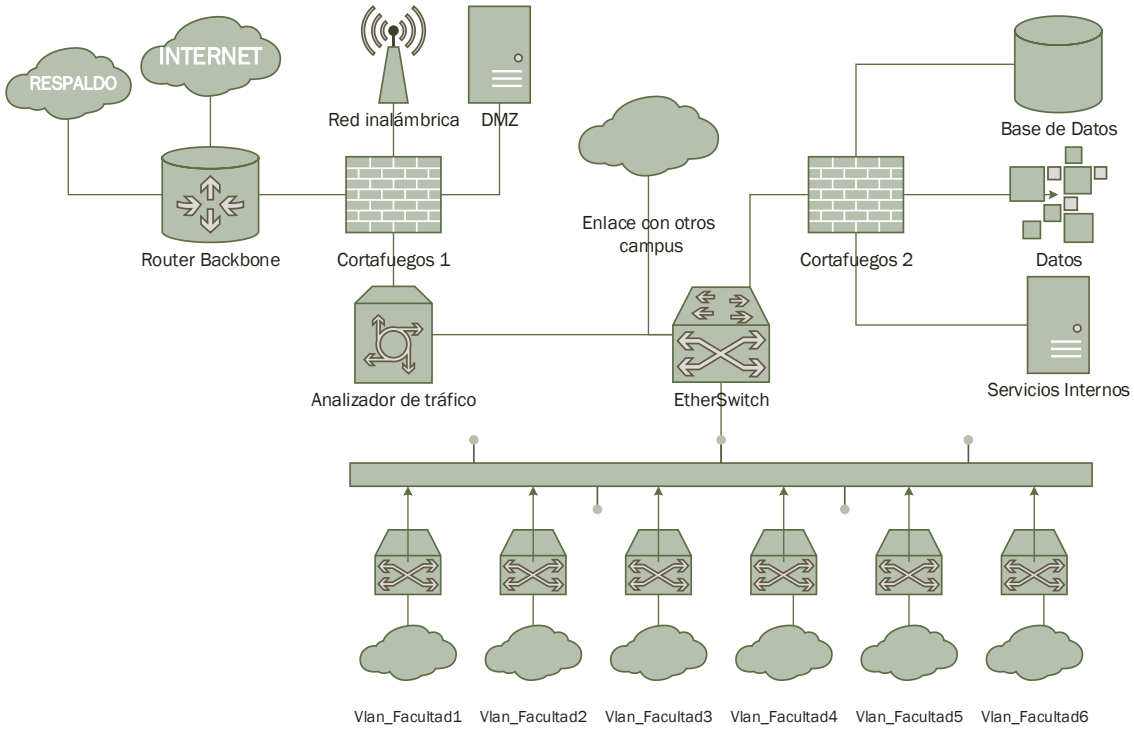



**Figura 10 Topología Lógica**

Control de acceso

Para que los usuarios tengan acceso a los sistemas y servicios deben seguir el reglamento establecido para la asignación de cuentas electrónicas, el cual consiste en asignar un usuario con su respectiva contraseña y un buzón del correo electrónico de la universidad.

La cuenta electrónica es el único medio que permite acceder tanto a los sistemas externos e internos en los cuales se definen roles y permisos para restringir las funcionalidades. El bloqueo de la cuenta se produce cuando se exceden el número de intentos erróneos a los sistemas.

Los usuarios fuera de la red corporativa pueden ingresar a los servicios internos a través de una VPN.

Entrega de Servicios

Respecto a los servicios que se entregan a la comunidad politécnica, entre los principales se encuentran sistemas académicos, financieros y administrativos en plataformas web y de escritorio que han sido desarrollados por personal interno de GTSI utilizando sus computadores de escritorio y además accediendo de forma remota para continuar con el desarrollo de las aplicaciones.

El servicio de correo electrónico es una herramienta fundamental para la comunicación interna que está siendo soportada por la plataforma Office 365 de Microsoft de forma híbrida, en red interna se encuentran los servidores de directorio activo y en la nube se almacenan los buzones de los usuarios.

La virtualización permite optimizar recursos y distribuir el almacenamiento dependiendo de las necesidades de cada servicio.

El almacenamiento y distribución de la información de manera electrónica es un servicio de vital importancia, se administran en bases de datos de desarrollo y producción; por ello se generan respaldos en cinta diaria y semanalmente de las configuraciones y datos prioritarios. Las cintas están siendo almacenadas en una caja fuerte ubicada en otro edificio.

El servicio de internet se entrega de forma alámbrica a todas las oficinas para uso del personal docente y administrativo y de forma inalámbrica para los estudiantes a través de una controladora de red que permite la gestión de los puntos de acceso ubicados en todo el campus Prosperina.

Soporte Técnico

Alrededor de 500 computadores y portátiles son gestionados por el área técnica, encargada de la instalación, configuración, actualización y mantenimiento de las mismas. El personal técnico sigue un procedimiento detallado para la respectiva instalación de los nuevos, considerando los programas utilitarios, antivirus y un software para control de inventario; además mantienen la norma que prohíbe la instalación de software no licenciado.

Operaciones

Las tareas que se llevan a cabo de forma periódica son:

- Semanalmente se da mantenimiento al generador de energía.

- Mensualmente se consideran mantenimientos de limpieza de los servidores de base de datos.
- Generación de nuevas versiones de las aplicaciones desarrolladas incluyendo mejoras o nuevos módulos.
- Actualización diaria de las firmas de antivirus en los servidores Windows.

Incidentes

- Los equipos de climatización se han averiado frecuentemente en los últimos meses.
- Algunos computadores del personal y servidores han sido víctimas de ataques por personas externas.
- Frecuentemente se desconecta el enlace principal con el proveedor de internet.
- La configuración de los equipos de comunicación han sido modificados por personas no autorizadas.
- La rápida adquisición de equipos produjo problemas de compatibilidad afectando la estabilidad de la red.

Actualmente GTSI no cuenta con:

- Política de seguridad
- Procesos definidos para la administración de cuentas
- Procedimiento de respuesta ante incidentes
- Respectiva directiva de copias de seguridad
- Sistema de detección de intrusos
- Control de cuarentena en la VPN
- Personal responsable de la seguridad de la información

## 5.4 Organigrama

El orden organización que se lleva en GTSI es el siguiente. Ver figura 11.

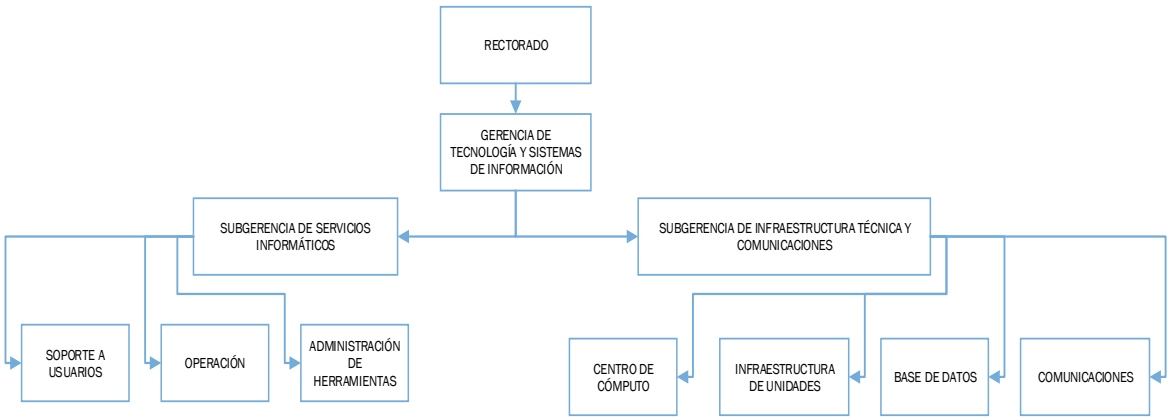



Figura 11 Organigrama de GTSI

## 5.5 Descripción de las Principales Funciones

Se han considerado los cargos que son responsables de cada una de las áreas.

- Gerencia

Encargado de administrar y representar a GTSI, proponer proyectos investigaciones y liderar los procesos de implementación y mejoramiento continuo.

- SubGerencia de Servicios Informáticos

Responsable de todos los procesos del área de sistemas, desde la planificación hasta le entrega y puesta en marcha de los sistemas informáticos.

- SubGerencia de Infraestructura Técnica y Comunicaciones

Responsable de todos los procesos de las áreas técnicas, redes y seguridad de TI.

- Jefe de Infraestructura y Redes

Responsable de la instalación y administración de los servidores físicos y virtuales y servicios de red, equipos de red como switches, routers, access points, puntos de acceso, cortafuegos, entre otros. Además se responsabiliza de la conexión continua e ininterrumpible de la red interna y de internet; así como también de las redes virtuales que conectan a los otros campus.

- Jefe de Sistemas administrativos, financieros y académicos

Responsable de la resolución de problemas, solicitud de acceso, solicitud de instalación o actualización, solicitud de capacitación, solicitud de cambios de los sistemas administrativos, financieros y académicos.

Los desarrolladores son un personal permanente que recibe capacitaciones sobre nuevas técnicas y tecnologías de relacionadas con el desarrollo.

- Responsable de base de datos

Responsable de conceder los permisos de acceso a los usuarios en las aplicaciones dependiendo de las solicitudes realizadas por los responsables de los procesos, y además del mantenimiento, configuración y soporte de las bases de datos.

- Jefe Técnico

Responsable del mantenimiento y configuración de los computadores de escritorio, portátiles y periféricos; instalación de los programas utilitarios. Además es responsable de resolver problemas a la alimentación eléctrica del centro de datos y UPS.

El equipo técnico es rotativo porque lo conforman estudiantes de la universidad que están por culminar sus estudios, por ende a menudo se producen errores de configuración en los equipos del personal administrativo.

# 6 Caso de Estudio – Análisis de Riesgo

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, tanto el impacto potencial como el residual.
5. Evaluar el riesgo del sistema en estudio, tanto el riesgo potencial como el residual.
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.

El análisis mediante la herramienta PILAR se ha realizado para tener una guía referencial respecto al estudio realizado de forma manual, PILAR identifica las amenazas que afectan a los activos de forma directa e indirecta para finalmente obtener gráficas con los resultados.

## 6.1 Modelo de Valor

El modelo de valor está conformado por la identificación de los activos considerados prioritarios en las actividades fundamentales de la organización, relación entre los activos, la valoración; y finalmente los resultados obtenidos reflejan la importancia que incurren cada uno dentro de la organización.

### 6.1.1 Identificación de Activos

Equipamiento - Hardware

- Servidores.- Se consideran todos los equipos físicos de tipo torre y rack que alojan algún programa o aplicación, se encuentran dentro del centro de datos y son administrados por el personal de infraestructura y sistemas.
- Equipos de comunicaciones.- Se consideran todos los equipos que conforman la red de voz y datos ubicados en el centro de datos que son administrados por personal de infraestructura.
- Robot de cintas.- Equipo físico que realiza los respaldos en cinta de la información de los servidores ubicado en el centro de datos y es administrado por el personal de infraestructura.
- Computador de personal.- Equipo de computación que utiliza el personal de GTSI para trabajar.

Equipamiento - Software

- Sistemas académicos, financieros y administrativos.- Se consideran a los sistemas prioritarios para la administración de la organización que son gestionados por los desarrolladores.
- Almacenamiento – bases de datos.- Se considera a la información almacenada y respaldada originada de los datos de los servicios prestados, esto es administrado por administrador de bases de datos. También se consideran a las cintas magnéticas que almacenan la información respaldada.
- Correo electrónico.- se considera al sistema de correo electrónico.
- Virtualización.- se considera al servicio que permite el funcionamiento de los servidores virtuales.

Comunicaciones

- Internet.- Se considera al servicio y demás elementos necesarios para lograr el acceso hacia el Internet.
- Red alámbrica.- se considera a las conexiones alámbricas ya sean de fibra óptica o cable UTP.
- Red inalámbrica.- se considera a la señal de red emitida por los puntos de acceso.
- Enlace con proveedor.- se considera al servicio y equipos que conlleva la comunicación exitosa con el proveedor de Internet.

Equipamiento Auxiliar

- UPS.- se consideran a las baterías que protegen a los servidores y equipos de comunicación de fallos eléctricos.
- Generador eléctrico.- se considera al dispositivo que genera energía eléctrica cuando no hay servicio eléctrico.
- Equipos de climatización.- se consideran a los elementos que mantienen la temperatura adecuada en el centro de datos y cuartos de rack.
- Cableado eléctrico.- se considera a la red eléctrica existente entre el centro de datos, cuarto de rack y cuarto del generador eléctrico.

Instalaciones

- Centro de datos.- es el lugar donde se concentran todos los servidores y equipos de comunicación.
- Cuarto de rack.- o cuarto de telecomunicaciones, están ubicados en los diferentes edificios de la organización y es donde se encuentran los equipos de comunicación que tienen un enlace directo con el centro de datos.

