UNIVERSIDAD TÉCNICA DEL NORTE

Facultad de Ingeniería en Ciencias Aplicadas Carrera de

Ingeniería en Sistemas Computacionales

GESTIÓN DE RIESGOS INFORMÁTICOS APLICANDO UNA METODOLOGÍA DE ANÁLISIS PARA VERIFICAR LA SEGURIDAD DE LA INFORMACIÓN EN UNA EMPRESA DE AUDITORÍA, CONSULTORÍA Y CAPACITACIÓN

Trabajo de grado previo a la obtención del título de Ingeniero en Sistemas Computacionales

Autor:

Cristhian Andrés Buitrón Gonzaga

Director:

MSc. Daisy Imbaquingo

Ibarra-Ecuador

UNIVERSIDAD TÉCNICA DEL NORTE

BIBLIOTECA UNIVERSITARIA

AUTORIZACIÓN DE USO Y PUBLICACIÓN A FAVOR DE LA UNIVERSIDAD TÉCNICA DEL NORTE

1. IDENTIFICACIÓN DE LA OBRA

En cumplimiento del Art. 144 de la Ley de Educación Superior, hago la entrega del presente trabajo a la Universidad Técnica del Norte para que sea publicado en el Repositorio Digital Institucional, para lo cual pongo a disposición la siguiente información:

DATOS DE CONTACTO			
CÉDULA DE IDENTIDAD:	1004154017		
APELLIDOS Y NOMBRES:	Buitrón Gonzaga Cristhian Andrés		
DIRECCIÓN:	Los Ceibos, Río Amazonas Y Río Chambo 3-11		
EMAIL:	cabuitrong@utn.edu.ec		
TELÉFONO FIJO:	062-954-076	**TELÉFONO MÓVIL:**	0998992524

DATOS DE LA OBRA	
TÍTULO:	Gestión de riesgos informáticos aplicando una metodología de análisis para verificar la seguridad de la información en una empresa de auditoría, consultoría y capacitación.
AUTOR (ES):	Buitrón Gonzaga Cristhian Andrés
FECHA: DD/MM/AAAA	23/03/2021
SOLO PARA TRABAJOS DE GRADO	
PROGRAMA:	☒ **PREGRADO** ☐ **POSGRADO**
TITULO POR EL QUE OPTA:	Ingeniero en Sistemas Computacionales
ASESOR /DIRECTOR:	Msc. Daisy Imbaquingo

2. CONSTANCIAS

El autor (es) manifiesta (n) que la obra objeto de la presente autorización es original y se la desarrolló, sin violar derechos de autor de terceros, por lo tanto la obra es original y que es (son) el (los) titular (es) de los derechos patrimoniales, por lo que asume (n) la responsabilidad sobre el contenido de la misma y saldrá (n) en defensa de la Universidad en caso de reclamación por parte de terceros.

Ibarra, a los 09 días del mes de abril de 2021

EL AUTOR:

(Firma):.....

Nombre: Buitrón Gonzaga Cristhian Andrés

CERTIFICACIÓN DIRECTOR DE TESIS

En mi calidad de tutor del Trabajo de Grado presentado por el egresado **BUITRÓN GONZAGA CRISTHIAN ANDRÉS** para optar por el Título de Ingeniería en Sistemas Computacionales cuyo tema es **GESTIÓN DE RIESGOS INFORMÁTICOS APLICANDO UNA METODOLOGÍA DE ANÁLISIS PARA VERIFICAR LA SEGURIDAD DE LA INFORMACIÓN EN UNA EMPRESA DE**

AUDITORÍA, CONSULTORÍA Y CAPACITACIÓN. Considero que el presente trabajo reúne los requisitos y méritos suficientes para ser sometido a la presentación pública y evaluación por partedel tribunal examinador que designe.

En la ciudad de Ibarra, a los 05 días del mes de abril del 2021

DAISY ELIZABETH IMBAQUINGO ESPARZA

Firmado digitalmente por DAISY ELIZABETH IMBAQUINGO ESPARZA
Fecha: 2021.04.06 11:28:29 -05'00'

MSc. Daisy Imbaquingo

TUTOR TRABAJO DE GRADO

DEDICATORIA

A Dios porque es quien dirige mi camino.

A mi madre que es mi pilar fundamental, mi soporte, mi guía, la persona que siempre está ahí, la mujer que quito alimento de su boca para dármela a mí, la persona que me daba sus últimas monedas para poder ir a estudiar, todo lo que soy y seré en mi vida se lo debo a ella.

AGRADECIMIENTOS

A mi padre Eduardo Buitrón quien a pesar de no estar junto a mí nunca dejo de darme apoyo y esas ganas de continuar.

A mi hermando Fernando Dorado quien es un padre para mí ya que nunca dejo de apoyarme económicamente, sentimentalmente.

A mis tías, tíos, prim@s que con un granito de arena me apoyaron siempre.

A la Universidad Técnica del Norte con su Carrera de Ingeniería en Sistemas Computaciones que me ofrecieron todo el conocimiento.

A la Ing. Daisy Imbaquingo quien logró ser una guía dentro de este camino universitario y quien es un ejemplo de mujer, docente y amiga.

A mis docentes Marco Pusdá, Cathy Guevara, Antonio Quiña, Mauricio Rea, Alex Guevara quienes me brindaron su conocimiento dentro y fuera del aula.

A Edwin Bastidas quien estuvo desde el día cero, siendo un compañero en las aulas y amigo en la vida.

A Celeste Imbaquingo quien ha sido ese soporte sentimental y quien nunca soltó mi mano aún más en los momentos difíciles.

- **Contenido**

Resumen

Este trabajo investigativo tiene como finalidad gestionar los riesgos informáticos aplicando una metodología de análisis para verificar la seguridad de la información para una empresa de auditoria, consultoría y capacitación.

Para cumplir con los objetivos se realizó la búsqueda de la metodología que se apegue más al enfoque y a la realidad de la falta de experiencia en el campo que se engloba este trabajo.

El capítulo uno define un marco teórico para poder entender y encaminar este trabajo, para poder tener una visión clara de los conceptos que engloba la Seguridad de la Información y la Gestión de Riesgos Informáticos en entidades que están implicadas en esta área.

El capítulo dos se usa el método Delphi para comparar la metodología Magerit e ISO 27005 dicho método se basa en consultar a un grupo de expertos en el área y escoger la que al final del proceso sea la adecuada.

El capítulo tres muestra la aplicación en todo su contexto de la metodología Magerit que salió ganadora de la comparación, para aplicar dicha metodología se usa la herramienta Pilar que es desarrollada en base a Magerit.

Palabras clave: Seguridad de la información, Gestión de Riesgos Informáticos, Método Delphi, Magerit, ISO 27005, Pilar.

Abstract

The purpose of this investigative work is to manage computer risks by applying an analysis methodology to verify information security for an auditing, consulting and training company.

To meet the objectives, a search was carried out for the methodology that more closely adheres to the approach and the reality of the lack of experience in the field that this work encompasses.

Chapter one defines a theoretical framework to be able to understand and guide this work, in order to have a clear vision of the concepts that include Information Security and Computer Risk Management in entities that are involved in this area.

Chapter two uses the Delphi method to compare the Magerit and ISO 27005 methodology. This method is based on consulting a group of experts in the area and choosing the one that is appropriate at the end of the process.

Chapter three shows the application in all its context of the Magerit methodology that was the winner of the comparison, to apply this methodology the Pilar tool is used, which is developed based on Magerit.

Keywords: Information Security, IT Risk Management, Delphi Method, Magerit, ISO 27005, Pilar.

INTRODUCCIÓN

PROBLEMA

ANTECEDENTES

IBM Security presentó los resultados del estudio global “Cost of Data Breach”, el cuál presenta los efectos que ocurren al momento de la pérdida de datos en las empresas, este estudio está basado en las 12 economías globales, el cuál manifiesta que en el año 2017 las empresas en promedio han perdido $3.62 millones, siendo el sector de la salud uno de los más afectados, tomando en cuenta que los incidentes de seguridad representan $141 por registro robado dentro de las empresas. (Ponemon & Whitemore, 2017)

Las organizaciones deben ser veloces al momento de contener un incidente relacionado con la pérdida de datos afectando de manera directa a su economía, todo esto se podría ahorrar si las organizaciones contaran con un equipo de respuesta de incidentes al igual que un análisis de riesgos a los que puedan estar expuestos junto con normas y políticas que minimicen el proceso. (Ponemon & Whitemore, 2017)

Las empresas y sus sistemas de información se enfrentan a factores internos y externos que amenazan la confidencialidad, integridad y disponibilidad de su información, con frecuencia existen incidentes a nivel mundial de ataques informáticos o fraudes en donde su activo más importante es la información que se ve afectada y puesta en riesgo.

SITUACIÓN ACTUAL

En la actualidad las empresas manejan la información desde el lado práctico y se ve como algo que siempre está disponible, ya que se toman acciones para su protección solamente cuando sucede algún incidente. (Posada, 2016)

En determinadas empresas a la información se ve como algo productivo, ya que expresan que no genera beneficios y por consiguiente no tienen un grado de cuidado. Pero al momento que se observa que el beneficio puede verse disminuido, por su falta, es ahí cuando a la información la consideran como un activo muy importante para la organización. (Posada, 2016)

La mayoría de las empresas generan un listado de activos de información valorados de acuerdo con su impacto en términos de la pérdida de los tres principios básicos de la seguridad de la información que son: la Confidencialidad, la Integridad y la Disponibilidad. (Almeida, 2017)

La gestión de riesgos ayuda a la empresa a saber en qué estado de afectación se encuentra, y así tomar cartas en el asunto para poder mitigarlos, ya que eliminarlos por completo no se puede. (Almeida, 2017)

PLANTEAMIENTO DEL PROBLEMA

¿Cómo la Gestión de Riesgos de Seguridad de la Información ayudaría a la empresa de Consultoría y Capacitación al manejo de la información?

El personal de empresas de Auditoría, Consultoría y Capacitación gestionan diferentes tipos de información, al no tener definidos lineamientos claros se podría provocar algunas brechas de seguridad, esto se resuelve identificando el riesgo existente y tratándolos Figura 1.

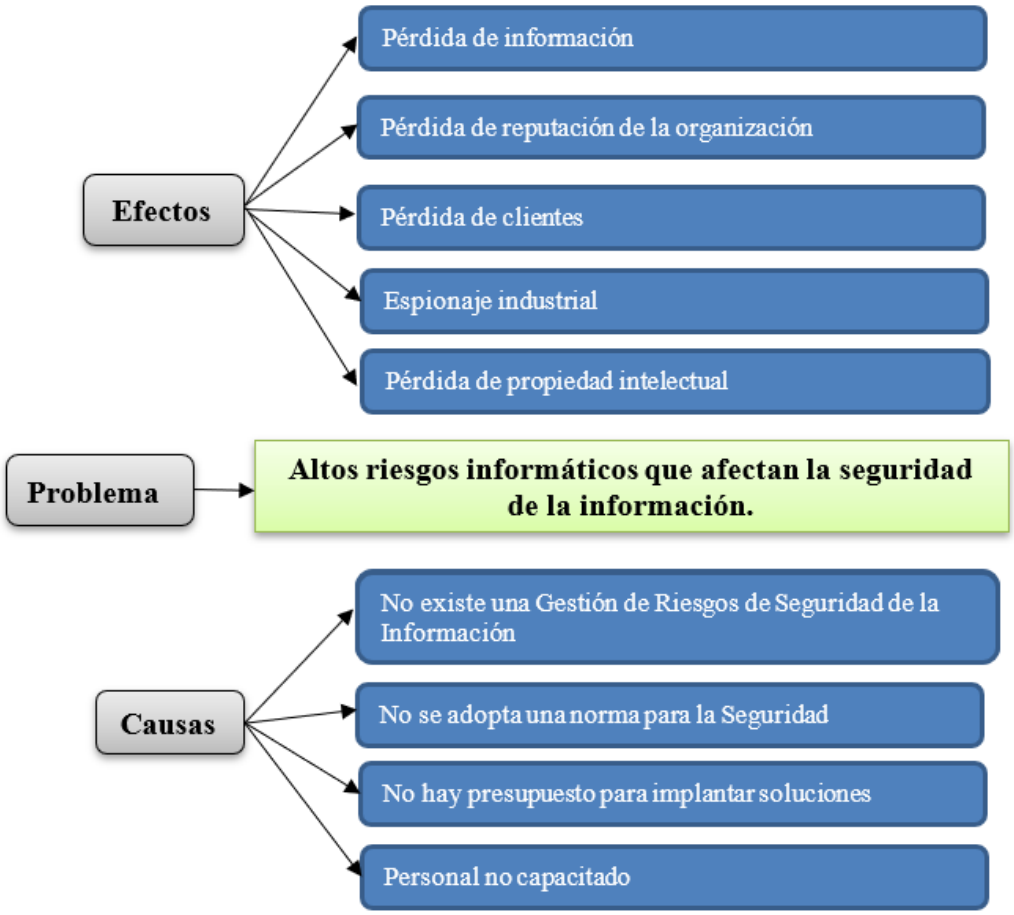


Figura 1 *Planteamiento del problema*
Fuente: Propia

OBJETIVOS

OBJETIVOS ESPECÍFICOS

a) Fundamentar un marco teórico para la gestión de riesgos de la seguridad de la información.
b) Realizar comparativa entre dos metodologías de gestión de riesgos de seguridad de la información.
c) Aplicar la metodología seleccionada para la gestión de riesgos de seguridad de la información.

OBJETIVO GENERAL

Gestionar los riesgos informáticos aplicando una metodología de análisis para verificar la seguridad de la información en una empresa de auditoría, consultoría y capacitación.

ALCANCE

Para una buena gestión de riesgos es importante tener un inventario de activos de información, que permitió clasificar a los activos a los que se debe brindar mayor protección pues identifica claramente sus características y rol al interior de un proceso (*MINTIC*, 2019)

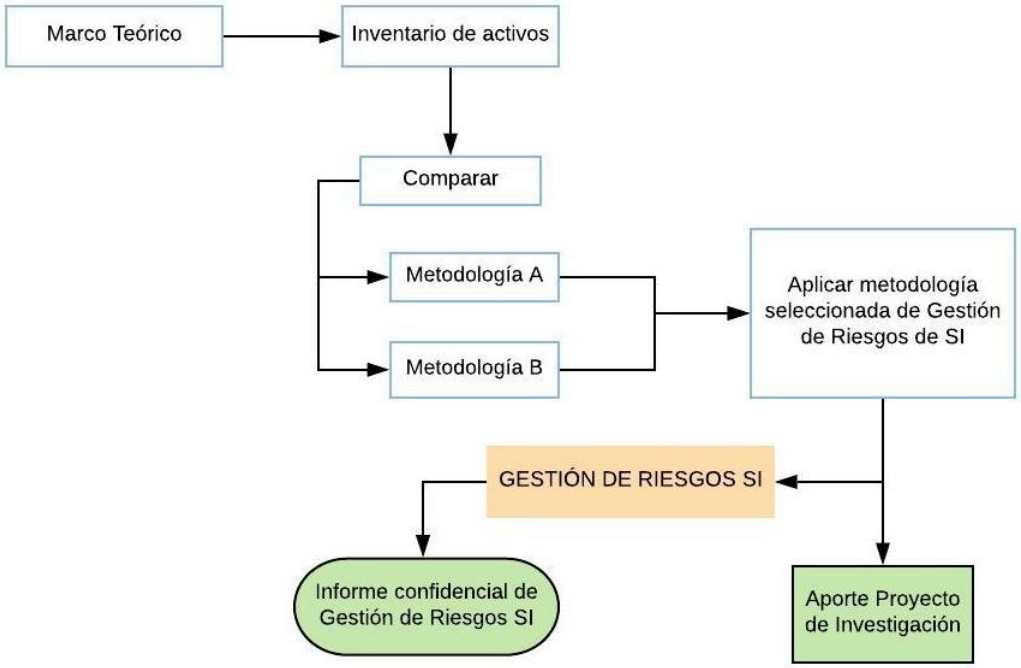


Figura 2 *Alcance gestión de riesgos SI*
Fuente: Propia

Marco teórico

Dentro del marco teórico se realiza una búsqueda exhaustiva de temas de Seguridad de la Información en donde se encuentre la gestión de riesgos informáticos, la información deberá ser de fuentes confiables siendo estos artículos, trabajos de grados publicados y verificados.

Consiste en analizar y presentar las teorías que existen sobre el problema a investigar, también incluye los trabajos e investigaciones que existen y todos los antecedentes sobre lo que se va a desarrollar como investigación. El marco teórico se refiere a todas las fuentes de consulta teórica que se puede disponer sobre el problema a investigar. (*SAMPIERI, Hernández Roberto*, 2018)

Inventario de activos

Un activo es cualquier bien que tiene valor para la organización. (Andrés & Gómez, 2019) Se realizará una recopilación de todos los bienes tecnológicos del área seleccionada dentro de la empresa para la realización de la gestión de riesgos.

Metodología de valoración de riesgos

Seleccionar y comparar dos de las metodologías más usadas para la gestión de riesgos en empresas de Auditoría y Consultoría a nivel mundial, la comparación se realizará aplicando aspectos relevantes en la aplicación y resultados de la gestión realizada.

Se elegirá por la que en la comparación resulte más efectiva a la hora de gestionar los riesgos de seguridad de la información.

Gestión de riesgos

Actividades coordinadas para dirigir y controlar una organización con respecto a los riesgos. (Andrés & Gómez, 2019)

Se aplicó la metodología seleccionada para la gestión de riesgos de seguridad informáticos encontrando las amenazas y vulnerabilidades que cuenten los activos encontrados y determinando los riesgos existentes.

Valoración de riesgos

Los activos de información se valoraron de acuerdo con su impacto en términos de la pérdida de los tres principios básicos de la seguridad de la información que son: la Confidencialidad, la Integridad y la Disponibilidad. (Almeida, 2017)

Aporte proyecto de investigación

Como parte del proyecto de investigación de la tutora sugerida en este tema de tesis, se aportó con las características principales de cómo se aplica una metodología de análisis de riesgos informáticos dentro de empresas para después de ello realizar una comparativa con las instituciones de educación superior, que es una parte del proyecto de investigación.

JUSTIFICACIÓN

El proyecto tiene un enfoque a un objetivo de desarrollo sostenible que es:

Objetivo 16: Promover sociedades, justas, pacíficas e inclusivas

Este hace frente a desafíos de construir sociedades más pacíficas e inclusivas, es necesario que se establezcan reglamentaciones más eficientes, transparentes y presupuestos gubernamentales integrales y realistas. (United Nations, 2017)

16.a Fortalecer las instituciones nacionales pertinentes, incluso mediante la cooperación internacional, para crear a todos los niveles, particularmente en los países en desarrollo, la capacidad de prevenir la violencia y combatir el terrorismo y la delincuencia. (United Nations, 2017)

El plan nacional toda una vida cuenta con políticas que hacen referencia como son:

1.11 Impulsar una cultura de gestión integral de riesgos que disminuya la vulnerabilidad y garantice a la ciudadanía la prevención, la respuesta y atención a todo tipo de emergencias y desastres originados por causas naturales, antrópicas o vinculadas con el cambio climático. (Secretaría Nacional de Planificación y Desarrollo, 2017)

1.16 Promover la protección de los derechos de usuarios y consumidores de bienes y servicios. (Secretaría Nacional de Planificación y Desarrollo, 2017)

Justificación Tecnológica

El auge de la tecnología y el auge de la protección de la información avanza cada día y se presenta como una oportunidad de evolución de la sociedad creando una cultura de uso seguro de la información y de la tecnología en general.

Justificación Social

Con el crecimiento del uso del internet y de las herramientas informáticas disponibles que existen, se presentan riesgos que pueden afectar la seguridad de la información, es por eso por lo que la gestión de riesgos ayuda a tomar cartas en el asunto y transmitir seguridad.

Justificación Ambiental

El uso del papel ha significado un daño significativo a nuestro ambiente es por eso por lo que es necesario poder migrar del papel a lo digital, este proyecto ayuda a eso, teniendo todo digitalizado y a la mano del personal.