Personal

- Equipo de desarrollo.- se considera al personal encargado de desarrollar las aplicaciones o sistemas.
- Equipo técnico.- se considera al personal encargado de dar asesoría técnica.
- Administradores.- se consideran a los jefes de cada área.

### 6.1.2 Identificación de Activos en PILAR

El primer paso a realizar en la herramienta PILAR es la creación de un nuevo proyecto siguiendo el manual de usuario [21], luego identificar los activos mediante un código y un nombre (ver figura 12) y clasificarlos entre las siguientes categorías:

- Activos esenciales
- Servicios internos
- Equipamiento
- Servicios Subcontratados
- Instalaciones
- Personal

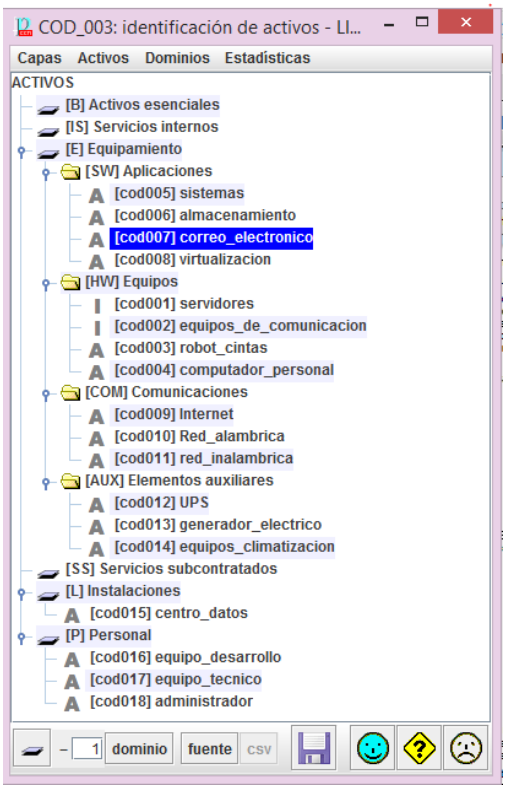



Figura 12 Identificación de activos

### 6.1.3 Árbol de dependencia de activos

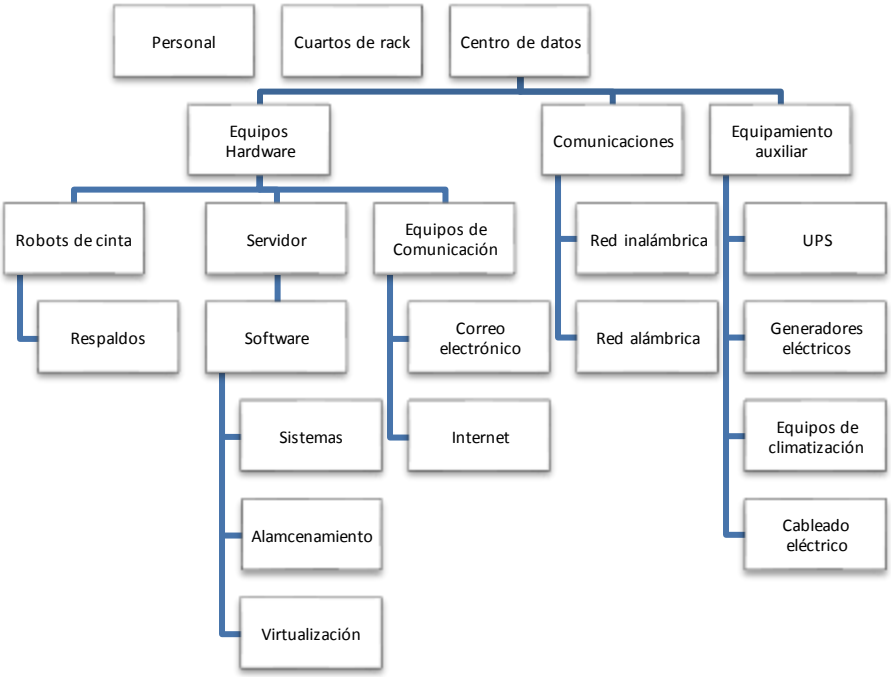



Figura 13 Árbol de dependencia de activos

En el árbol de dependencias de la figura 13 se encuentran desplegados de forma jerárquica los activos de acuerdo al nivel del dependencia que existe entre estos.

En el primer nivel se han considerado al centro de datos, que es el lugar donde se concentran los servidores y equipos de comunicación, 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 de hardware. Además 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.

### 6.1.4 Dependencia de Activos en PILAR

Para definir las dependencias de los activos se ha seguido el diagrama de dependencias detallado en el apartado anterior. En la figura 14 se ha determinado la dependencia existente entre los servidores con el equipamiento auxiliar, personal e instalaciones. El proceso se repite para cada uno de los activos.

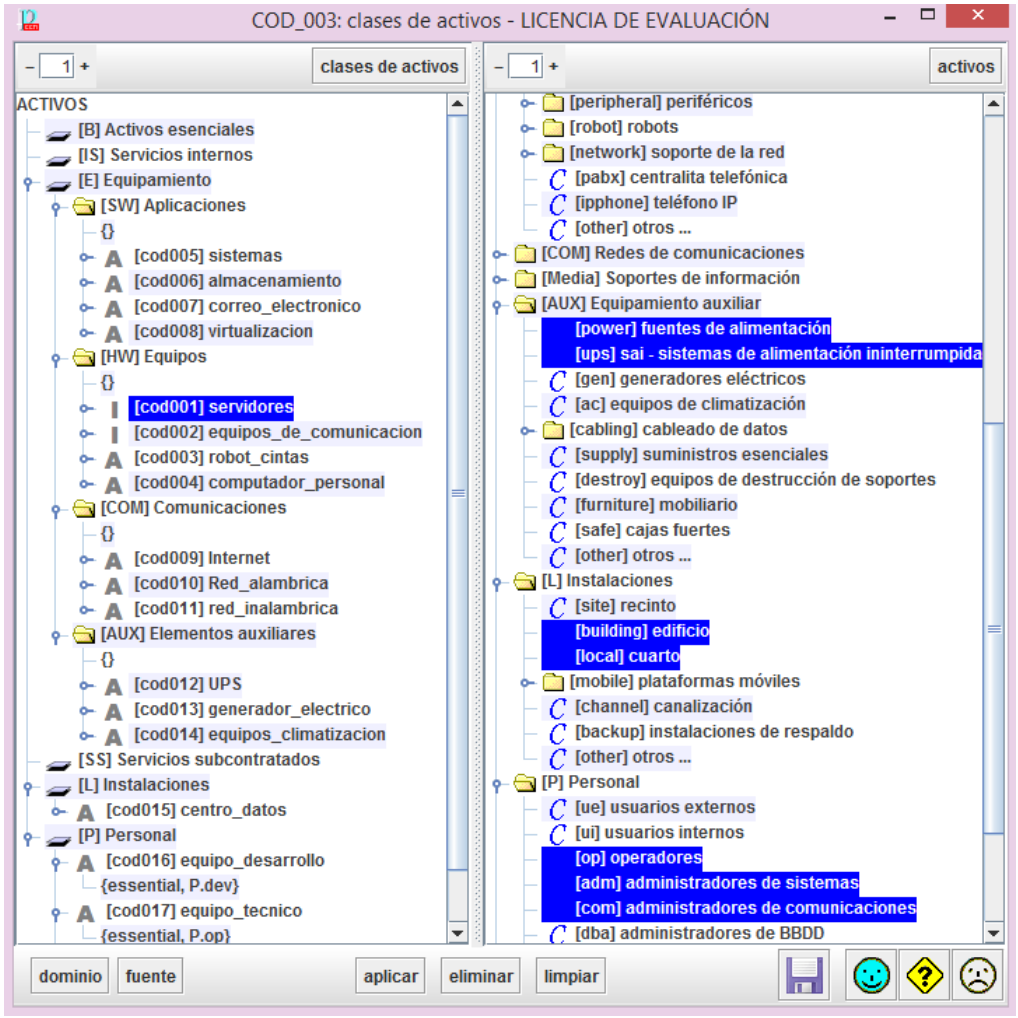



Figura 14 Definiendo la Dependencia entre activos

### 6.1.5 Valoración de Activos

A continuación se realizará la evaluación de los activos en cada uno de los parámetros de seguridad en que se verían afectados al exponerse ante los diversos tipos de amenazas

que causarían la pérdida de información o daños sobre el equipo que la almacena. Ver en las tablas 5 y 6 la valoración realizada bajo la escala de criterios definida en la tabla 7.

**Tabla 5 Valoración de activos (1)**

| | Equipamiento - Hardware | | | | | | | | | | | | Equipamiento - Software | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Servidores | | | Equipos de Comunicaciones | | | Robots de cintas | | | Computador de personal | | | Sistemas académicos, financieros y adm | | | Almacenamiento - Base de Datos | | | Correo electrónico | | | Virtualización | | | Internet | | |
| Amenaza | D | I | C | D | I | C | D | I | C | D | I | C | D | I | C | D | I | C | D | I | C | D | I | C | D | I | C |
| Incendio | 10 | | | 10 | | | 10 | | | 10 | | | 8 | | | 8 | | | 10 | | | 10 | | | 10 | | |
| Terremoto | 10 | | | 10 | | | 10 | | | 10 | | | 8 | | | 8 | | | 10 | | | 10 | | | 10 | | |
| Sobrecarga eléctrica | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Falla de generador eléctrico | 8 | | | 8 | | | 8 | | | 8 | | | 8 | | | 8 | | | 8 | | | 8 | | | 8 | | |
| Falla de equipos de climatización | 6 | | | 6 | | | 6 | | | 6 | | | 6 | | | 6 | | | 6 | | | 6 | | | 6 | | |
| Errores de configuración | | 5 | | | 6 | | | | | | | | | 6 | | | | | | 6 | | | 6 | | | | | |
| Desconexión física o lógica | 8 | | | 8 | | | | | | 2 | | | | | | 9 | | | 8 | | | 8 | | | 10 | | |
| Agotamiento de recursos | 6 | | | | | | | | | | | | | | | 8 | | | | | | | | | | | |
| Spyware | | 8 | | | | | | | | | 5 | | | | | | | | | | | | | | | | |
| Malware | 8 | 8 | | | | | | | | 5 | 5 | | | | | | | | | | | | | | | | |
| Phishing | | | | | | | | | | | | | | | | | | | | | 6 | | | | | | |
| Spam | | | | | | | | | | | | | | | | | | | | | 6 | | | | | | |
| Flooding | | | | 6 | | | | | | | | | | | | | | | | | | | | | | | |
| Acceso no autorizado | | | 9 | | | 9 | | | | | | 8 | | | 8 | | | 9 | | | 9 | | | 8 | | | |
| Robo | 10 | | | 10 | | | 10 | | | 8 | | | | | | | | | | | | | | | | | |
| Fuga de Información | | | | | | | | | | | | | | | | | | | | | | | | | | | |

**Tabla 6 Valoración de activos (2)**

| | Instalaciones | | | | | | Equipamientno auxiliar | | | | | | | | | | | | Personal | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Centro de datos | | | Cuartos de red | | | UPS | | | Generadores eléctricos | | | Equipos de climatización | | | Cableado eléctrico | | | Administradores | | | Equipo técnico | | | Equipo de desarrollo | | |
| Amenaza | D | I | C | D | I | C | D | I | C | D | I | C | D | I | C | D | I | C | D | I | C | D | I | C | D | I | C |
| Incendio | 10 | | | 10 | | | 10 | | | 10 | | | 10 | | | 10 | | | 10 | | | 10 | | | 10 | | |
| Terremoto | 10 | | | 10 | | | 10 | | | 10 | | | 10 | | | 10 | | | 10 | | | 10 | | | 10 | | |
| Sobrecarga eléctrica | 9 | | | 9 | | | 8 | | | 8 | | | 9 | | | 8 | | | | | | | | | | | |
| Falla de generador eléctrico | 8 | | | 8 | | | | | | 10 | | | | | | | | | | | | | | | | | |
| Falla de equipos de climatización | 8 | | | 8 | | | | | | | | | 10 | | | | | | | | | | | | | | |
| Errores de configuración | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Desconexión física o lógica | 10 | | | 10 | | | | | | | | | | | | 10 | | | | | | | | | | | |
| Agotamiento de recursos | 5 | | | 5 | | | | | | | | | | | | | | | | | | | | | | | |
| Spyware | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Malware | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Phishing | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Spam | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Flooding | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Acceso no autorizado | 8 | | | 8 | | | | | | | | | | | | | | | | 10 | 10 | | 10 | 10 | | 10 | 10 |
| Robo | | | | | | | 10 | | | 10 | | | 10 | | | 5 | | | | | | | | | | | |
| Fuga de Información | | | | | | | | | | | | | | | | | | | | 10 | 10 | | 10 | 10 | | 10 | 10 |

**Tabla 7 Escala de criterios**

| 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 |

En la gráfica de la figura 15 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 13; de esta forma sobresalen a simple vista los activos, tales como: las instalaciones, equipamiento auxiliar y entre los principales servicios ofrecidos están internet, almacenamiento de información, entre otros.