CAPITULO I
Marco Teórico

1.1 Seguridad de la información

Seguridad es un conjunto de sistemas, medios organizativos, medios humanos y acciones dispuestas para eliminar, reducir o controlar los riesgos y amenazas que puedan afectar a una persona a una entidad a una instalación o a un objeto. La seguridad proporciona las condiciones para afrontar el peligro, en síntesis, seguridad es la minimización del riesgo. (Mora, 2020)

La información, en términos generales se denomina un conjunto de datos que contiene un significado que aporta conocimiento, pero en términos informáticos posee un sentido diferente es decir se puede referir a una serie de datos codificados con el fin de realizar una acción especifica. (Morales, 2019)

La naturaleza y el tipo de tecnologías que constituyen la infraestructura de la información y comunicaciones han cambiado de manera significativa. El número y tipo de dispositivos, servicios y variedades que integran la infraestructura de acceso se ha multiplicado, e incluye ya variados elementos de tecnología fija, inalámbrica y móvil, así como una proporción creciente de accesos que están conectados de manera permanente. (Quiroz Zambrano & Macías Valencia, 2017)

La información es fundamental para la vida de todo ser humano, para cualquier tipo de empresa, así también para la sociedad en general, es por esto que surge la gran importancia que se debería conceder a todos los temas relacionados con la información, ya que esta es el actor principal dentro de cualquier acción que se realice. (Urbina, 2016)

Teniendo en cuenta lo antes mencionado se obtiene un punto de vista más amplio, en la norma ISO/IEC 27001 en donde define a la Seguridad de la Información como la preservación de su confidencialidad, su integridad y su disponibilidad, como se detalla en la Figura 3. (ISO/IEC 27001, 2017)

Figura 3. *Pilares fundamentales de la seguridad de la información*
Fuente: Buitrago (2017)

Los objetivos de la seguridad de la información son los siguientes:

- **Disponibilidad**

La disponibilidad de la información hace referencia a que la información esté accesible cuando la necesitemos. Algunos ejemplos de falta de disponibilidad de la información son: cuando nos es imposible acceder al correo electrónico corporativo debido a un error de configuración, o bien, cuando se sufre un ataque de denegación de servicio, en el que el sistema no permite accesos legítimos. Ambos tienen implicaciones serias para la seguridad de la información. (INCIBE, 2020)

- **Confidencialidad**

Se trata de la cualidad que debe poseer un documento o archivo para que éste solo se entienda de manera comprensible o sea leído por la persona o sistema que esté autorizado. Un ejemplo de control de la confidencialidad sería el uso cifrado de clave simétrica en el intercambio de mensajes. (Ortega, 2018)

- **Integridad**

Se trata de que la información debe ser correcta y esté libre de modificaciones y errores. La información puede ser alterada intencionadamente o ser incorrecta. Ejemplos de ataques contra la integridad de la información son la alteración malintencionada en los archivos del sistema informático mediante la explotación de una vulnerabilidad, o la modificación de un informe de ventas por un empleado malintencionado o por error humano. (INCIBE, 2020)

- **No repudio**

Es él envió de información a través de las redes con la capacidad de demostrar la identidad del emisor de esta información, soporta directamente la disuasión, el aislamiento de fallos, la detección y prevención de intrusiones y después la recuperación y las acciones legales pertinentes. El objetivo que se pretende es certificar que la información o los datos provienen realmente de la fuente que dice ser. (INSTITUTO NACIONAL DE CIBERSEGURIDAD, 2016)

1.1.1 Entidades implicadas en la seguridad

Las entidades implicadas se muestran en la Figura 4.

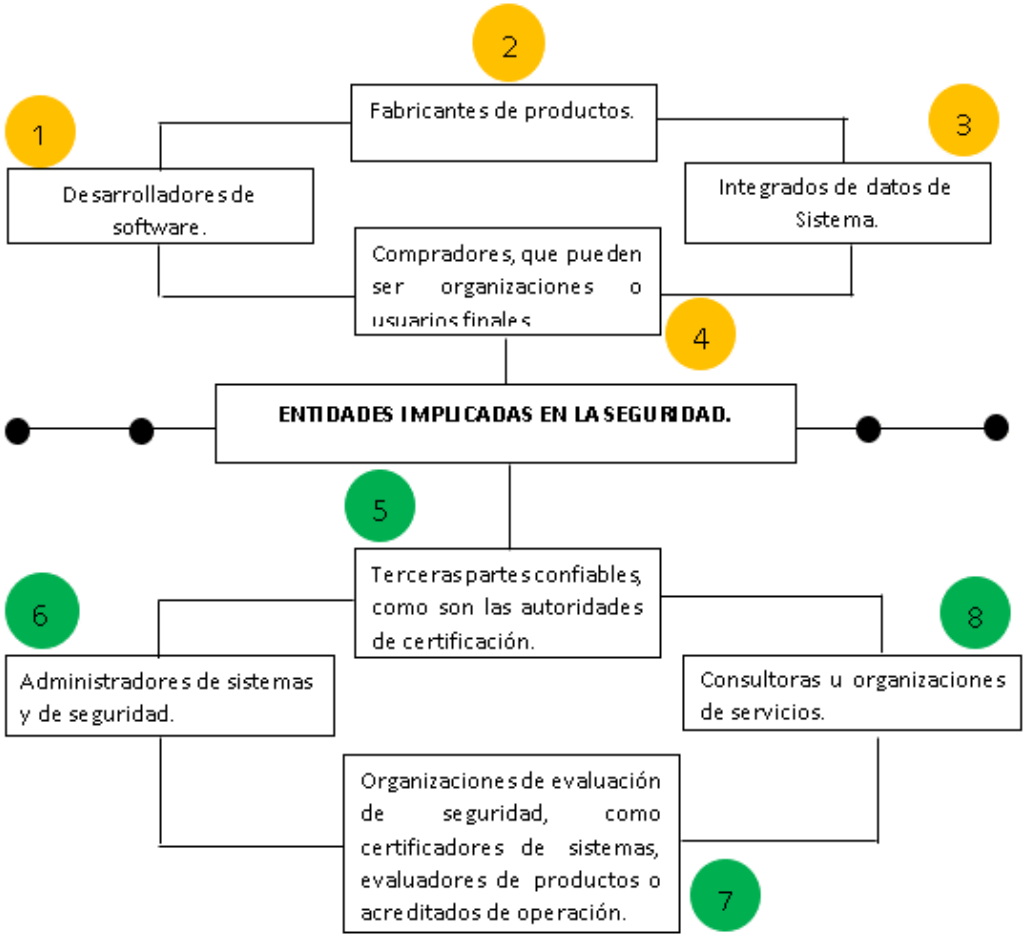


Figura 4. *Entidades implicadas en la seguridad de la información*
Fuente: Propia

Las actividades de seguridad deben ser tomadas en cuenta por todo el personal relacionado con los sistemas de información.

Dentro de las entidades u organizaciones se cometen errores en el tratamiento de la información, INCIBE(2020) presenta una lista de los errores comunes que se cometen y de cómo evitarlos como se presenta en la tabla 1.

Tabla 1*: Errores más comunes en el tratamiento de la información en una organización*

ERRORES	CÓMO EVITARLOS
Información importante de la que no se realiza copia de seguridad.	Para evitar este error tendremos que asegurarnos que tenemos una copia de seguridad actualizada de la información, al menos de aquella información más crítica.
Acceso a carpetas de red compartidas sin control de acceso, sin versionamiento e información ajena al puesto de trabajo .	Estos errores se pueden evitar si hacemos que la información sólo sea accesible a quien le necesita y esté autorizado para ello. Es decir implantar un control de acceso.
Presencia de discos duros portátiles ajenas a la organización. Falta de formación de los empleados en las herramientas que utilizan, como son servicios de nube, correo empresarial usándola en actividades personales.	Si no se limita el uso de aplicaciones no corporativas (correo personal, almacenamiento en la nube) y se controla el uso de los dispositivos externos al igual que una falta de formación, cometeremos estos errores.
Tirar los ordenadores y discos a la basura sin ningún control previo de su contenido.	Tener inventariado los equipos es esencial pues algún día dejan de ser útiles, por obsoletos o por desgaste, ese el momento de deshacerse de ellos, borrar toda la información que tenían, de forma que no quede ni rastro de su uso previo, para la posterior eliminación de estos.

Fuente: INCIBE (2020)

1.2 Requisitos de la Seguridad de la Información

En la Figura 5 se detallan los requisitos de la seguridad de la información.

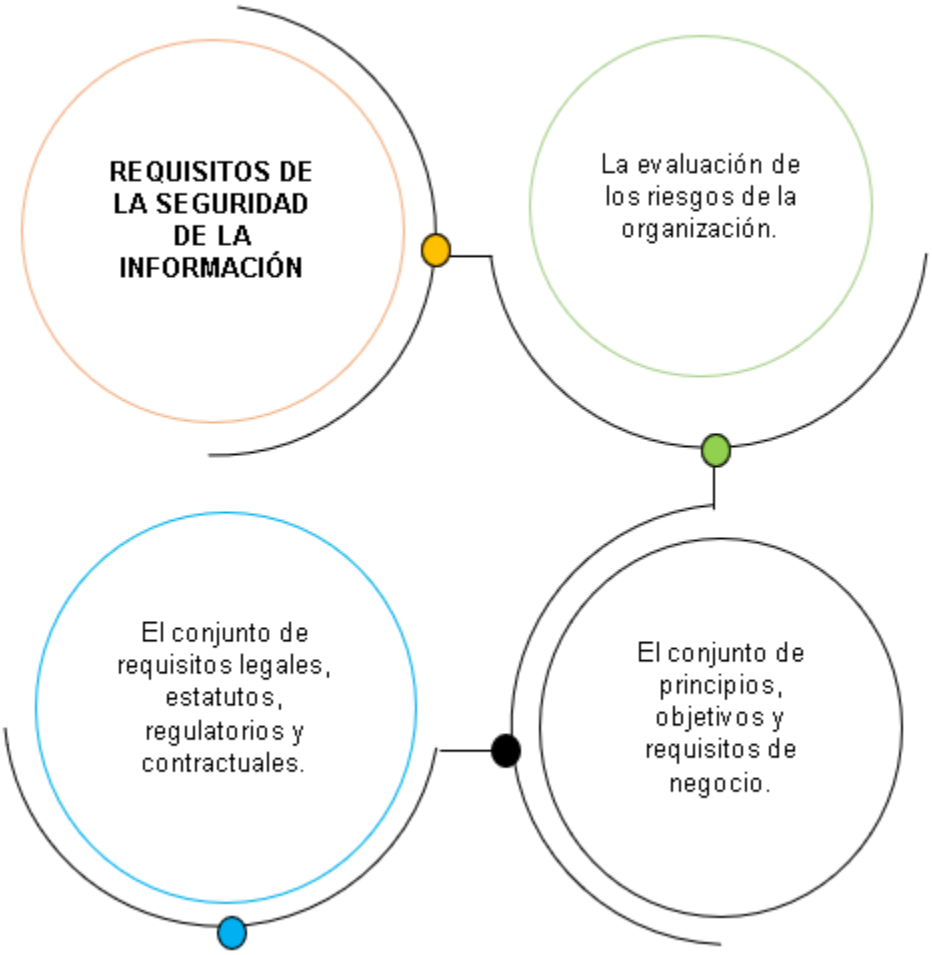


Figura 5 *Requisitos de la Seguridad de la Información*
Fuente: ISO/IEC 27008 (2017)

1.3 Seguridad de la información en la gestión de proyectos

La seguridad de la información debe integrarse en el método o métodos de gestión de proyectos de toda organización para asegurar que los riesgos de seguridad de la información se identifican y se contemplan en el marco de un proyecto. Esto se aplica en general en cualquier proyecto, en este trabajo de titulación se aplicó a una organización el proceso de gestión de riesgos de seguridad de la información. Según (ISO/IEC 27002, 2017) los métodos de gestión de proyectos deberían exigir que:

- Los objetivos de seguridad de la información estén incluidos en los objetivos del proyecto.
- Realizar una evaluación de riesgos de seguridad de la información en una fase temprana del proyecto para identificar los controles necesarios.

1.4 Sistema de Gestión de Seguridad de la Información (SGSI)

El Sistema de Seguridad de la Información (SGSI) es el elemento más importante de la norma ISO 27001, que unifica los criterios para la evaluación de los riesgos asociados al manejo de la información corporativa en las empresas, es por tanto, el conjunto de prácticas orientadas a garantizar la seguridad, la integridad y la confidencialidad de estos datos. (ISOTools, 2016)

La base exitosa de un SGSI es seguir un ciclo de mejora contínua llamado PDCA que viene de las siglas Planificar, Hacer, Verificar y Actuar, en inglés “Plan, Do, Check, Act” como se puede observar en la (Figura 6), también conocido como Círculo de Deming, por ser Edwards Deming su autor. Este ciclo describe los cuatro pasos esenciales que se deben llevar a cabo de forma sistemática para lograr la mejora continua en un SGSI. (Instituto Nacional de Tecnologías de la Comunicación, 2016)

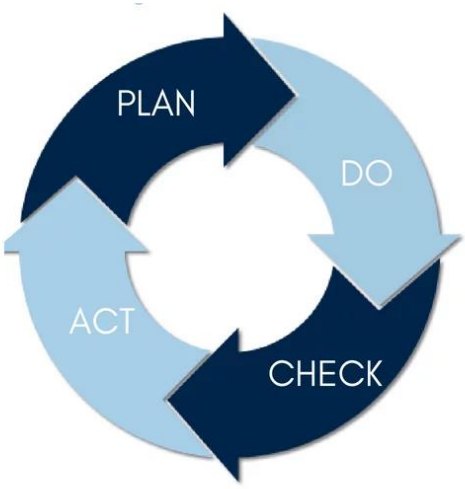


Figura 6 *Ciclo de Deming*
Fuente: Deming (2015)

Tabla 2 *:Descripción de las fases de Deming PDCA*

PLAN	**DO**
La planificación establece el alcance, políticas, objetivos, procesos y procedimientos del SGSI en términos de la organización, sus activos, tipo de tecnología a utilizar, se identifican los riesgos, amenazas y vulnerabilidades a los que se exponen los activos, y la asignación del propietario del SGSI.	Esta parte ejecuta el plan de tratamiento de riesgos para alcanzar los objetivos planteados, aquí se gestionan los recursos asignados al SGSI para el mantenimiento de la seguridad de la información implementando procedimientos y controles que permitan una detección y respuesta a los incidentes de seguridad.
CHECK	**ACT**

La verificación se ejecuta para detectar a tiempo errores, identificar brechas, detectar incidentes etc. Para garantizar que el modelo de seguridad funciona de acuerdo con lo previsto es necesario revisar regularmente la efectividad del SGSI atendiendo al cumplimiento de los objetivos planteados.	Realizar acciones preventivas y correctivas de acuerdo con las lecciones aprendidas de las experiencias propias y de otras organizaciones, comunicando las mismas a todas las partes implicadas en el SGSI, y plantear mejoras que alcancen los objetivos previstos.

Fuente: Deming (2020)

Dentro de este desarrollo de trabajo de titulación se abarcará la parte de la Gestión de Riesgos de la Seguridad de la Información, dicha gestión abarca en el proceso de **DO** (Hacer), dentro del modelo de Deming que ejecuta el plan de tratamiento de riesgos.

1.4.1 Gestión de riesgos de la seguridad de la información

Todas las organizaciones se enfrentan diariamente a riesgos de cualquier tipo donde la gestión de riesgos se define como la disciplina que existe para hacer frente a riesgos no especulativos, es decir aquellos riesgos que pueden ocasionar una pérdida para la organización. (Calder & Watkins, 2018)

Los responsables de la seguridad de la información son conscientes de la existencia de amenazas que suponen un peligro para la consecución de sus objetivos como se presenta en la figura 7, para esto dedican esfuerzos y recursos a mantener estos riesgos por debajo de un límite previamente consensuado en sus organizaciones. (Urbina, 2016)

Figura 7 *Objetivos de la Gestión de Riesgos*
Fuente: Arévalo & Moscoso (2017)

La gestión de riesgos aplica un ciclo del cual se debería seguir para que esta sea efectiva y puede desarrollarse sin ninguna novedad en el proceso (ISOTools, 2016). Dentro de este ciclo se encuentra aspectos que se detallan en la figura 8.

Figura 8 *Ciclo de la gestión de riesgos*
Fuente: Basel Institute on Governance Sucursal Perú (2017)

Estos aspectos se engloban a un solo punto de partida y de llegada que es la Dirección de la organización, sin el compromiso de esta no se podría llegar a realizar la gestión de riesgos de la seguridad de la información.

1.4.2 Tipos de riesgos de la seguridad de la información

En el mundo empresarial todas las actividades de administración giran en torno al procesamiento de diferentes datos sobre infraestructuras y sistemas que son utilizados todo el tiempo, en las organizaciones la información que se maneja es vital para el funcionamiento de la misma, por ello si se perdieran datos o si personas malintencionadas tuvieran acceso a ellos sería una catástrofe para dicha institución, debido a que el principal riesgo tecnológico es el de información, entonces se debe proteger este recurso aplicando opciones de seguridad. (Imbaquingo, Pusdá, & Jácome, 2017)

ISOTOOLS (2019) define al “riesgo como la probabilidad de sufrir daños o pérdidas” siendo el riesgo el nivel más simple dentro del proceso de gestión de riesgos que identifica y prioriza los peligros inherentes al desarrollo de un producto, sistema u organización.

Los riesgos se disminuyen con la implementación de salvaguardias, también conocidas como un mecanismo de protección frente a las amenazas, reduciendo la frecuencia de las amenazas y limitando el daño causado por estas (Castillo, Cisneros, Méndez, & Jácome, 2018); sin embargo

no es posible disminuir o atenuar todos los riesgos de forma completa debido al gran coste económico e incertidumbres que pueden surgir.

Riesgo Inherente

Es aquel existente por la naturaleza de la operación o actividad en ausencia de las acciones de la dirección para modificar su probabilidad e impacto Figura 9. (Cañas, 2019)

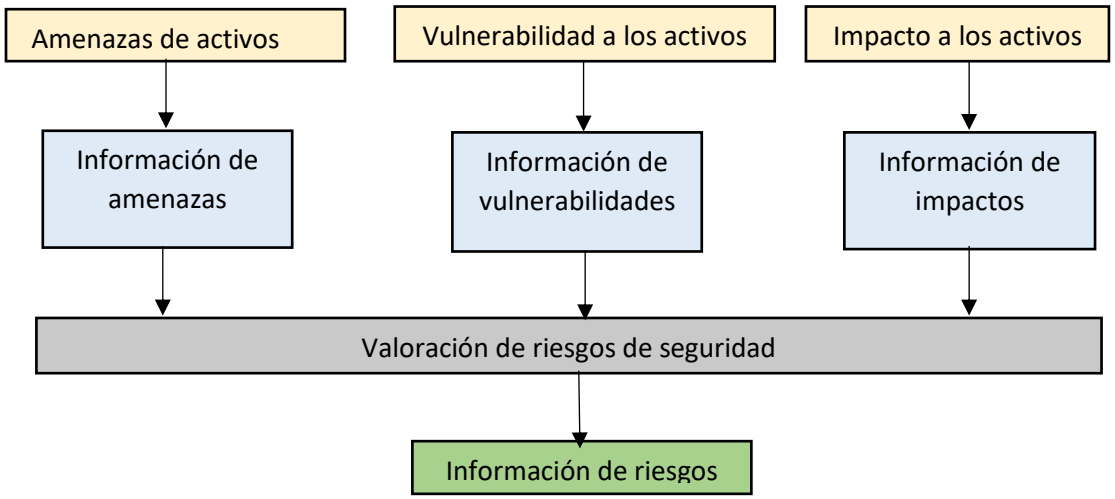


Figura 9 *Componentes del proceso de riesgos*
Fuente: Almeida (2017)

Cualquier actividad que el ser humano realice está expuesta a riesgos de diversa índole los cuales influyen de distinta forma en los resultados esperados. La capacidad de identificar estas probables eventualidades, su origen y posible impacto constituye ciertamente una tarea difícil pero necesaria para el logro de los objetivos. En el caso específico de cualquier empresa el desempeño depende de la gestión de los riesgos inherentes a su actividad siendo algunos de ellos de compleja identificación y de difícil medición. (Vanegas, 2016)

El riesgo inherente es propio del trabajo o proceso, que no puede ser eliminado, es decir, en todo trabajo o proceso se encontrarán riesgos para las personas o para la ejecución de la actividad en sí misma, su cálculo se presenta en la Figura 10.

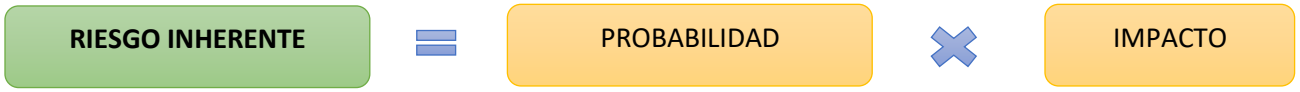


Figura 10 *Cálculo del Riesgo Inherente*
Fuente: Deloitte (2019)

Riesgo Residual

Según (Da Cunha, 2016), el riesgo residual es el riesgo existente después de la implementación de medidas de seguridad; es decir que después de hacer todo el tratamiento del riesgo, aún existe esa exposición o peligro a dicho riesgo el cual deberá ser asumido y vigilado.

Otra definición que se puede encontrar según la NTC 5254 es el “nivel resultante del riesgo después de que se han tomado medidas de tratamiento de riesgo” para lo cual la aprobación del plan de tratamiento de riesgos y la aceptación de los riesgos residuales de seguridad de la información es por parte de los dueños de los riesgos, es decir la organización encabezada por la Alta Dirección.

Finalmente, se calcula el “riesgo neto o residual”, que resulta de la relación entre el grado de manifestación de los riesgos inherentes y la gestión de mitigación de riesgos establecida por la administración. A partir del análisis y determinación del riesgo residual los administradores pueden tomar decisiones como la de continuar o abandonar la actividad dependiendo del nivel de riesgos; fortalecer controles o implantar nuevos controles. Esta decisión está delimitada a un análisis de costo beneficio y riesgo (Vanegas, 2016), su cálculo se describe en la Figura 11.

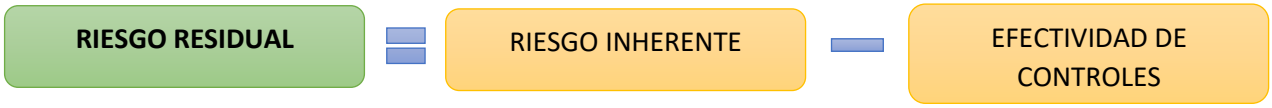


Figura 11 *Cálculo del Riesgo Residual*
Fuente: Deloitte (2019)

1.4.3 Análisis de riesgos

“El análisis de riesgos es conocido como el proceso sistemático para estimar la magnitud de los riesgos a los que está expuesta una organización y permite determinar la naturaleza, el costo y la protección que tiene un sistema” (Arévalo & Moscoso, 2017, p. 33). El análisis de riesgos busca establecer la probabilidad de ocurrencia de los riesgos y el impacto de sus consecuencias, calificándolos y evaluándolos con el fin de obtener información para establecer el nivel de riesgo y las acciones que se van a implementar.(Morales, 2019)

Dentro de este análisis se identifica los riesgos existentes para después proponer contramedidas o las llamadas salvaguardias que junto a controles y medidas de seguridad se pueda llegar a cumplir los objetivos de la organización. (Arévalo & Moscoso, 2017)

Los riesgos se encuentran divididos por zonas y colores los cuales se detallan en la Figura 12.