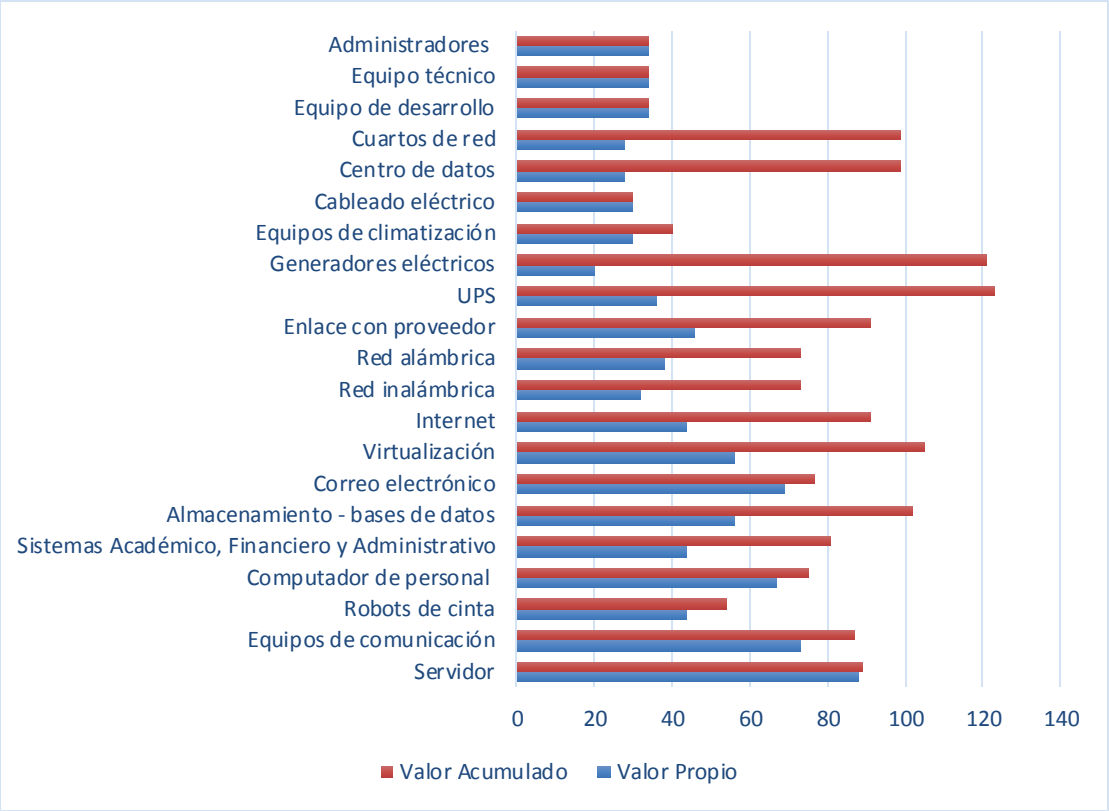



Figura 15 Valor Propio y Acumulado de Activos

PILAR permite valorar los activos en base a tres niveles: alto, medio y bajo; en la figura 16 se presenta la evaluación de activos en cada uno de los parámetros de seguridad.

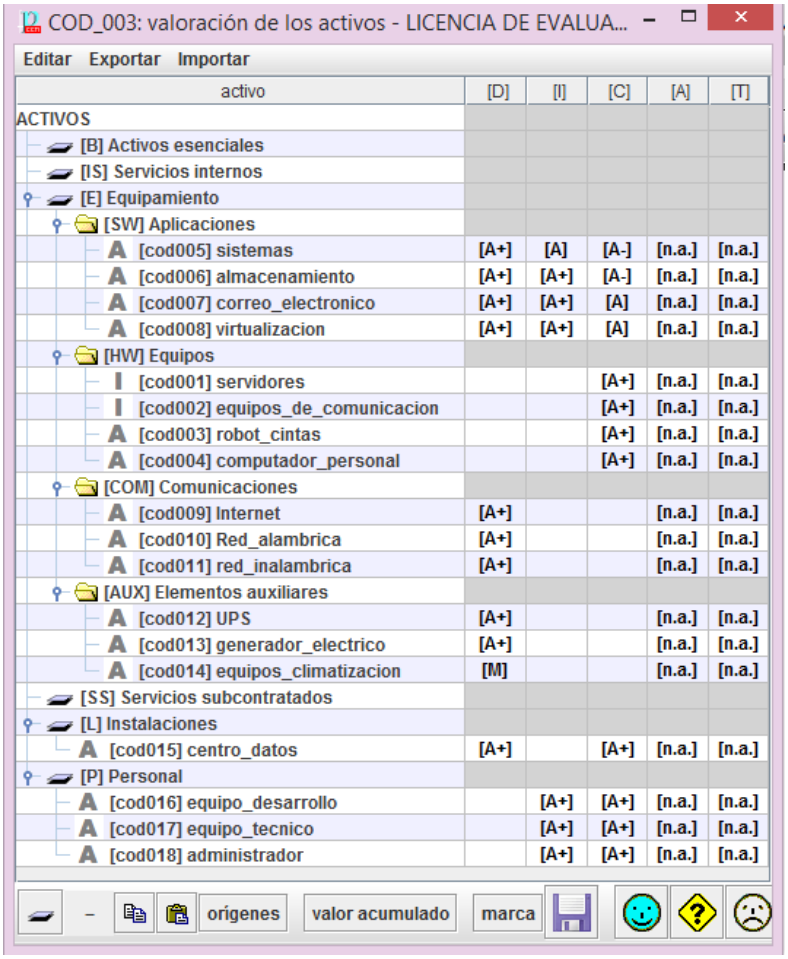



Figura 16 Valoración de los activos

## 6.2 Mapa de Riesgos

De la valoración de los activos realizada se han considerado las amenazas que producen más daños, para evaluar el nivel de degradación, frecuencia y el riesgo implicado.

### 6.2.1 Valoración de Amenazas por Activos

Tabla 8 Valoración de amenazas por activos

| Tipos de Activos | Activos | Amenazas Relevantes | Degradación | Frecuencia | Riesgo |
|---|---|---|---|---|---|
| Equipamiento - Hardware | Servidores | Incendio | MA | MB | Medio |
| | | Terremoto | MA | MB | Medio |
| | | Robo | A | B | Medio |
| | | Acceso no autorizado | A | M | Alto |
| | | Falla de generador eléctrico | A | B | Medio |
| | Equipos de comunicaciones | Incendio | MA | MB | Medio |
| | | Terremoto | MA | MB | Medio |
| | | Robo | A | B | Medio |

| | | | | | |
|---|---|---|---|---|---|
| | | Acceso no autorizado | M | B | Alto |
| | | Desconexión Física o lógica | MA | A | Alto |
| | | Falla de generador eléctrico | A | MB | Medio |
| | Robot de cintas | Incendio | MA | MB | Medio |
| | | Terremoto | MA | MB | Medio |
| | | Robo | A | B | Medio |
| | Computador de personal | Incendio | MA | MB | Medio |
| | | Terremoto | MA | MB | Medio |
| | | Robo | MA | B | Medio |
| | | Malware | M | A | Alto |
| Equipamiento - Software | Sistemas académicos, financieros y administrativos | Incendio | MA | MB | Medio |
| | | Terremoto | MA | MB | Medio |
| | | Acceso no autorizado | M | A | Alto |
| | Almacenamiento – bases de datos | Acceso no autorizado | M | M | Medio |
| | | Desconexión física lógica | MA | B | Medio |
| | | Agotamiento de recursos | MA | M | Alto |
| | Correo electrónico | Incendio | MA | MB | Medio |
| | | Terremoto | MA | MB | Medio |
| | | Acceso no autorizado | A | A | Alto |
| | | Desconexión física o lógica | MA | M | Alto |
| | Virtualización | Incendio | MA | MB | Medio |
| | | Terremoto | MA | MB | Medio |
| | | Acceso no autorizado | MA | A | Alto |
| | | Desconexión física o lógica | MA | M | Alto |
| | Internet | Incendio | MA | MB | Medio |
| | | Terremoto | MA | MB | Medio |
| | | Desconexión física o lógica | MA | MA | Alto |
| Comunicaciones | Red alámbrica | Incendio | MA | MB | Medio |
| | | Terremoto | MA | MB | Medio |
| | Red inalámbrica | Incendio | MA | MB | Medio |
| | | Terremoto | MA | MB | Medio |
| | Enlace con proveedor | Incendio | MA | MB | Medio |
| | | Terremoto | MA | MB | Medio |
| | | Desconexión física o lógica | MA | A | Alto |
| Equipamiento Auxiliar | UPS | Incendio | MA | MB | Medio |
| | | Terremoto | MA | MB | Medio |
| | | Falla de equipos de climatización | A | MA | Alto |
| | Generador eléctrico | Incendio | MA | MB | Medio |

| | | | | | |
|---|---|---|---|---|---|
| | | Terremoto | MA | MB | Medio |
| | Equipos de climatización | Incendio | MA | MB | Medio |
| | | Terremoto | MA | MB | Medio |
| | | Falla de equipos de climatización | MA | MA | Alto |
| | Cableado eléctrico | Incendio | MA | MB | Medio |
| | | Terremoto | MA | MB | Medio |
| | | Desconexión física o lógica | MA | B | Medio |
| Instalaciones | Centro de datos | Incendio | MA | MB | Medio |
| | | Terremoto | MA | MB | Medio |
| | | Acceso no autorizado | MA | B | Medio |
| | Cuarto de rack | Incendio | MA | MB | Medio |
| | | Terremoto | MA | MB | Medio |
| | | Acceso no autorizado | MA | B | Medio |
| Personal | Equipo de desarrollo | Incendio | MA | MB | Medio |
| | | Terremoto | MA | MB | Medio |
| | | Fuga de información | A | M | Medio |
| | Equipo técnico | Incendio | MA | MB | Medio |
| | | Terremoto | MA | MB | Medio |
| | | Fuga de información | A | A | Alto |
| | Administradores | Incendio | MA | MB | Medio |
| | | Terremoto | MA | MB | Medio |
| | | Fuga de información | A | A | Alto |

### 6.2.2 Valoración de Activos por Amenaza

**Tabla 9 Valoración de activos por amenaza**

| Tipo de Amenaza | Amenaza | Activo | Degradación | Frecuencia | Riesgo |
|---|---|---|---|---|---|
| Naturales y de Entorno | Incendio y Terremoto | Servidores | MA | MB | Medio |
| | | Equipos de Comunicaciones | MA | MB | Medio |
| | | Robot de cintas | MA | MB | Medio |
| | | Computador de personal | MA | MB | Medio |
| | | Sistemas académicos, financieros y administrativos | MA | MB | Medio |
| | | Almacenamiento – bases de datos | MA | MB | Medio |
| | | Correo electrónico | MA | MB | Medio |
| | | Virtualización | MA | MB | Medio |
| | | Internet | MA | MB | Medio |
| | | Red alámbrica | MA | MB | Medio |
| | | Red alámbrica | MA | MB | Medio |
| | | Enlace con proveedor | MA | MB | Medio |
| | | UPS | MA | MB | Medio |

| | | | | | |
|---|---|---|---|---|---|
| | | Generador eléctrico | MA | MB | Medio |
| | | Equipos de climatización | MA | MB | Medio |
| | | Cableado eléctrico | MA | MB | Medio |
| | | Centro de datos | MA | MB | Medio |
| | | Cuarto de rack | MA | MB | Medio |
| | | Equipo de desarrollo | MA | MB | Medio |
| | | Equipo técnico | MA | MB | Medio |
| | | Administradores | MA | MB | Medio |
| Ataque no deliberado | Falla de generador eléctrico | Servidores | A | B | Medio |
| | | Equipos de comunicaciones | A | B | Medio |
| | Agotamiento de recursos | Almacenamiento – bases de datos | MA | M | Medio |
| | Falla de equipos de climatización | UPS | A | MA | Alto |
| | | Equipos de climatización | MA | MA | Alto |
| Ataque deliberado | Acceso no autorizado | Servidores | A | M | Alto |
| | | Equipos de comunicaciones | M | B | Alto |
| | | Sistemas académicos, financieros y administrativos | M | A | Alto |
| | | Almacenamiento – bases de datos | MA | M | Medio |
| | | Correo electrónico | A | A | Alto |
| | | Virtualización | MA | A | Alto |
| | | Centro de datos | MA | B | Medio |
| | | Cuarto de rack | MA | B | Medio |
| | Robo | Servidores | A | B | Medio |
| | | Equipos de comunicaciones | A | B | Medio |
| | | Robot de cintas | MA | B | Medio |
| | | Computador de personal | MA | B | Medio |
| | Desconexión Física o lógica | Equipos de comunicaciones | M | A | Alto |
| | | Almacenamiento – bases de datos | MA | B | Medio |
| | | Correo electrónico | MA | M | Alto |
| | | Virtualización | MA | M | Alto |
| | | Internet | MA | MA | Alto |
| | | Enlace con proveedor | MA | A | Alto |
| | | Cableado eléctrico | MA | B | Medio |
| | Fuga de información | Equipo de desarrollo | A | B | Medio |
| | | Equipo técnico | A | A | Alto |
| | | Administradores | A | A | Alto |
| | Malware | Computador de personal | M | A | Alto |

Los resultados obtenidos tras la evaluación del nivel de degradación y frecuencia en que podrían materializarse las amenazas sobre los activos, demuestran que los niveles de riesgos presentes son medio y alto. Las amenazas con un nivel alto de riesgo son:

- Acceso no autorizado.- Afecta de forma directa a la integridad y confidencialidad de la información, debido a varios factores: las contraseñas de las cuentas con privilegios no se cambian de forma periódica, algunas no cumplen los requisitos de una contraseña compleja, no existe un directiva de control del acceso remoto, aún siguen activas las cuentas de ex empleados y tampoco se comprueba de forma periódica la configuración de los cortafuegos.
- Desconexión física o lógica.- Afecta a la disponibilidad de la información y es debido a que de forma continua se presentan caídas en el enlace con el proveedor de internet, lo cual provoca problemas en los demás servicios dependientes del internet. Referente a la desconexión física, existe esta amenaza al no tener armarios con puertas en el centro de datos ni en los cuartos de red, y por esto las conexiones de los equipos de comunicación y servidores se encuentran expuestas.
- Fuga de información.- Afecta a la confidencialidad de la información al no existir un proceso formal de salida de empleados, ni una política sobre el almacenamiento de información institucional en los computadores personales.
- Malware.- Afecta la integridad de la información almacenada en los servidores y equipos del personal que no cuentan con un software antimalware.
- Fallas de equipos de climatización.- Afecta la disponibilidad de la información que es procesada en los centros de datos y cuartos de rack, cuando se presentan problemas con los equipos de climatización, porque han superado el ciclo de servicio y requieren ser renovados.

En PILAR es posible identificar las amenazas que pueden influir sobre un activo, en la figura 17 se presenta las amenazas que afectan a los servidores.


Figura 17 Identificación de amenazas – Servidores

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 figura 18 se aprecian los resultados obtenidos en la valoración de las amenazas que afectan a los servidores.

| activo | frecuencia | [D] | [I] | [C] |
|---|---|---|---|---|
| ACTIVOS | | | | |
| [B] Activos esenciales | | | | |
| [IS] Servicios internos | | | | |
| [E] Equipamiento | | | | |
| [SW] Aplicaciones | | | | |
| [HW] Equipos | | | | |
| [cod001] servidores | | 100% | 50% | 100% |
| [N.1] Fuego | 1 | 100% | | |
| [N.2] Daños por agua | 1 | 100% | | |
| [N.*] Desastres naturales | 0,5 | 100% | | |
| [I.1] Fuego | 1 | 100% | | |
| [I.2] Daños por agua | 1 | 100% | | |
| [I.*] Desastres industriales | 1 | 100% | | |
| [I.3] Contaminación medioambiental | 1 | 10% | | |
| [I.4] Contaminación electromagnética | 0,1 | 10% | | |
| [I.5] Avería de origen físico o lógico | 1 | 50% | | |
| [I.6] Corte del suministro eléctrico | 1 | 100% | | |
| [I.7] Condiciones inadecuadas de temperatura o humedad | 1 | 100% | | |
| [I.11] Emanaciones electromagnéticas | 0,1 | | | 1% |
| [E.2] Errores del administrador del sistema / de la seguridad | 1 | 20% | 20% | 20% |
| [E.15] Alteración de la información | 1 | | 10% | |
| [E.18] Destrucción de la información | 1 | 1% | | |
| [E.19] Fugas de información | 1 | | | 10% |
| [E.23] Errores de mantenimiento / actualización de equipos (hardwa | 1 | 1% | | |
| [E.24] Caída del sistema por agotamiento de recursos | 10 | 50% | | |
| [E.25] Pérdida de equipos | 0,1 | 100% | | 100% |
| [E.28] Indisponibilidad del personal | 1 | 10% | | |
| [A.5] Suplantación de la identidad | 1 | | 10% | 50% |
| [A.6] Abuso de privilegios de acceso | 1 | 10% | 10% | 50% |

Figura 18 Valoración de amenazas - Servidores

## 6.3 Evaluación de Salvaguardas

Las salvaguardas planteadas han sido elegidas siguiendo los consejos de implantación del estándar ISO/IEC 27001 y el modelo de seguridad por capas de la figura 19, este diagrama descriptivo ayuda a reconocer las necesidades o falencias en el ámbito de la seguridad de datos ya que se tienen varios niveles de defensa. Es importante mencionar que cada acción de protección tiene un costo, por lo que en cada caso se debe evaluar 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. [22]

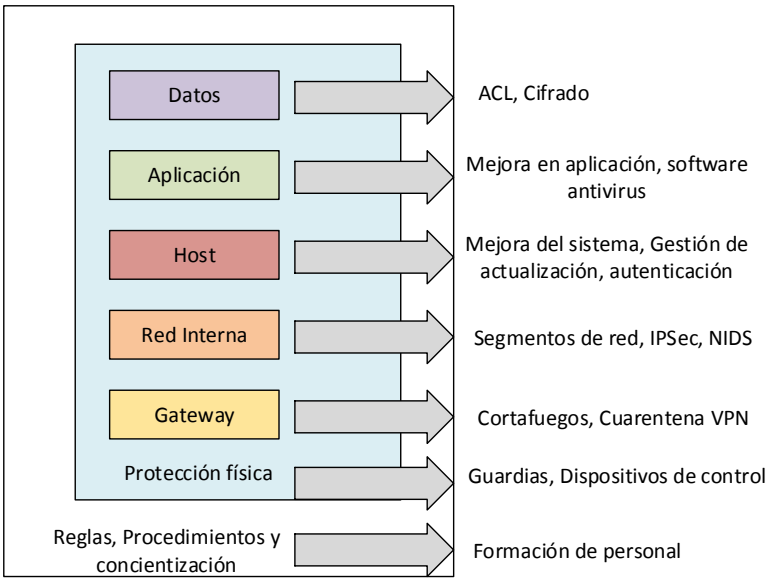



Figura 19 Modelo de seguridad por capas

Tabla 10 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 del 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 |

En la tabla 8 se tienen las salvaguardas que indican el nivel de madurez de la seguridad. 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 los niveles L1 y L2 se consideran a los procedimientos existentes pero aún falta mejorar su gestión, como son los referentes a la seguridad física, dentro del plan de emergencia ante incendios es necesario asignar los responsables y definir los procedimientos necesarios para llevar a cabo la restauración de la información respaldada; referente a los equipos de climatización, sería ideal la renovación de los equipos o mejorar los mantenimientos; realizar la instalación de los armarios con puerta en el centro de datos y también en los cuartos de rack para mayor seguridad de los equipos.

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.

Las salvaguardas con nivel L3 y L4 son aquellas que están siendo implementadas de forma correcta y que podrían optimizarse para mejorar la seguridad física y lógica. Los niveles de salvaguardas objetivo son nivel L4 y L5 dependiendo del caso, siempre tratando de aplicar y optimizar los procedimientos de protección.

Se puede ver reflejado en los resultados obtenidos que existe un desequilibrio en cuanto a las protecciones físicas y lógicas; las protecciones físicas se han estado implementando de forma correcta y tan solo requieren ser optimizados; en cambio en la

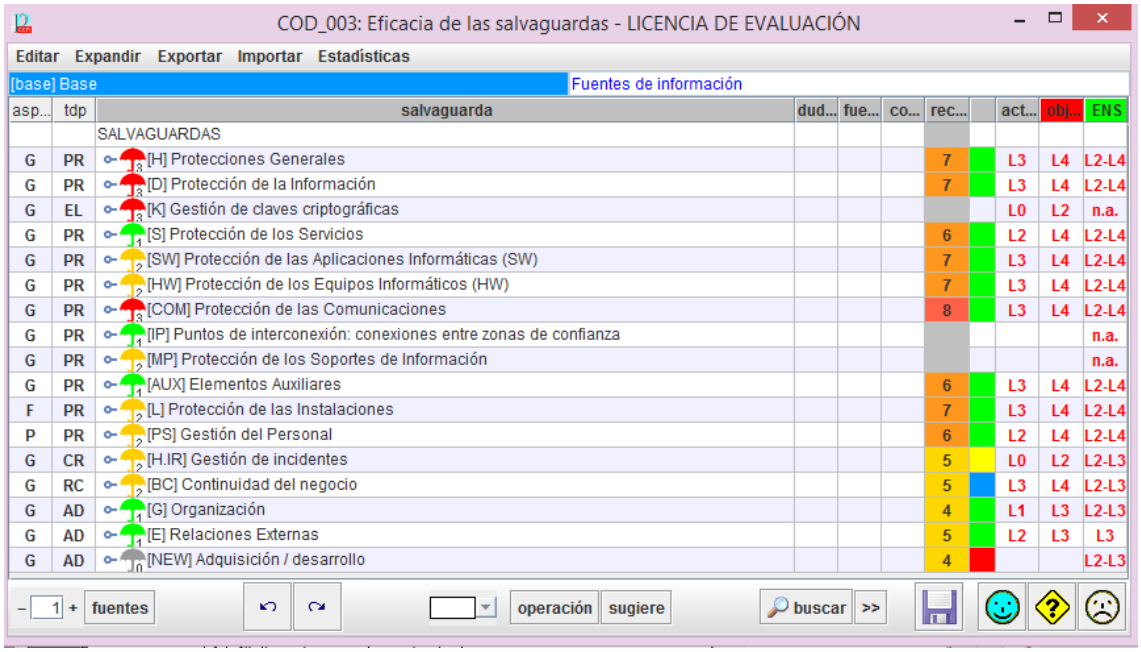
protección lógica, referente a la definición de procedimientos y directivas aún requieren ser analizadas, desarrolladas y gestionadas.

### 6.3.1 Evaluación de Salvaguardas PILAR

Las salvaguardas en PILAR se tratan bajo 4 aspectos:

- G – Gestión
- T – Técnico
- F – Seguridad física
- P – Gestión de personal

La columna "recomendación" indica la valoración estimada de la salvaguarda teniendo en cuenta el tipo de activos, el rango va desde el 0 al 10. En las siguientes columnas se ingresan los niveles de las salvaguardas actuales, objetivo y por último el nivel que PILAR recomienda.




| asp... | tdp | salvaguarda | dud... | fue... | co... | rec... | | act... | obj... | ENS |
|---|---|---|---|---|---|---|---|---|---|---|
| | | SALVAGUARDAS | | | | | | | | |
| G | PR | [H] Protecciones Generales | | | | 7 | | L3 | L4 | L2-L4 |
| G | PR | [D] Protección de la Información | | | | 7 | | L3 | L4 | L2-L4 |
| G | EL | [K] Gestión de claves criptográficas | | | | | | L0 | L2 | n.a. |
| G | PR | [S] Protección de los Servicios | | | | 6 | | L2 | L4 | L2-L4 |
| G | PR | [SW] Protección de las Aplicaciones Informáticas (SW) | | | | 7 | | L3 | L4 | L2-L4 |
| G | PR | [HW] Protección de los Equipos Informáticos (HW) | | | | 7 | | L3 | L4 | L2-L4 |
| G | PR | [COM] Protección de las Comunicaciones | | | | 8 | | L3 | L4 | L2-L4 |
| G | PR | [IP] Puntos de interconexión: conexiones entre zonas de confianza | | | | | | | | n.a. |
| G | PR | [MP] Protección de los Soportes de Información | | | | | | | | n.a. |
| G | PR | [AUX] Elementos Auxiliares | | | | 6 | | L3 | L4 | L2-L4 |
| F | PR | [L] Protección de las Instalaciones | | | | 7 | | L3 | L4 | L2-L4 |
| P | PR | [PS] Gestión del Personal | | | | 6 | | L2 | L4 | L2-L4 |
| G | CR | [H.IR] Gestión de incidentes | | | | 5 | | L0 | L2 | L2-L3 |
| G | RC | [BC] Continuidad del negocio | | | | 5 | | L3 | L4 | L2-L3 |
| G | AD | [G] Organización | | | | 4 | | L1 | L3 | L2-L3 |
| G | AD | [E] Relaciones Externas | | | | 5 | | L2 | L3 | L3 |
| G | AD | [NEW] Adquisición / desarrollo | | | | 4 | | | | L2-L3 |

Figura 20 Identificación de salvaguardas

Como se puede visualizar en la figura 21, el nivel de salvaguardas actuales está entre 2 y 3 lo cual 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.