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

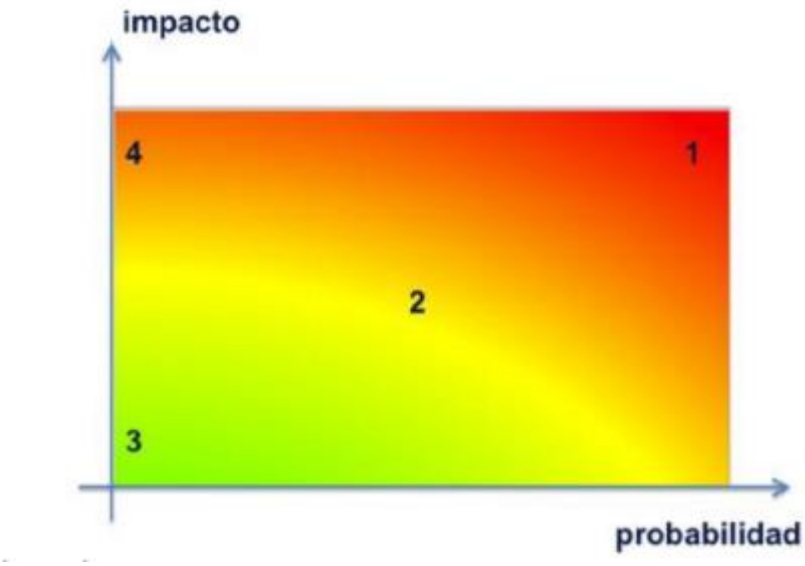


Figura 12 *Zonas de riesgos*
Fuente: Almeida (2017)

A continuación, se describen los principales elementos para tener en cuenta en el proceso de gestión de riesgos.

Activo

Según la ISO 27001:2013 activo es “un componente o funcionalidad de un sistema de información susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización. Incluye: información, datos, servicios, aplicaciones (software), equipos (hardware), comunicaciones, recursos administrativos, recursos físicos y recursos humanos.” es decir es cualquier cosa que tenga valor para la organización.

Tabla 3: *Ejemplo de activos en una Organización*

Activo	
Activos materiales	**Activos Intangibles**
Equipos informáticos	Aplicaciones informáticas
Servidores físicos	Gestores de copias de seguridad
Equipos red local	Sistemas operativos
Periféricos y pendrives	Comunicaciones
Portátiles, tabletas y móviles	Gestores de bases de datos
Oficinas e instalaciones	Suministros
Personal propio	

Fuente: Propia

Amenaza

Según la UNE 71504:2008 es la “causa potencial de un incidente que puede causar daños a un sistema de información o a una organización”. Las amenazas son “cosas que ocurren”. Y, de todo lo que puede ocurrir, interesa lo que puede pasarle a nuestros activos y causar un daño.(MAGERIT, 2019)

Las amenazas afectan directamente a las propiedades de la información: integridad, disponibilidad, confidencialidad y autenticidad. (Imbaquingo, Pusdá, & Jácome, 2017)

Vulnerabilidad

Se denomina vulnerabilidad a toda debilidad que puede ser aprovechada por una amenaza, o más detalladamente a las debilidades de los activos o de sus medidas de protección que facilitan el éxito de una amenaza potencial. Las vulnerabilidades son debilidades asociadas a los activos de una organización, estas debilidades pueden ser explotadas por una amenaza causando incidentes no deseados que pueden resultar en pérdida o daño de estos activos. (MAGERIT, 2019)

Control atenuante

Son aquellos activos y medidas que consiguen reducir las posibilidades de amenazas y, por tanto, el nivel de riesgo del sistema tecnológico de la organización. (Imbaquingo, Pusdá, & Jácome, 2017)

Impacto

Es la medida del daño sobre el activo derivado de la materialización de una amenaza. Conociendo el valor de los activos (en varias dimensiones) y la degradación que causan las amenazas, es directo derivar el impacto que estas tendrían sobre el sistema. (MAGERIT, 2019)

Tabla 4 *:Impacto acumulado e Impacto repercutido*

Impacto Acumulado	Impacto Repercutido
Es el calculado sobre un activo teniendo en cuenta: • Su valor acumulado (el propio más el acumulado de los activos que dependen de él) • Las amenazas a que está expuesto. - El impacto acumulado se calcula para cada activo, por cada amenaza y en cada dimensión de valoración, siendo una función del valor acumulado y de la degradación causada. - El impacto es tanto mayor cuanto mayor es el valor propio o acumulado sobre un activo y también cuando sea la degradación del activo atacado. - El impacto acumulado, al calcularse sobre los activos que soportan el peso del sistema de información, permite determinar las salvaguardas de que hay que dotar a los medios de trabajo.	Es el calculado sobre un activo teniendo en cuenta: • Su valor propio. • Las amenazas a que están expuestos los activos de los que depende. - El impacto repercutido se calcula para cada activo, por cada amenaza y en cada dimensión de valoración, siendo una función del valor propio y de la degradación causada. - El impacto es tanto mayor cuanto mayor es el valor propio de un activo y también cuando sea la degradación del activo atacado. - El impacto repercutido, al calcularse sobre los activos que tienen valor propio, permite determinar las consecuencias de las incidencias técnicas sobre la misión del sistema de información.

Fuente: Magerit (2019)

Probabilidad

Es la posibilidad de ocurrencia de un hecho, suceso o acontecimiento. La frecuencia de ocurrencia implícita se corresponde con la amenaza Figura 13. Para estimar la frecuencia se puede considerar datos empíricos (datos objetivos) del histórico de una empresa, o en opiniones de expertos o del empresario (datos subjetivos). (INCIBE, 2015)

Figura 13. *Activo, amenaza, vulnerabilidad e impacto*
Fuente: INCIBE (2019)

1.5 Metodologías para la gestión de riesgos de la seguridad de la información

La implantación de sistemas de gestión de riesgos, comenzó a tomar relevancia desde la década de los noventas, período en que fue necesario reconvertir y replantear la forma de hacer negocios, como consecuencia de la ocurrencia de fraudes a importantes entidades, perdiendo la confianza del público en general; su impacto a nivel mundial desencadenó una serie de medidas que conlleva a mejores prácticas, tendientes a evitar fraudes de cualquier naturaleza; se emitieron sendos documentos técnicos y en algunos países, consideraron emitir leyes. (ISOTools, 2016)

Las metodologías para la gestión de los riesgos usadas a nivel mundial coinciden en que el empleo de estas de forma planificada a través de un proceso formal, fortalecen las operaciones y procesos de las entidades, independientemente del tamaño o actividad empresarial. (Cañas, 2019)

Una metodología de análisis y gestión de riesgos sigue un proceso sistemático para estimar la magnitud de los riesgos a los que se encuentra expuesta una organización, seleccionando e implantando salvaguardas para conocer, prevenir, impedir, reducir o controlar los riesgos identificados. (Mariño, 2017)

Ealde Business School en una publicación del año 2016 llamada Metodologías en Gestión de Riesgos indica que “Las compañías pueden adoptar diferentes posturas y seguir distintas metodologías en relación con el Risk Management. Algunas de las metodologías en gestión de riesgos más destacadas internacionalmente son:”

1.5.1 MAGERIT

Siguiendo la terminología de la normativa ISO 31000, Magerit responde a lo que se denomina "Proceso de Gestión de los Riesgos", sección 4.4 ("Implementación de la Gestión de los Riesgos") dentro del "Marco de Gestión de Riesgos" Figura 14. En otras palabras, MAGERIT implementa el Proceso de Gestión de Riesgos dentro de un marco de trabajo para que los órganos de gobierno tomen decisiones teniendo en cuenta los riesgos derivados del uso de tecnologías de la información.

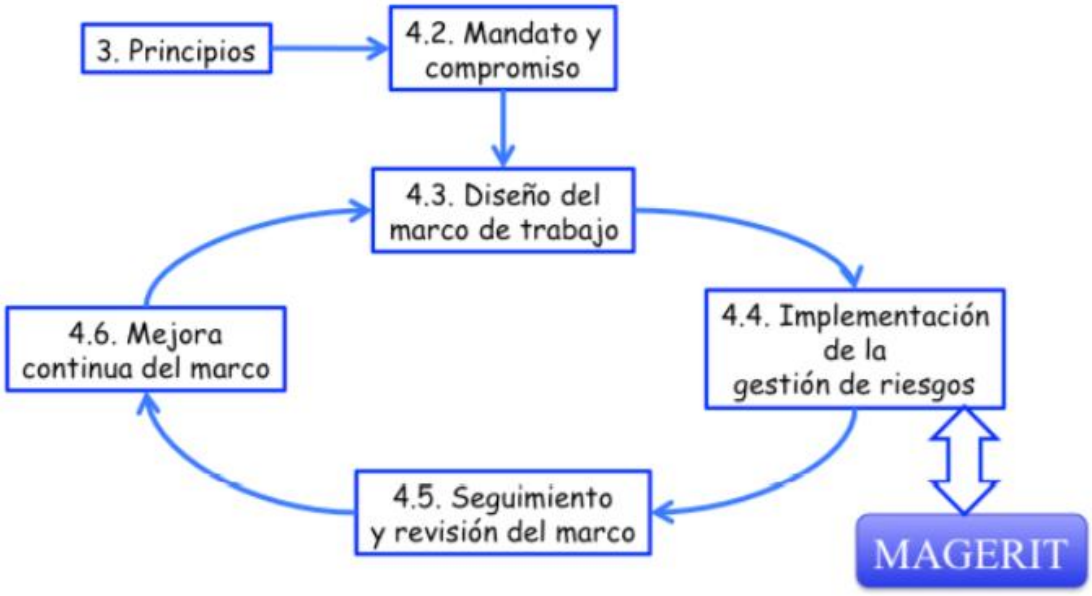


Figura 14 *Marco de trabajo para la gestión de riesgos*
Fuente: ISO 31000

Magerit V3.0 persigue los siguientes objetivos:

- Directos
    a. Concienciar a los responsables de las organizaciones de información de la existencia de riesgos y de la necesidad de gestionarlos.
    b. Ofrecer un método sistemático para analizar los riesgos derivados del uso de tecnologías de la información y comunicaciones (TIC).
    c. Ayudar a descubrir y planificar el tratamiento oportuno para mantener los riesgos bajo control.
- Indirectos

a. Preparar a la Organización para procesos de evaluación, auditoría, certificación o acreditación, según corresponda en cada caso.

Las actividades para el análisis de riesgos que se realizan con esta metodología son las siguientes:

***Tabla 5**:Formalización de actividades Magerit*

MAR - Método de Análisis de Riesgos
MAR.1 Caracterización de los activos
MAR.11 – Identificación de activos
MAR.12 – Dependencias entre activos
MAR.13 – Valoración de los activos
MAR.2 Caracterización de las amenazas
MAR.21 – Identificación de las amenazas
MAR.22 – Valoración de las amenazas
MAR.3 Caracterización de las salvaguardas
MAR.31 – Identificación de las salvaguardas pertinentes
MAR.32 – Valoración de las salvaguardas
MAR.4 Estimación de riesgo
MAR.41 – Estimación de impacto
MAR.42 – Estimación del riesgo

Fuente: Magerit (2019)

- **Proceso de Gestión de Riesgos de MAGERIT**

Según (Magerit, 2019) nos detalla el proceso de la siguiente manera.

A la vista de los impactos y riesgos a que está expuesto el sistema, hay que tomar una serie de decisiones condicionadas por diversos factores:

- La gravedad del impacto y/o del riesgo.
- Las obligaciones a las que por ley esté sometida la Organización.
- Las obligaciones a las que por reglamentos sectoriales esté sometida la Organización.
- Las obligaciones a las que por contrato esté sometida la Organización.

Dentro del margen de maniobra que permita este marco, pueden aparecer consideraciones adicionales sobre la capacidad de la Organización para aceptar ciertos impactos de naturaleza intangible tales como:

- Imagen pública de cara a la Sociedad (aspectos reputacionales)

- Política interna: relaciones con los propios empleados, tales como capacidad de contratar al personal idóneo, capacidad de retener a los mejores, capacidad de soportar rotaciones de personas, capacidad de ofrecer una carrera profesional atractiva, etc. • relaciones con los proveedores, tales como capacidad de llegar a acuerdos ventajosos a corto, medio o largo plazo, capacidad de obtener trato prioritario, etc.
- Relaciones con los clientes o usuarios, tales como capacidad de retención, capacidad de incrementar la oferta, capacidad de diferenciarse frente a la competencia, ... • relaciones con otras organizaciones, tales como capacidad de alcanzar acuerdos estratégicos, alianzas, etc.
- Nuevas oportunidades de negocio, tales como formas de recuperar la inversión en seguridad
- Acceso a sellos o calificaciones reconocidas de seguridad.

Todas las consideraciones anteriores desembocan en una calificación de cada riesgo significativo, determinándose si:

1. Es crítico en el sentido de que requiere atención urgente.
2. Es grave en el sentido de que requiere atención.
3. Es apreciable en el sentido de que pueda ser objeto de estudio para su tratamiento.
4. Es asumible en el sentido de que no se van a tomar acciones para atajarlo.

La opción 4, aceptación del riesgo, siempre es arriesgada y hay que tomarla con prudencia y justificación. Las razones que pueden llevar a esta aceptación son:

- Cuando el impacto residual es asumible.
- Cuando el riesgo residual es asumible.
- Cuando el coste de las salvaguardas oportunas es desproporcionado en comparación al impacto y riesgo residuales.

La calificación de los riesgos tendrá consecuencias en las tareas subsiguientes, siendo un factor básico para establecer la prioridad relativa de las diferentes actuaciones.

1.5.2 Norma ISO/IEC 27005:2018

La norma “ICONTEC NTC-ISO/IEC 27005:2018 tecnología de la información, técnicas de seguridad, gestión del riesgo de seguridad de la información” fue publicada en julio de 2008 y presenta las directrices para la gerencia del riesgo de seguridad de información. Emplea los

conceptos de norma ISO 27001:2018, que especifica los requisitos de sistemas de gestión de la seguridad de la información. (Kowask Bezerra, Alcántara Lima, Motta, & Piccolini, 2016)

Según la Norma (ISO 27005,2018) describe todo el proceso necesario para la gestión del riesgo de seguridad de la información y las actividades necesarias para la perfecta ejecución de la gestión como se detalla en la (Figura 15). Presenta prácticas para gestión del riesgo de la seguridad de la información. Las técnicas en ella descritas siguen el concepto, los modelos y los procesos globales especificados en la norma ISO/IEC 27001, además de presentar la metodología de evaluación y tratamiento de los riesgos requeridos por la misma norma y estructurada de la siguiente manera:

- La información de fondo se proporciona en la Cláusula 5.
- En la cláusula 6 se ofrece una visión general del proceso de gestión de riesgos de seguridad de la información.
- Todas las actividades de gestión de riesgos de seguridad de la información que se presentan en la Cláusula 6 se describen posteriormente en las siguientes cláusulas:

- Establecimiento de contexto en la Cláusula 7;
- Evaluación de riesgos en la Cláusula 8;
- Tratamiento de riesgo en la Cláusula 9;
- Aceptación del riesgo en la Cláusula 10;
- Aceptación del riesgo en la Cláusula 10;
- Comunicación de riesgos en la Cláusula 11;
- Monitoreo y revisión de riesgos en la Cláusula 12.

En los anexos se presenta información adicional para las actividades de gestión de riesgos de seguridad de la información. El establecimiento del contexto está respaldado por el Anexo A (que define el alcance y los límites del proceso de gestión de riesgos de seguridad de la información). La identificación y valoración de los activos y las evaluaciones de impacto se analizan en el Anexo B. El Anexo C proporciona ejemplos de amenazas típicas y el Anexo D discute vulnerabilidades y métodos para la evaluación de vulnerabilidades. En el Anexo E se presentan ejemplos de enfoques de evaluación de riesgos de seguridad de la información.

- Las restricciones para la modificación del riesgo se presentan en el Anexo F.

- Todas las actividades de gestión de riesgos presentadas en la Cláusula 7 a la Cláusula 12 están estructuradas de la siguiente manera:

Entrada: identifica cualquier información requerida para realizar la actividad.

Acción: describe la actividad.

Guía de implementación: proporciona orientación sobre la realización de la acción. Parte de esta guía puede no ser adecuada en todos los casos, por lo que otras formas de realizar la acción pueden ser más apropiadas.

Salida: identifica cualquier información derivada después de realizar la actividad.

Figura 15 *ISO 27005*
Fuente: ISO 27005 (2018)

CAPITULO II

DESARROLLO

2.1 Comparación de Metodologías

Ealde Business School en el 2020 realizó una publicación la que indica las metodologías más usadas en relación con el Risk Management dentro del ámbito empresarial y destacadas internacionalmente para la Gestión de Riesgos como son Magerit y la ISO 27005. (Ealde Business School, 2020)

Como se explica en el capítulo I se escogió dos metodologías para realizar la comparativa respectiva como detalla en la figura 16.

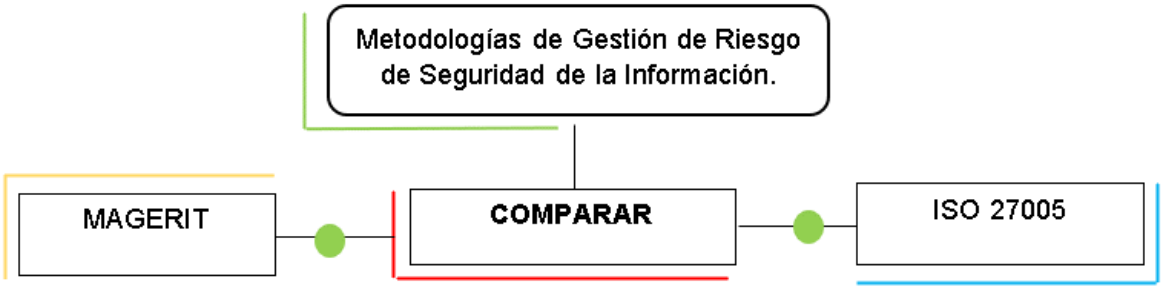


Figura 16 Comparativa de metodologías
Fuente: Propia

2.2 Método DELPHI

El método Delphi consiste en una técnica de obtención de información, basada en la consulta a expertos de un área, con el fin de obtener la opinión de consenso más fiable del grupo consultado. Estos expertos son sometidos individualmente a una serie de cuestionarios en profundidad que se intercalan con retroalimentación de lo expresado por el grupo y que, partiendo de una exploración abierta, tras las sucesivas devoluciones, producen una opinión que representa al grupo.(Torrado-Fonseca, 2016)

Desde un punto de vista metodológico, el método Delphi es una estrategia relativamente flexible que nos ha permitido actuar con autonomía y adaptar su dinámica habitual a los objetivos de nuestra investigación. El punto de partida para la puesta en marcha de esta estrategia Delphi ha sido la existencia de un problema de investigación que requeriría de la opinión de un grupo de expertos cuyos conocimientos sobre el tema, características y experiencia se estimaron a priori como apropiados para la consecución de los objetivos de nuestra investigación. (Llorente Pozo, Pérez Gutiérrez, 2017)

La siguiente información es tomada del artículo ´´El Método Delphi escrito por Mercedes Reguant-Álvarez y Mercedes Torrado-Fonseca y publicado en el 2016 en la Revista Reire (Revista d´Innovació i Recerca en Educació) de la Universidad de Barcelona.

2.2.1 Fases del proceso

Como cualquier técnica, su uso esta pausado por varias fases, tal como se presenta en la figura 17.

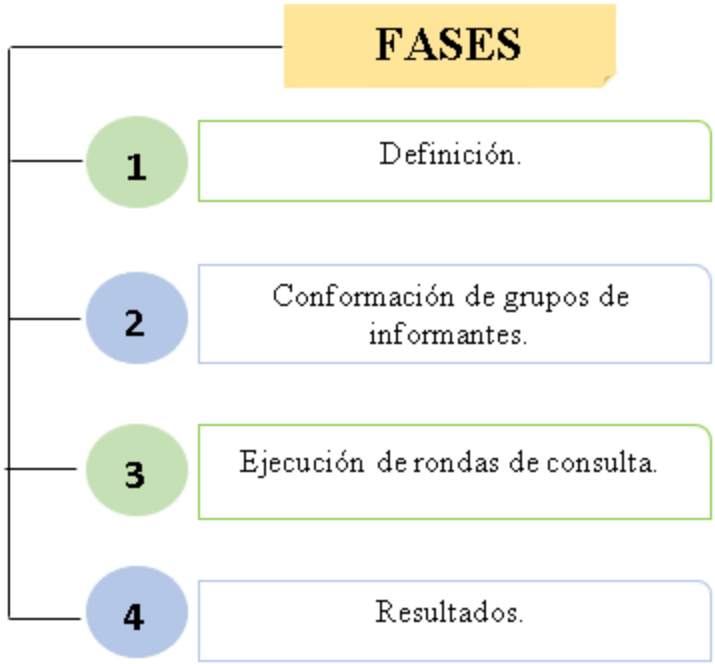


Figura 17 Fases del proceso de Delphi
Fuente: Torrado Fonseca, Reguant Álvarez

2.2.1.1 Fase 1 de definición

A partir del problema de investigación acotado, se debe formular el objetivo de la consulta, identificar las dimensiones de acuerdo con las necesidades que deben explorarse e identificar posibles fuentes de información. (Torrado-Fonseca, 2016)

Teniendo en cuenta que el problema de investigación de este tema de titulación es **"Altos riesgos informáticos que afectan la seguridad de la información"** se obtiene un objetivo el cuál es:

- Realizar comparativa entre dos metodologías de gestión de riesgos de seguridad de la información.