## 6.4 Estado de Riesgo

**Tabla 11 Evaluación de impacto y riesgo**

| 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 |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | Desconexión física o lógica | 9 | 6 | 3 | 6 | 6 | 2 |
| Red alámbrica | Incendio | 10 | 7 | 5 | 4 | 4 | 2 |
| | Terremoto | 10 | 7 | 5 | 4 | 4 | 2 |
| Red alámbrica | Incendio | 10 | 7 | 5 | 4 | 4 | 2 |
| | Terremoto | 10 | 7 | 5 | 4 | 4 | 2 |
| Enlace con proveedor | Incendio | 10 | 7 | 5 | 4 | 4 | 2 |
| | Terremoto | 10 | 7 | 5 | 4 | 4 | 2 |
| | Desconexión física o lógica | 9 | 6 | 3 | 6 | 4 | 2 |
| UPS | Incendio | 10 | 7 | 5 | 4 | 4 | 2 |
| | Terremoto | 10 | 7 | 5 | 4 | 4 | 2 |
| | Falla de equipos de climatización | 9 | 7 | 3 | 8 | 8 | 4 |
| Generador eléctrico | Incendio | 10 | 7 | 5 | 4 | 4 | 2 |
| | Terremoto | 10 | 7 | 5 | 4 | 4 | 2 |
| Equipos de climatización | Incendio | 10 | 7 | 5 | 4 | 4 | 2 |
| | Terremoto | 10 | 7 | 5 | 4 | 4 | 2 |
| | Falla de equipos de climatización | 9 | 7 | 3 | 8 | 8 | 4 |
| Cableado eléctrico | Incendio | 10 | 7 | 5 | 4 | 4 | 2 |
| | Terremoto | 10 | 7 | 5 | 4 | 4 | 2 |
| | Desconexión física o lógica | 9 | 6 | 3 | 6 | 6 | 2 |
| Centro de datos | Incendio | 10 | 7 | 5 | 4 | 4 | 2 |
| | Terremoto | 10 | 7 | 5 | 4 | 4 | 2 |
| | Acceso no autorizado | 9 | 6 | 3 | 6 | 4 | 2 |
| Cuarto de rack | Incendio | 10 | 7 | 5 | 4 | 4 | 2 |
| | Terremoto | 10 | 7 | 5 | 4 | 4 | 2 |
| | Acceso no autorizado | 9 | 6 | 3 | 6 | 4 | 2 |
| Equipo de desarrollo | Incendio | 10 | 7 | 5 | 4 | 4 | 2 |
| | Terremoto | 10 | 7 | 5 | 4 | 4 | 2 |
| | Fuga de información | 9 | 6 | 3 | 7 | 5 | 3 |
| Equipo técnico | Incendio | 10 | 7 | 5 | 4 | 4 | 2 |
| | Terremoto | 10 | 7 | 5 | 4 | 4 | 2 |
| | Fuga de información | 9 | 6 | 3 | 7 | 5 | 3 |
| Administradores | Incendio | 10 | 7 | 5 | 4 | 4 | 2 |
| | Terremoto | 10 | 7 | 5 | 4 | 4 | 2 |
| | Fuga de información | 9 | 6 | 3 | 7 | 5 | 3 |

En la tabla 9 se han evaluado el impacto y riesgo de cada amenaza que afecta a los activos. En la evaluación del impacto potencial, actual y el objetivo se han valorado las salvaguardas actuales antes de ser implementadas, el estado actual y el nivel que se

lograría al implementar las nuevas salvaguardas; obteniéndose bajos niveles de impacto considerado como residual, el cual debería ser parte de un nuevo análisis de riesgo.

Mientras la evaluación del riesgo potencial, actual y objetivo se ha considerado el impacto y la probabilidad de que pueda materializarse; también obteniéndose un riesgo residual que debería ser analizado para un nuevo estudio.

### 6.4.1 Impacto Acumulado

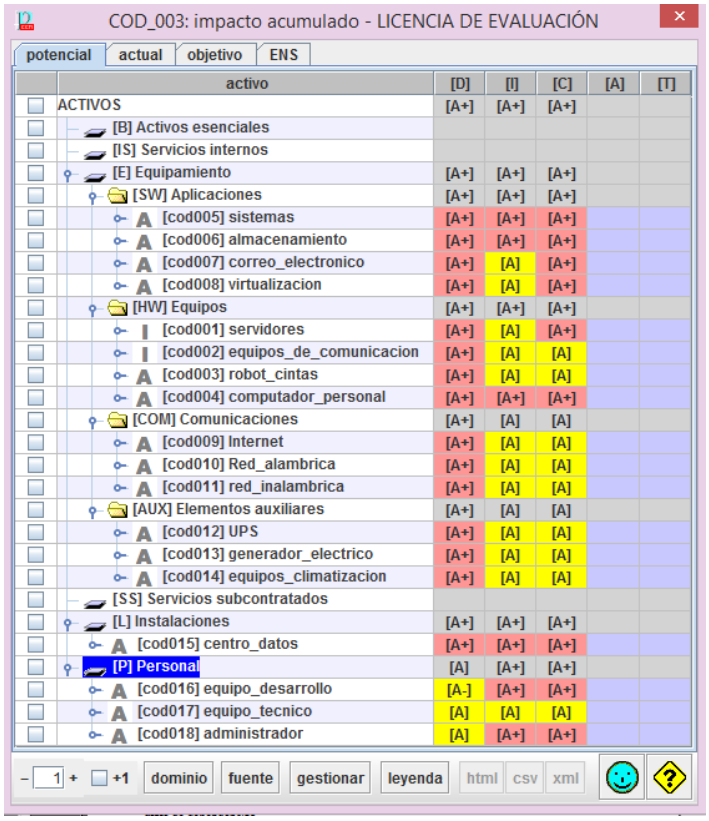



Figura 21 Impacto Acumulado Potencial

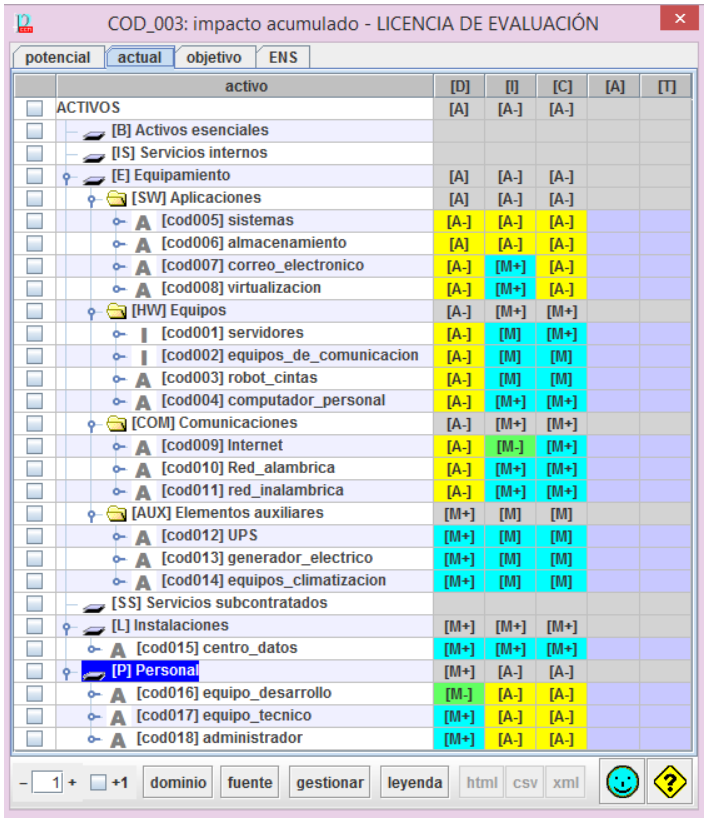



Figura 22 Impacto Acumulado Actual

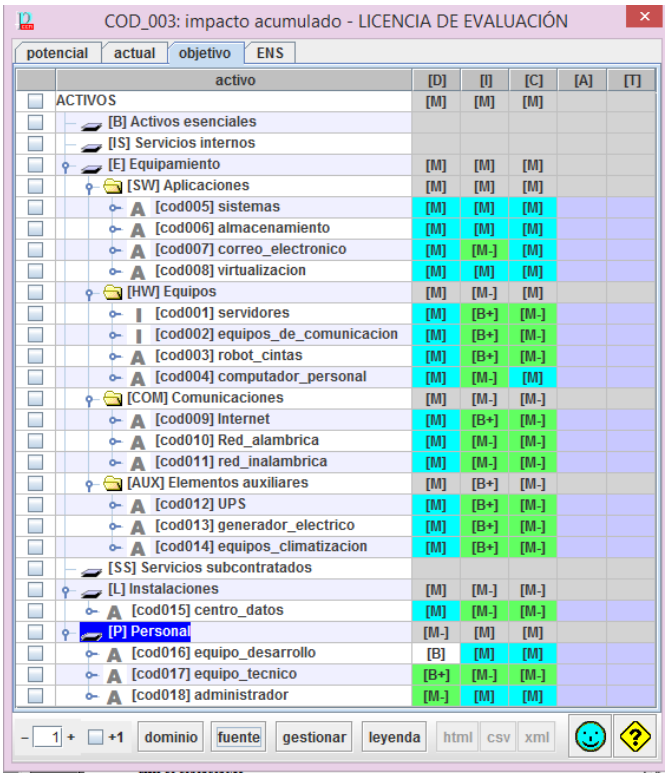



Figura 23 Impacto Acumulado Objetivo

En las figuras 21 y 22 se puede contrastar la importancia de aplicar salvaguardas para disminuir los niveles del impacto, actualmente están en nivel medio, y el nivel objetivo es llegar a obtener un bajo impacto, ver la figura 23.

### 6.4.2 Riesgo Acumulado

PILAR permite medir los niveles de criticidad de los riesgos a los cuales se encuentran expuestos lo activos. Como se visualiza en la figura 24, el parámetro que se encuentra más expuesto es la disponibilidad en el caso que no existiesen salvaguardas. En la figura 25 refleja el nivel del riesgo actual, el cual es medio al igual que los resultados realizados manualmente y en la figura 26 se obtiene el riesgo acumulado objetivo que debe seguir en evaluación para tratar de disminuirlo o si es posible eliminarlo.