Basados ya nuestro objetivo identificamos los criterios que se deben explorar basados en la realidad que tiene el autor de este trabajo que es la falta de experiencia, práctica y que es por primera vez que efectúa una Gestión de Riesgos y siendo una realidad de muchas otras personas, para poder solventar que no solo es la realidad del autor de este trabajo se realizó una encuesta en busca de los criterios que debería tener una metodología para ser aplicada, dicha encuesta se la realizó a un grupo de 74 personas que son alumnos de la materia de Evaluación y Auditoría de la Carrera de Ingeniería en Sistemas Computacionales, dentro de dicha encuesta se preguntó “Qué criterios buscaría en una metodología de Gestión de Riesgos de la Seguridad de la Información para ser aplicada?” y los criterios a escoger son los que se detalla en la figura 18.

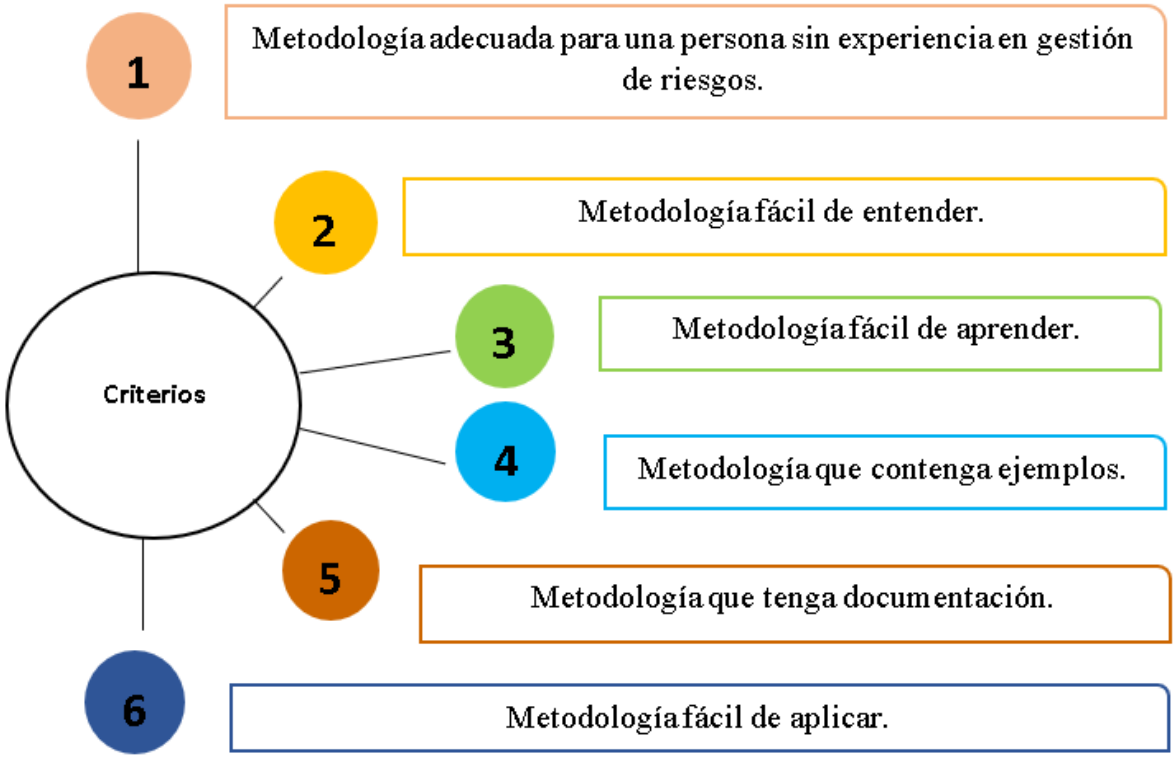


Figura 18 Dimensiones a explorar
Fuente: Propia

Ya con las dimensiones a tomar en cuenta, realizamos la encuesta y los resultados obtenidos son los que se detalla en la figura 19.

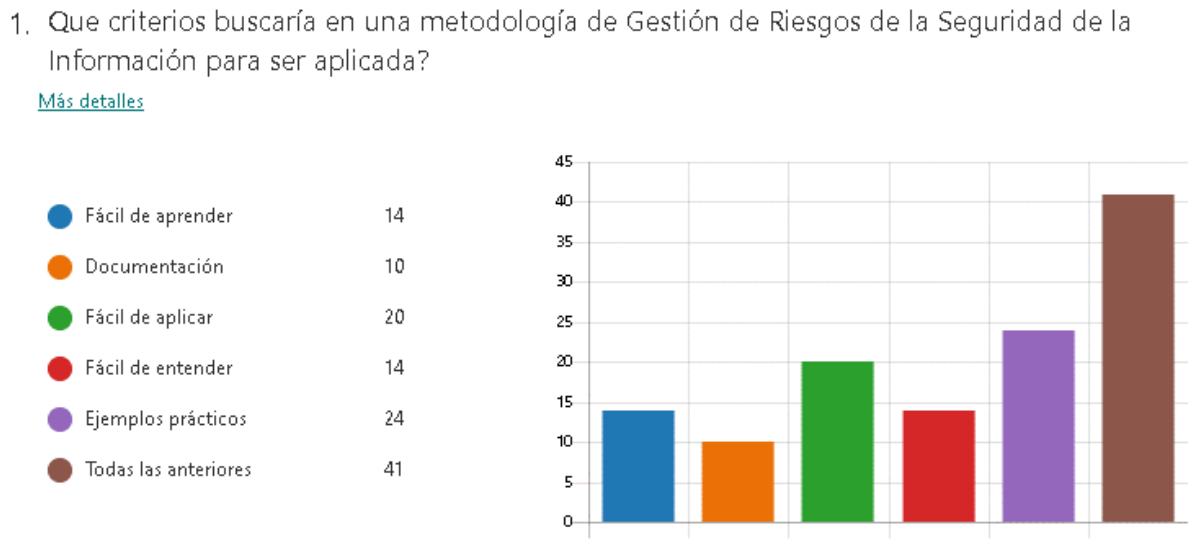


Figura 19 Resultados de encuesta
Fuente: Propia

Los resultados afirman que los criterios que debe tener una metodología en una persona que no tiene experiencia y que está empezando en esta área son los que se observa en la figura 19 siendo la respuesta más votada la opción de “Todas las anteriores”.

Una vez obtenido los criterios, identificamos las fuentes de información que son:

- Expertos en Gestión de Riesgos de Seguridad de la Información.
- Magerit.
- ISO 27005.

2.2.1.2 Fase 2 de conformación de grupos de informantes

La información de esta fase 2 de conformación de informantes es tomada del artículo The Delphi method as a research tool: an example, design considerations and applications escrito por Chitu Okoli , Suzanne D. Pawlowski y publicado en el año 2004.

Proporcionar pautas detalladas sobre como seleccionar expertos calificados es un procedimiento riguroso cuyo propósito es asegurar la identificación de estos y que tengan un conocimiento profundo de los temas especificados en las dimensiones de la figura 18. (Okoli & Pawlowski, 2004)

Chiut Okoli y Suzanne D. Pawlowski (2004) indica que para identificar a los expertos se preparó una hoja de trabajo de nominación de recursos de conocimiento (KRNW), el propósito de la hoja de trabajo es ayudar a categorizarlos antes de seleccionarlos, es muy importante no

escribir ningún nombre especifico de los participantes. Esta hoja de trabajo se divide en 4 pasos que son:

Paso 1: Identificar las disciplinas, organizaciones y literatura.

Dividimos a los expertos en paneles que constituyen 4 áreas generales con las que trabaja la organización brindando sus servicios, las cuáles se detallan en la tabla 6.

Tabla 6 Hoja de trabajo KRNW

Disciplina	Organizaciones	Literatura
Académica	Banca	SGSI
Seguridad de la información	Gobierno	ISO 27001
Gestión de Riesgos	Empresa privada	Magerit
	Organizaciones sociales	

Fuente: (Okoli & Pawlowski, 2004)

Esta clasificación se la realiza con el objetivo de tener perspectivas diferentes, dado que el objetivo es obtener un grado razonable de consenso. Esta clasificación también permite comparar las perspectivas de los diferentes grupos de interés.

Paso 2: Escriba los nombres de personas de la disciplina, organización y literatura.

En este paso se detalla la tabla 7 y se omite los nombres de cada experto en las áreas de la tabla 6 debido a la confidencialidad que nos exige el método Delphi.

Tabla 7 Descripción de KRNW

Disciplina	Organizaciones	Literatura
Académica	**Banca**	**SGSI**
Profesores de grado y postgrados a nivel nacional	Experto que trabaje dentro de la banca	Publicaciones sobre SGSI
Seguridad de la información	**Gobierno**	**ISO 27001**
		Publicaciones sobre ISO 27001

Expertos certificados y con amplia experiencia	Experto que trabaje en una entidad de gobierno	
Gestión de Riesgos	**Empresa privada**	**Magerit**
Expertos certificados y con amplia experiencia	Experto que sea dueño o trabaje en la empresa privada	Publicaciones sobre Magerit
	Organizaciones sociales	
	Miembros de alguna organización social en ciberseguridad	

Fuente: (Okoli & Pawlowski, 2004)

Paso 3: Nominar a expertos adicionales

Se hace el contacto en primera instancia con los expertos definidos en un inicio para que ellos nominen a otros, este paso fue omitido por cuestiones de disponibilidad de tiempo de los expertos que se cuenta actualmente.

Paso 4: Clasificación de los expertos

Teniendo en cuenta los perfiles de la tabla 7 se escogió a 5 profesionales que cumplen con los requisitos, cabe recalcar que durante todo el proceso se ha garantizado el **anonimato de los participantes**.

2.2.1.3 Fase 3 de ejecución de rondas a consultar

Para poder determinar un cuestionario se debe conocer las fases que cuenta cada metodología, para esto se realizó un análisis de estas teniendo en cuenta las partes que definen cada una de sus fases, en la tabla 8 observamos como se divide Magerit.