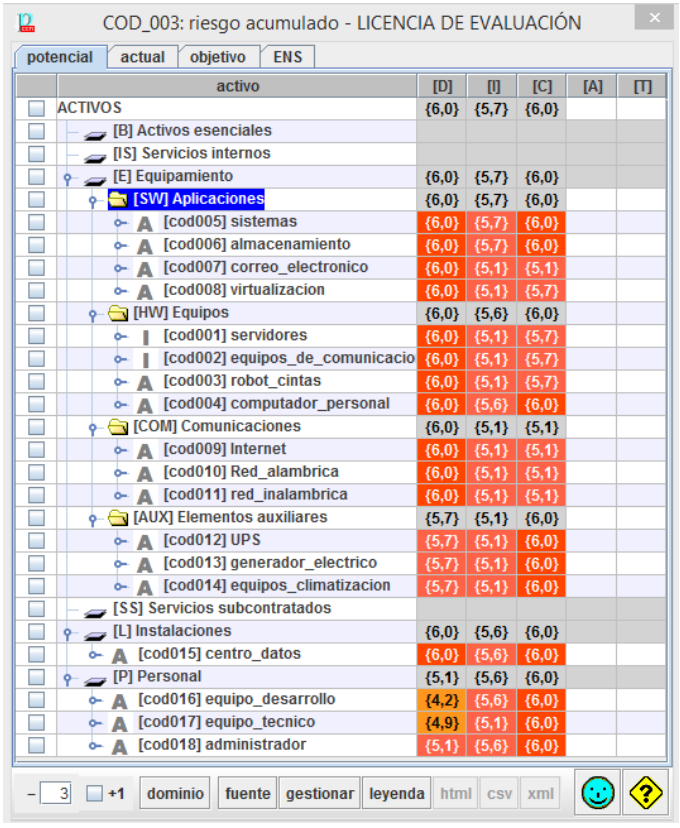



Figura 24 Riesgo Acumulado Potencial

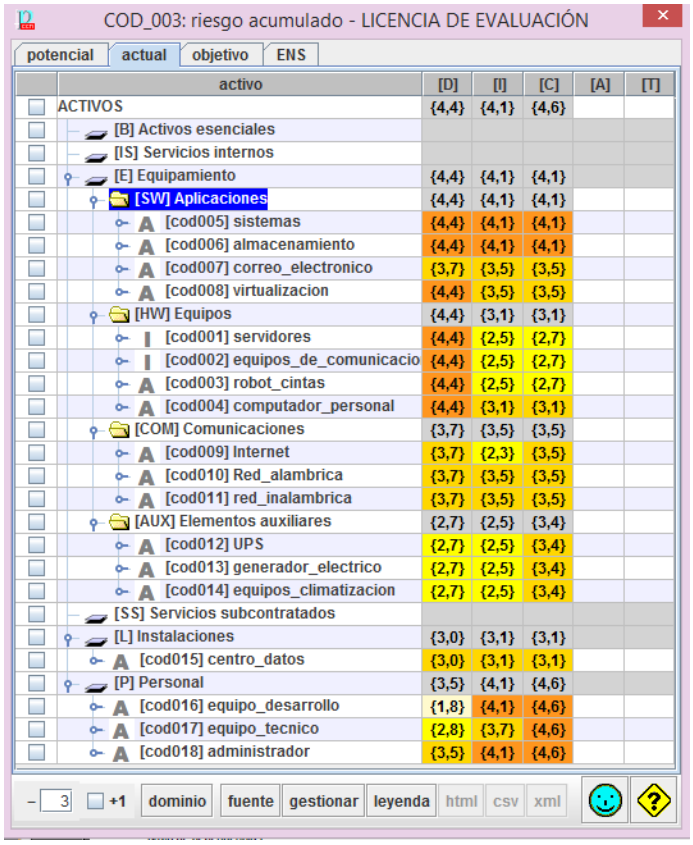



Figura 25 Riesgo Acumulado Actual

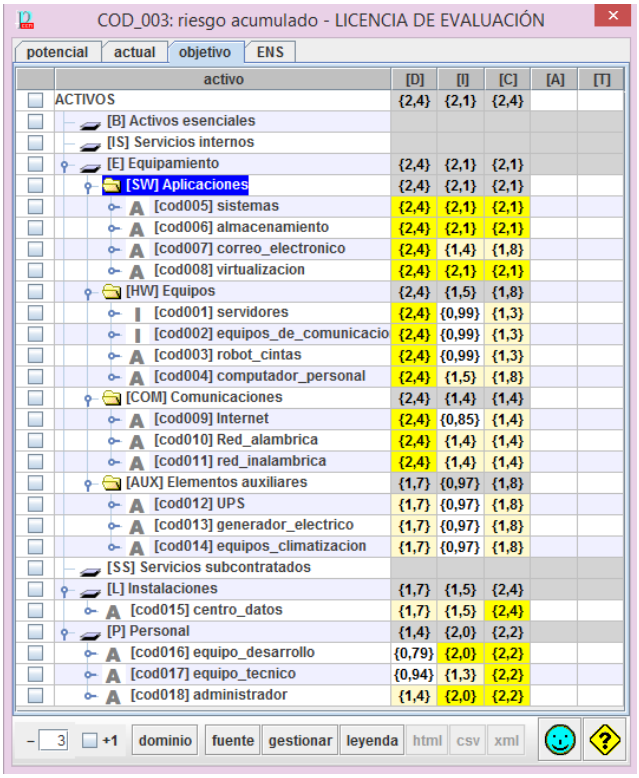



Figura 26 Riesgo Acumulado Objetivo

### 6.4.3 Informes

Se han obtenido los gráficos resultantes de las evaluaciones realizadas. La figura 28 presenta los parámetros de seguridad que se afectan en cada activo, prevaleciendo la confiabilidad en la mayoría de activos.

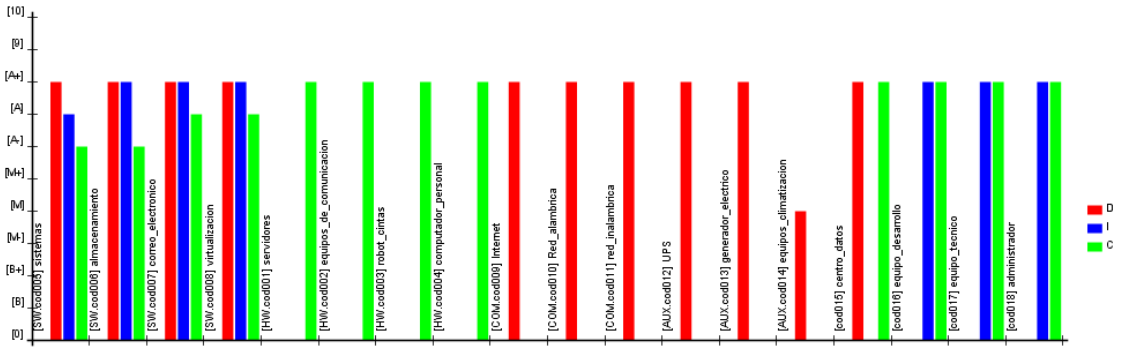



Figura 27 Valor de Activo

En las figuras 29 y 30 se reflejan los valores del impacto y riesgos acumulados sobre cada uno de los activos definidos en las gráficas radiales, en el cual se consideran la implementación de las salvaguardas antes planteadas que permiten que estos valores disminuyan los parámetros de vulnerabilidad de los activos hasta el nivel objetivo.

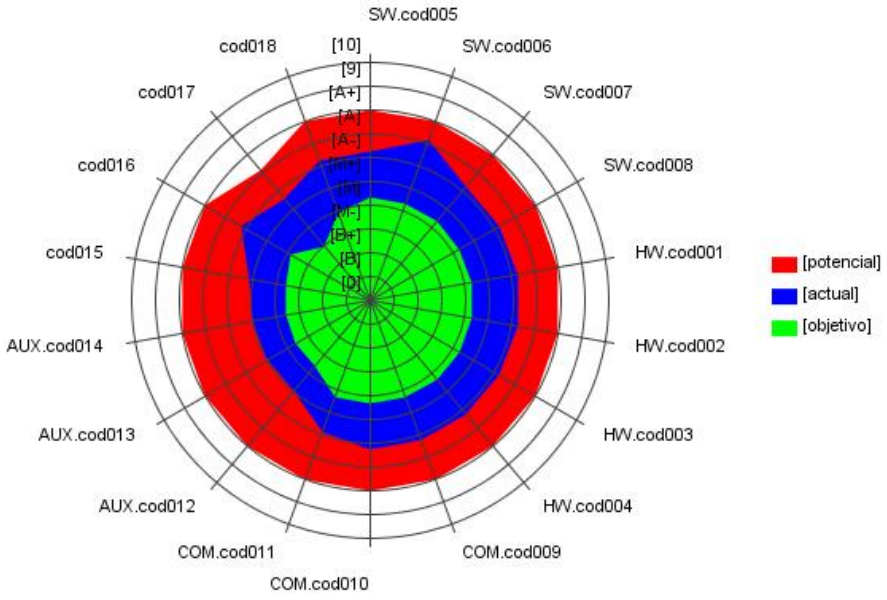



Figura 28 Impacto Acumulado

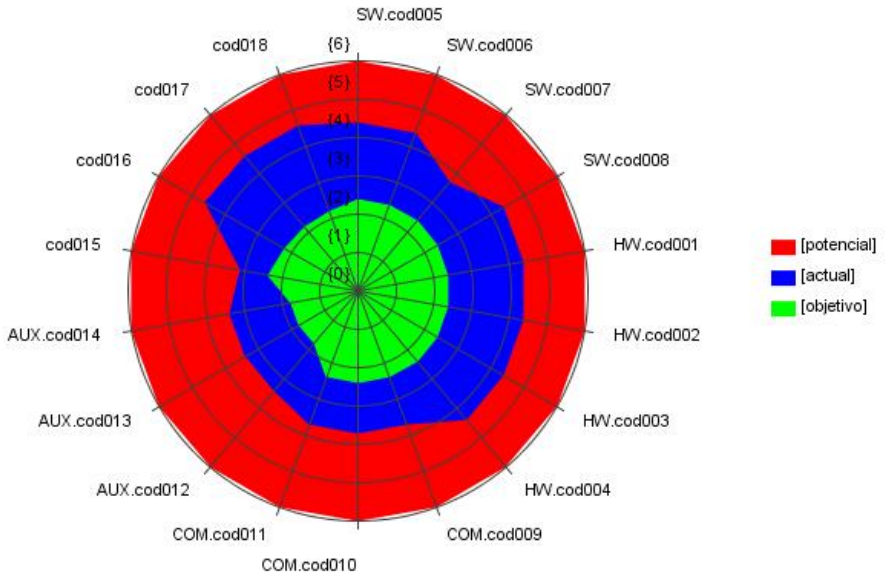



Figura 29 Riesgo Acumulado

## 6.5 Plan de Seguridad

En esta etapa final es necesario informar al personal de las áreas implicadas sobre los activos evaluados con sus respectivas amenazas y salvaguardas factibles.

En el presente análisis de riesgos se han considerado los activos que forman parte de los principales servicios que brinda GTSI a la comunidad politécnica, entre los cuales están: acceso a los sistemas para fines académicos, financieros y administrativos, proveer el acceso a la intranet e internet de forma alámbrica e inalámbrica y almacenar de forma segura la información que se genera diariamente.

Las amenazas presentes que requieren eliminarse o reducirse de forma urgente son las referentes al acceso no autorizado, las desconexiones físicas y lógicas, y el agotamiento de recursos; luego se encuentran las amenazas que están siendo controladas por el momento pero requieren de algunos cambios o mejoras para incrementar la seguridad.

Respecto a las salvaguardas citadas, es primordial tener el apoyo y colaboración de todo el personal implicado como son los jefes y administradores de cada área para que la adaptación de nuevas normas y procedimientos se realice de forma progresiva y consciente. Entre las principales salvaguardas se encuentran las relacionadas a aumentar la seguridad de la información, y esto se logra incrementando las medidas de seguridad a las cuentas de acceso a los sistemas, monitoreando las reglas de acceso y adquiriendo los procedimientos necesarios para restaurar la información si sucediera algún desastre natural.

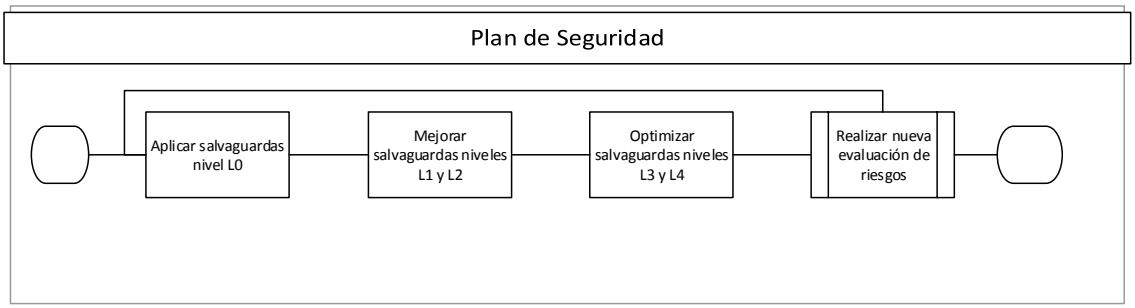
Para que la gestión de riesgos sea un proceso exitoso, este debe permanecer siempre en revisión por el grupo de seguridad a contratar para que ellos se aseguren que los niveles de riesgo no aumenten y las salvaguardas se apliquen de forma correcta y continua; para ello es necesario analizar datos estadísticos alimentados por la respectiva revisión de documentación como los registros de incidentes y resultados de encuestas realizadas al personal.

### 6.5.1 Marco de Referencia

En el Anexo se ha desarrollado una política de seguridad, la cual contiene parámetros, normas y responsables de los procesos de cada área. La política de seguridad debe someterse a evaluaciones y aprobaciones por parte del personal de seguridad y Gerencia para realizar las mejoras y correcciones respectivas para implementarla; además definir la frecuencia de revisión dentro del plan de gestión de riesgos.

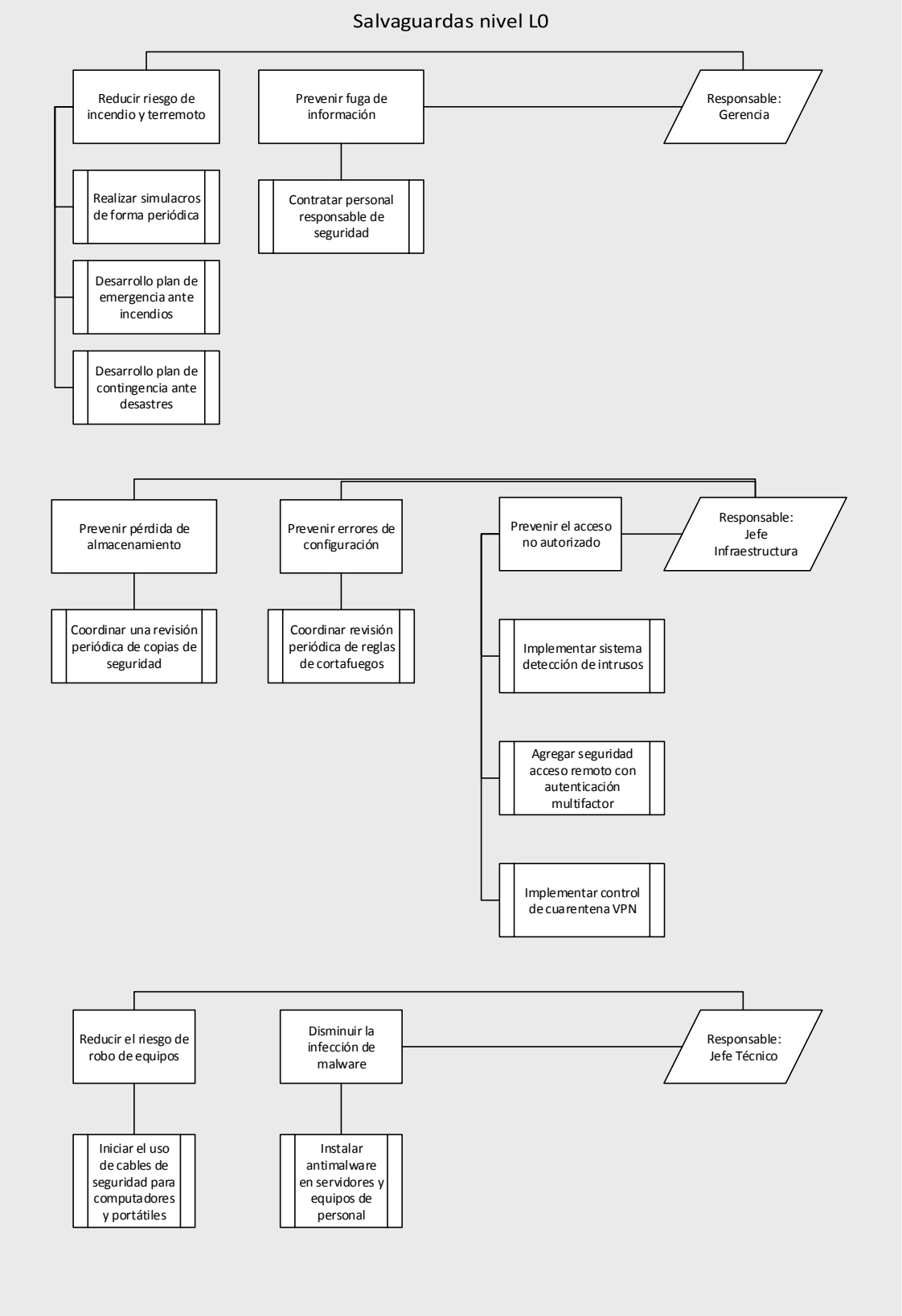
### 6.5.2 Plan de Ejecución

A continuación se presenta el proceso a seguir para implementar el plan de gestión de los riesgos existentes:

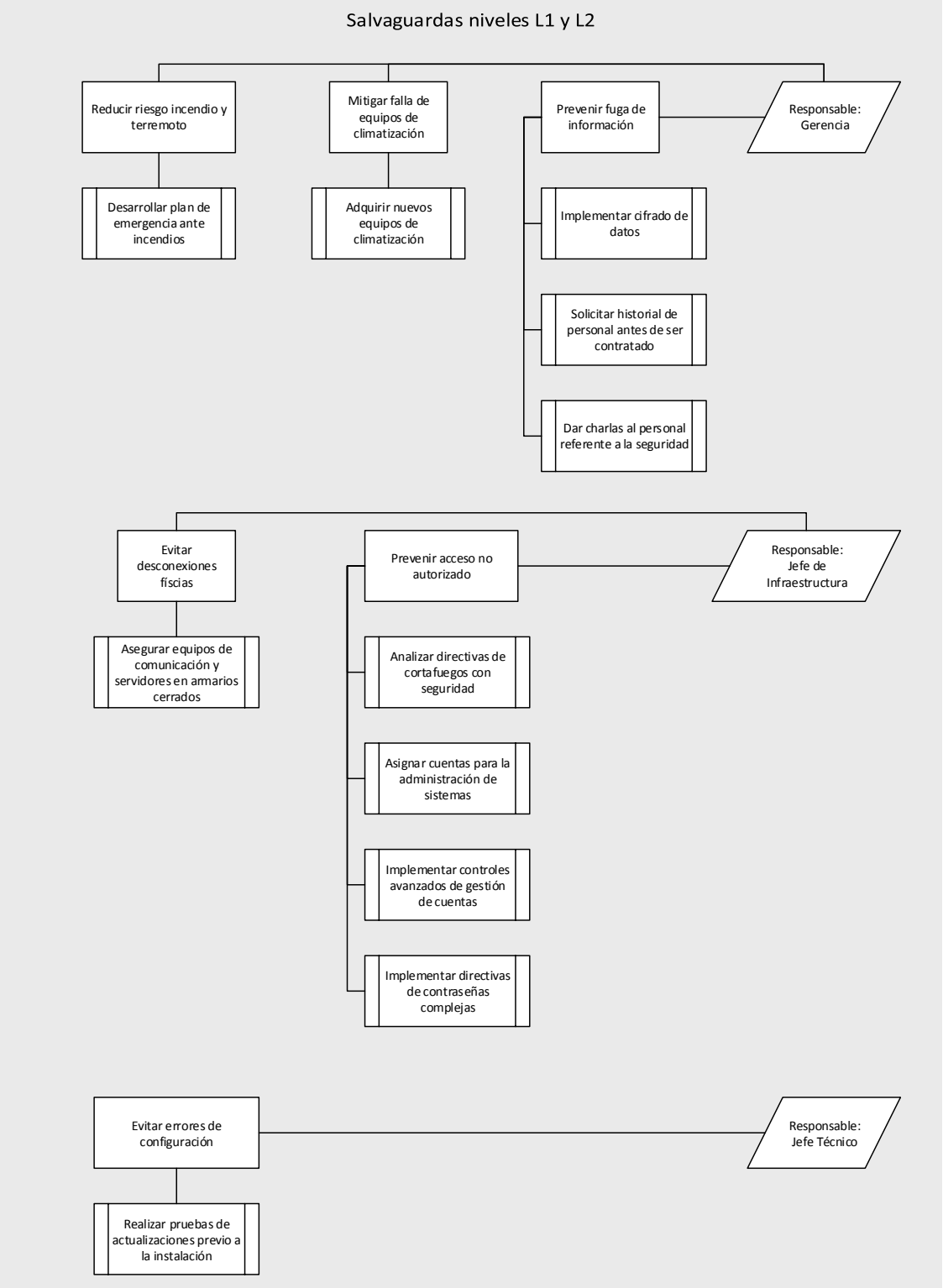



En primera instancia se deberán aplicar las salvaguardas con prioridad mayor es decir las de nivel L0 como medias preventivas y luego las salvaguardas con niveles superiores que conforman las medidas correctoras.

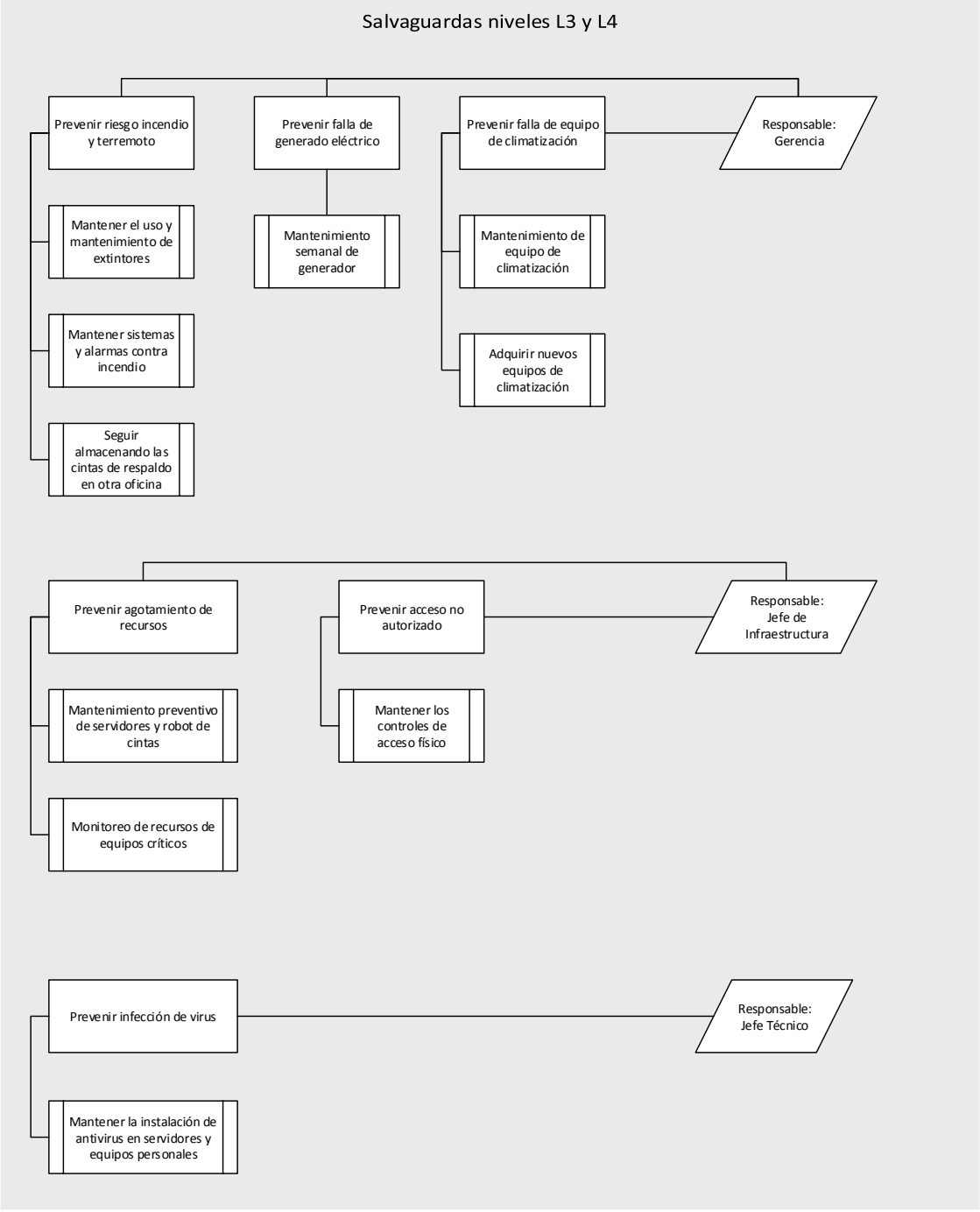
Entre las salvaguardas de nivel L0 se encuentran la prevención contra incendio y terremoto, prevención de la fuga de información, prevención de pérdida de almacenamiento y la prevención de acceso no autorizado.




En las salvaguardas de nivel L1 y L2 se encuentran los procesos que requieren de mejoras en la gestión.




En las salvaguardas de nivel L3y L4 se encuentran los procesos se han implementado y deben mantenerse y optimizarlos en lo posible.




Luego de haber definido e implementado los diversos procesos a realizar dentro del plan de seguridad es necesario volver a realizar un nuevo análisis de riesgo para conocer el nivel de riesgo obtenido, y así tratar de aplicar las medidas de seguridad necesarias para mantener la seguridad de la información. El tiempo de implementación del plan de seguridad no ha sido considerado porque éste depende de una serie de factores como financieros y administrativos.

# 7 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 amenazas a los cuales se encuentran expuestos los activos que forman parte del departamento de informática de la ESPOL, 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.

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.

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 de GTSI, 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.

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.

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.

# Bibliografía


[1] C. Klüppelberg, D. Straub and I. Welpe, Eds., Risk - A Multidisciplinary Introduction. Springer, 2014.

[2] (2009). ISO/Guide 73:2009(en). Available: https://www.iso.org/obp/ui/#iso:std:iso:guide:73:ed-1:v1:en.

[3] J. R. Vacca, Ed., Computer and Information Security Handbook. Elsevier, 2012.

[4] (2012). ISO27000.ES. Available: http://www.iso27000.es/sgsi.html.

[5] M. Amutio, J. Candau and J. Mañas, Eds., MAGERIT – Versión 3.0. Metodología De Análisis y Gestión De Riesgos De Los Sistemas De Información. Libro I - Método. 2012. Página 27.

[6] M. Amutio, J. Candau and J. Mañas, Eds., MAGERIT – Versión 3.0. Metodología De Análisis y Gestión De Riesgos De Los Sistemas De Información. Libro I - Método. 2012. Página 10

[7] R. Johnson and M. Merkow, Eds., Security Policies and Implementation Issues 2010. Página 3-19.

[8] (2015). About ISO. Available: http://www.iso.org/iso/home/about.htm.

[9] P. Pritzker, "Assessing Security and Privacy Controls in Federal Information Systems and Organizations," NIST, 2014.

[10] M. Amutio, J. Candau and J. Mañas, Eds., MAGERIT – Versión 3.0. Metodología De Análisis y Gestión De Riesgos De Los Sistemas De Información. Libro I - Método. 2012. Página 8

[11] R. Caralli, J. Stevens, L. Young and W. Wilson, Eds., Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process. 2007.

[12] A. Calder and S. Watkins, "Information Security Risk Management for ISO27001/ISO27002," 2010.

[13] CLUSIF, Ed., MEHARI. 2010.

[14] M. S. Lund, B. Solhaug and K. Stolen, Eds., Model-Driven Risk Analysis - the CORAS Approach. Springer-Verlag Berlin Heidelberg, 2011.

[15] (2014). Herramienta de Evaluación de Seguridad de Microsoft (MSAT). Available: https://technet.microsoft.com/es-es/library/cc185712.aspx.

[16] Le Logiciel Risicare. Objectifs de l'outil Risicare. Disponible en: http://www.ysosecure.com/methode-MEHARI/logiciel-risicare-mehari.html

[17] M. Amutio, J. Candau and J. Mañas, Eds., MAGERIT – Versión 3.0. Metodología De Análisis y Gestión De Riesgos De Los Sistemas De Información. Libro I - Método. 2012. Página 125

[18] M. Amutio, J. Candau and J. Mañas, Eds., MAGERIT – Versión 3.0. Metodología De Análisis y Gestión De Riesgos De Los Sistemas De Información. Libro I - Método. 2012. Páginas 22 - 45

[19] (2014). Misión y Visión de la ESPOL. Available: http://www.espol.edu.ec/espol/main.jsp?urlpage=mision.jsp.

[20] (2014). Transparencia de ESPOL. Available: http://www.transparencia.espol.edu.ec/sites/default/files/documentos/organigrama.pdf.

[21] A. Barco and J. Mañas, Eds., GUÍA DE SEGURIDAD DE LAS TIC (CCN-STIC-470D) - MANUAL DE USUARIO PILAR Versión 5.1. 2011.

[22] (2014). Security Content Overview. Available: https://msdn.microsoft.com/en-us/library/cc767969.aspx.

## Anexo: Política de Seguridad

La Gerencia de Tecnología y Sistemas de Información está conformada por departamentos de servicios y una Gerencia. Los departamentos son infraestructura, redes, técnico y sistemas, estas son las áreas encargadas de brindar los servicios informáticos a la comunidad politécnica.

La política de seguridad está conformada por una serie de normas y procedimientos que cubren varios aspectos con la finalidad de proteger la información y los recursos:

1. De equipos

Instalación de equipos de computación

1.1 Todo equipo de computación ya sean laptop, computador de escritorio o servidor que esté conectado a la red interna debe sujetarse a las normas y procedimientos de instalación que debe generar el departamento de infraestructura.

1.2 GTSI en coordinación con el departamento de Activo Fijo deberá tener un registro de todos los equipos de computación y de comunicación.

1.3 El equipo que sea de propósito específico y tenga una misión crítica asignada, requiere estar ubicado en un área que cumpla con todos los requerimientos de: seguridad física, condiciones ambientales, alimentación eléctrica, y acceso por el personal de GTSI.

1.4 Los responsables de las áreas de apoyo interno de los departamentos deberán en conjunción con el departamento de redes cumplir con las normas de instalación, y notificaciones correspondientes de actualización, reubicación, reasignación, y todo aquello que implique movimientos en su ubicación, de adjudicación, sistema y misión.

1.5 La protección física de los equipos corresponde a la persona asignada, y le corresponde notificar al departamento técnico cualquier anomalía o cambio de ubicación.

Mantenimiento de equipos de computación

1.6 Le corresponde al departamento técnico la realización del mantenimiento preventivo y correctivo de los equipos, la instalación, verificación de la seguridad física y el acondicionamiento requerido. Para tal fin se deben emitir normas y procedimientos respectivos.

1.7 El personal técnico de apoyo interno de los departamentos académicos se apegarán a los requerimientos establecidos a las normas y procedimientos que el departamento técnico emita.

1.8 Los responsables del departamento técnico no están autorizados a dar mantenimiento preventivo y correctivo a equipos que no pertenezcan a la institución.

Reubicación de equipos de computación

1.9 La reubicación del equipo de computación se realizará satisfaciendo las normas y procedimientos que el departamento técnico emita para ello.

1.10En caso de existir personal técnico de apoyo de los departamentos académicos, éste deberá notificar de los cambios tanto físico como de software al departamento técnico, y en su caso si cambiara de responsable al departamento de Activo Fijo. Notificando también los cambios de equipos inventariados.

1.11La reubicación de un equipo de computación se podrá realizar bajo la autorización del responsable y jefe del departamento técnico, con los medios necesarios para la instalación del equipo.

2 Control de Acceso

Acceso a Áreas Críticas

2.1 El acceso del personal se llevará a cabo de acuerdo a las normas y procedimientos que dicta la Gerencia.

2.2 En concordancia con la política de la institución y debido a la naturaleza de estas áreas se llevará un registro permanente del acceso y salida de personal, sin excepción.

2.3 La Gerencia deberá proveer de la infraestructura de seguridad requerida con base en los requerimientos específicos de cada área.

2.4 Bajo condiciones de emergencia, el acceso a las áreas de servicio crítico estará sujeto a las que especifiquen las autoridades superiores de la institución.

Control de Acceso al equipo de computación

2.5 Todos y cada uno de los equipos son asignados a un responsable, por lo que es de su competencia hacer buen uso de los mismos.

2.6 Las áreas donde se tiene el equipo de propósito general cuya misión es crítica estarán sujetas a los requerimientos que la Gerencia emita.

2.7 Los accesos a las áreas críticas deberán ser clasificados de acuerdo a las normas que dicte la Gerencia de común acuerdo con el comité de seguridad.

Control de acceso local a la red

2.8 El departamento de redes es responsable de proporcionar a los usuarios el acceso a los recursos informáticos.

2.9 La Gerencia es la responsable de difundir el reglamento para el uso de la red y de procurar su cumplimiento.

2.10El acceso lógico a los equipos de comunicación como son switches, enrutadores, cortafuegos, servidores, etc., conectados a la red son administrados por el departamento de redes.

2.11Todo equipo de computación que esté o sea conectado a la red de la institución, o aquellas que en forma autónoma se tengan y que sean propiedad de la institución, debe de sujetarse a los procedimientos de acceso que emite el departamento de redes.

Control de acceso remoto

2.12La Gerencia es la responsable de proporcionar el servicio de acceso remoto y las normas de acceso a los recursos informáticos disponibles.

2.13Para dar acceso a los servidores a terceros deberán dar a conocer el tiempo e indicar la finalidad del uso al jefe de infraestructura.

2.14El usuario de los servicios deberá sujetarse al reglamento de uso y en concordancia con los lineamientos generales del uso de Internet.

2.15El acceso remoto que realicen personas ajenas a la institución deberán cumplir las normas que emita la Gerencia.

Acceso a los Sistemas Administrativos

2.16Tendrán acceso a los sistemas administrativos solo el personal administrativo autorizado y éste dependerá del perfil que tenga definido.

2.17El manejo de información administrativa que se considere de uso restringido deberá ser cifrada con el objeto de garantizar su integridad.

2.18La instalación y uso de los sistemas de información se rigen por el reglamento de uso de la organización y por las normas y procedimientos establecidos por el GTSI.

2.19Los servidores de bases de datos son dedicados, porque lo que se prohíbe el acceso a personal no autorizado.

2.20El control de acceso a cada sistema de información será determinado por la unidad responsable de generar y procesar los datos involucrados.

Web

2.21El departamento de sistemas es responsable de instalar y administrar los servidores web, es decir, sólo se permiten servidores de páginas autorizadas.

2.22El departamento de sistemas deberá emitir las normas y requerimientos para la instalación de servidores de páginas locales, base de datos, uso de la intranet institucional, así como las especificaciones para que el acceso a estos sea seguro.

2.23Los accesos a las páginas web a través de los navegadores deben sujetarse a las normas que previamente se manifiesten en el reglamento de acceso a la red.

2.24A los responsables de los servidores web corresponde la verificación de respaldo, actualización y protección adecuada.

2.25Toda la programación involucrada en la tecnología web deberá estar de acuerdo con las normas y procedimientos que la Gerencia emita.

2.26El material que aparezca en la página de internet de la institución deberá ser aprobado por la Gerencia, respetando la ley de propiedad intelectual.

2.27Referente a la seguridad, protección y diseño de las páginas deberá considerarse el diseño de las páginas electrónicas establecidas por la Gerencia.

2.28La Gerencia tiene la facultad de llevar a cabo la revisión periódica de los accesos a los servicios de información y conservar información del tráfico.

3 Utilización de los recursos de la red

3.1 Los recursos disponibles a través de la red serán de uso exclusivo para asuntos relacionados con las actividades sustantivas del centro.

3.2 El departamento de redes es responsable de emitir y dar seguimiento al reglamente para el uso de la red.

3.3 De acuerdo con las disposiciones de la institución, corresponde a GTSI administrar, mantener y actualizar la infraestructura de la red.

3.4 La Gerencia debe propiciar el uso de las tecnologías de la información con el fin de contribuir con las directrices económicas y ecológicas de la institución.

3.5 Dado el carácter confidencial que involucra el correo electrónico el comité de seguridad emite una reglamentación.

4 Software

<u>Adquisición del software</u>

4.1 En concordancia con la política de la institución, el comité de seguridad y la Gerencia son los organismos oficiales para establecer los mecanismos de procuración de sistemas informáticos.

4.2 La Gerencia promoverá y propiciará que la adquisición de software de dominio público provenga de sitios oficiales y seguros.

4.3 Corresponde a la Gerencia emitir las normas para el tipo de licenciamiento, cobertura, transferibilidad, certificación y vigencia.

Instalación del software

4.4 El departamento técnico debe emitir las normas y procedimientos para la instalación y supervisión del software básico para cualquier tipo de equipo.

4.5 En los equipos de computación y telecomunicaciones, únicamente se permitirá la instalación de software con licenciamiento apropiada y de acorde a la propiedad intelectual.

4.6 El departamento técnico es el responsable de brindar asesoría y supervisión para la instalación de software informático, así mismo el departamento de redes para el software de telecomunicaciones.

4.7 Cualquier software que la Gerencia considere que pone en riesgo los recursos de la institución no está permitido.

4.8 Para proteger la integridad de los sistemas informáticos y telecomunicaciones, es necesario que todos los equipos involucrados dispongan de software de seguridad como son antivirus, vacunas, privilegios de acceso, parches de seguridad, y otros que se apliquen.

4.9 La protección lógica de los sistemas corresponde a quienes se les asignó el equipo y les compete notificar cualquier movimiento al departamento técnico.

Actualización del software

4.10La adquisición y actualización de software para equipo de computación y telecomunicaciones se llevara a cabo de acuerdo a la calendarización que anualmente sea propuesta por la Gerencia.

4.11Corresponde al departamento de infraestructura autorizar cualquier adquisición y actualización del software.

4.12Las actualizaciones del software de uso común se llevaran a cabo de acuerdo al plan de actualización desarrollado por la Gerencia.

Auditoría de software instalado

4.13El departamento de auditoría es el responsable de realizar revisiones periódicas para asegurar que sólo los programas con licencia están instalados en los computadores de la institución.

4.14La Gerencia propiciará la conformación de un grupo especializado en auditoría de sistemas de computación y sistemas de información.

4.15Corresponderá al grupo especializado dictar las normas, procedimientos y calendarios de auditoría.

Software propiedad de la institución

4.16Todos los programas desarrollados o comprados por la institución son propiedad de la institución y mantendrán los derechos que la ley de propiedad intelectual les confiera.

4.17La Gerencia en coordinación con el departamento técnico deberá tener un registro de todos los paquetes de programación propiedad de la institución.

4.18Es obligación de todos los usuarios que manejen información masiva, mantener el respaldo correspondiente de la misma ya que se considera como un activo de la institución que debe preservarse.

4.19Los datos, base de datos, información generada por el personal y los recursos informáticos de la institución deben ser resguardados.

4.20Corresponderá al departamento de infraestructura promover y difundir los mecanismos de respaldo y salvaguarda de los datos y de los sistemas.

4.21El departamento técnico administrará los diferentes tipos de licencia de software y vigilará su vigencia en concordancia con la política informática.

Uso de Software de la Institución

4.22Cualquier software que requiera ser instalado para trabajar sobre la red deberá ser evaluado por el departamento técnico.

4.23Todo software de propiedad de la institución deberá ser usado exclusivamente para asuntos relacionados con las actividades de la institución.

5 Supervisión y Evaluación

5.1 Cada uno de los departamentos de GTSI donde esté en riesgo la seguridad en la operación, servicio y funcionalidad del departamento, deberá emitir las normas y procedimientos que corresponda.

5.2 Las auditorías de cada actividad donde se involucren aspectos de seguridad lógica y física deberán realizarse periódicamente y deberá sujetarse al calendario que establezca la Gerencia o el grupo especializado de seguridad.

5.3 Para efectos de que la institución disponga de una red con alto grado de confiabilidad, será necesario que se realice un monitoreo constante sobre todos y cada uno de los servicios que las tecnologías de la internet e intranet dispongan.

5.4 Los sistemas considerados críticos, deberán estar bajo monitoreo permanente.

Generales

1. Cada uno de los departamentos deberá de emitir los planes de contingencia que correspondan a las actividades críticas que realicen.

2. Debido al carácter confidencial de la información, el personal de GTSI deberá conducirse de acuerdo a los códigos de ética profesional y normas y procedimientos establecidos.

Sanciones

1. Cualquier violación a las políticas y normas de seguridad deberá ser sancionada de acuerdo al reglamento emitido por la Gerencia.

2. Corresponderá a la Gerencia hacer las propuestas finales sobre las sanciones a quienes violen las disposiciones en materia de informática de la institución.

3. Todas las acciones en las que se comprometa la seguridad dela red y que no estén previstas en esta política, deberán ser revisadas por la Gerencia para dictar una resolución sujetándose al estado derecho.