Tabla 8 Fases de Magerit

MAGERIT	
FASE I: Planificación	Roles y funciones Contexto Criterios para la evaluación del riesgo
FASE II: Ejecución	**Análisis/Evaluación de los riesgos** **Caracterización de los activos** Identificación de los activos Dependencias entre activos Valoración de los activos **Caracterización de las amenazas** Identificación de amenazas Valoración de las amenazas **Caracterización de las salvaguardas** Identificación de las salvaguardas pertinentes Valoración de las salvaguardas **Estimación del estado de riesgo** Estimación del impacto Estimación del riesgo **Decisión de tratamiento** Eliminación Mitigación Compartición Financiación
FASE III: Finalización	Comunicación y consulta Seguimiento y revisión Documentación

Fuente: Propia

El mismo análisis se lo realizó para la ISO 27005 en la tabla 9 podemos observar las partes que definen cada una de las fases dentro de esta metodología.

Tabla 9 Fases de ISO 27005

ISO 27005	
FASE I: Planificación	Contexto Alcance y límites Criterios para la evaluación del riesgo
FASE II: Ejecución	**Análisis/Evaluación de los riesgos** ***Identificación del riesgo*** Identificación de activos

	Identificación de activos primarios Identificación de activos de soporte e infraestructura Identificación de amenazas Identificación de controles existentes Identificación de vulnerabilidades Identificación de las consecuencias ***Análisis del riesgo*** Evaluación de las consecuencias Evaluación de la probabilidad Determinación del nivel del riesgo ***Evaluación del riesgo*** Lista de riesgos con los niveles de valores y criterios Comparación del nivel de riesgo Lista de riesgos ordenados por priorización **Tratamiento y aceptación del riesgo** Modificación del riesgo Retención del riesgo Acción de evitar el riesgo Compartir el riesgo Aceptación del riesgo
FASE III: Finalización	Comunicación y consulta Monitoreo y análisis de los factores de riesgo Monitoreo, análisis crítico y mejoramiento del proceso de la gestión de riesgo Documentación

Fuente: Propia

Basados en las tablas de las dos metodologías se realizó un cuestionario de preguntas enfocadas a los puntos más importantes y relevantes que cuentan cada una de las metodologías, las preguntas se detallan en la tabla 10.

Tabla 10 Preguntas para expertos

Pregunta 1	¿Entre Magerit y la ISO 27005 cuál considera es la metodología más apropiada para una persona que desea implementar por primera vez una Gestión de Riesgos de Seguridad de la Información?
Pregunta 2	Al momento de definir los criterios de evaluación del riesgo considerando Magerit e ISO 27005 ¿Cuál metodología ofrece las mejores consideraciones para evaluar los riesgos de seguridad de la información y por qué?

Pregunta 3	¿De acuerdo con su experticia en el manejo de metodologías de evaluación de riesgos de seguridad de la información, que metodología le ayuda a identificar de manera más acertada activos de información?
Pregunta 4	¿Cuándo se aplica la definición de las amenazas que afectan a un activo, cuál considera la metodología más adecuada entre ISO 27005 y Magerit?
Pregunta 5	¿Cuál metodología entre ISO 27005 y Magerit considera usted explica de manera más clara la forma de valoración de amenazas?
Pregunta 6	¿Cuál metodología entre ISO 27005 y Magerit cuenta con un proceso más claro para la identificación de controles existentes?
Pregunta 7	¿En su experiencia que metodología cree usted que explica de manera más detallada el proceso de tratamiento de riesgos de Seguridad de la Información?
Pregunta 8	¿Desde su experiencia profesional si debiese recomendar una metodología para la Gestión de Riesgos de Seguridad de la Información para que aplique una persona sin experiencia cuál sería entre ISO 27005 y Magerit? Elija solo una.
Pregunta 9	¿Qué criterios cree usted que cuenta Magerit?
Pregunta 10	¿Qué criterios cree usted que cuenta ISO 27005?

Fuente: Propia

2.2.1.4 Fase 4 de resultados

Se analiza la información obtenida por parte de los expertos en la tabla 11 y se deja claro que hubo respuesta y retroalimentación de estas en el transcurso de las entrevistas a cada uno de los participantes.

Tabla 11 Respuestas de la entrevista

	Pregunta 1	Pregunta 2	Pregunta 3	Pregunta 4	Pregunta 5	Pregunta 6	Pregunta 7	Pregunta 8	Pregunta 9	Pregunta 10
Experto 1	ISO 27005	MAGERIT	MAGERIT	MAGERIT	ISO 27005	ISO 27005	MAGERIT	ISO 27005	Documentación Ejemplos Facilidad de aprendizaje	Facilidad de aplicación Facilidad de aprendizaje Facilidad de entender Ejemplos
Experto 2	ISO 27005	MAGERIT	MAGERIT	MAGERIT	MAGERIT	NINGUNA	MAGERIT	ISO 27005	Automatización Ejemplos Documentación Facilidad de aprendizaje	Facilidad de aplicación Facilidad de aprendizaje Fácil de enseñar Fácil de entender
Experto 3	MAGERIT	NINGUNA	MAGERIT	MAGERIT	MAGERIT	NINGUNA	NINGUNA	ISO 27005	Automatización Ejemplos Fácil de entender Documentación	Facilidad de aplicación Facilidad de aprendizaje Automatización Documentación
Experto 4	MAGERIT	ISO 27005	ISO 27005	ISO 27005	ISO 27005	ISO 27005	ISO 27005	ISO 27005	Aplicado para Pymes Fácil de aplicar Fácil de entender Documentación	Fácil de enseñar Fácil de entender Ejemplos
Experto 5	ISO 27005	MAGERIT	ISO 27005	ISO 27005	ISO 27005	ISO 27005	MAGERIT	ISO 27005	Facilidad de aplicación Fácil de entender Ejemplos Aplicado a Pymes	Facilidad de aprendizaje Automatización Aplicado a Pymes Fácil de entender Fácil de enseñar Documentación
	ISO 27005	MAGERIT	MAGERIT	MAGERIT	ISO 27005	ISO 27005	MAGERIT	ISO 27005		

Fuente: Propia

Obtenidas las respuestas por parte de los entrevistados se obtiene el siguiente resultado por preguntas cerradas que comprende desde la pregunta 1 a la 8 como se detalla en la figura 20.

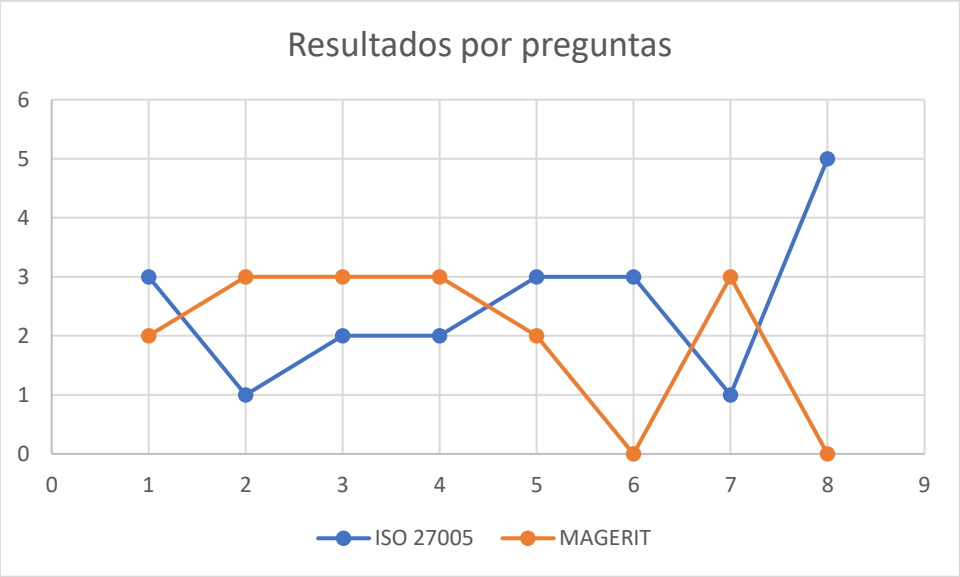


Figura 20 Resultados por preguntas cerradas
Fuente: Propia

Teniendo en cuenta los resultados individuales por preguntas cerradas se hace un resultado general en donde se obtiene un empate como se detalla en la figura 21.

Figura 21 Resultado general
Fuente: Propia

Una vez observado los resultados y el empate que se generó entre ISO 27005 y MAGERIT en las preguntas de la 1 a la 8, la manera de escoger la metodología a aplicarse es con las preguntas 9 y 10 del cuestionario, en las cuales cada experto escoge criterios dando su punto de vista y su explicación de porque escoge los diferentes aspectos que a su consideración tiene cada una de las metodologías nombradas para este caso de estudio.

Los criterios que escogieron los entrevistados en cada una de las metodologías de estudio deben ser las mismas en su mayoría a las dimensiones expuestas en la fase 1 de definición, para esto se escogerá a las que más nombran en cada una para poder comparar.

En la tabla 12 se detalla los criterios que más se repite por cada entrevistado en cada una de las metodologías.

Tabla 12 Criterios en común

MAGERIT	ISO 27005
- Documentación	- Fácil de aplicación
- Ejemplos	- Fácil de aprendizaje
- Fácil de entender	- Fácil de entender
- Facilidad de aprendizaje	- Fácil de enseñar

Fuente: Propia

Se hace una comparación en donde se tiene los criterios que se busca en una metodología y los que cuenta cada una de ellas según los entrevistados, se hace de manera cualitativa en donde si la metodología cuenta con el criterio en mención obtendrá un sí y en el caso que no cuente obtendrá un no como se detalla en la tabla 13.

Tabla 13 Comparativa de criterios

Criterios en búsqueda	ISO 27005	MAGERIT
Metodología adecuada para una persona sin experiencia en gestión de riesgos de seguridad de la información.	1	1
Metodología fácil de entender.	1	1
Metodología fácil de aprender.	1	1
Metodología que contenga ejemplos.	0	1

Metodología que tenga documentación.	0	1
Metodología fácil de aplicar	1	0
TOTAL	**4**	**5**

Fuente: Propia

Teniendo en cuenta los resultados de la comparación de los criterios obtenemos la ISO 27005 con un puntaje de 4 y a MAGERIT con un puntaje de 5, basado en estos resultados, la metodología seleccionada para la respectiva aplicación es Magerit de acuerdo con los criterios expuestos por los entrevistados.

CAPITULO III

Aplicación de la metodología de análisis de riesgos

3.1 PILAR

Para esta aplicación se usó la herramienta llamada P.I.L.A.R, es acrónimo de “Procedimiento Informático-Lógico para el Análisis de Riesgos” es una herramienta desarrollada por el Centro Nacional de Inteligencia para soportar el Análisis de Riesgos de Sistemas de Información basado en la metodología Magerit y financiado parcialmente por el Centro Criptológico Nacional de España. (CCN-CERT, 2020)

En esta herramienta se puede hacer todas las actividades que se realizan en el Análisis y Gestión de Riesgos:

Determinación de activos: Identificación, dependencias y valoración.

Determinación de amenazas.

Estimación de impactos.

Determinación de los criterios de aceptación del riesgo.

Determinación de las medidas de seguridad necesarias o Salvaguardas.

Este software permite hacer un Análisis sobre las dimensiones de valoración como son: confidencialidad, disponibilidad, autenticidad y trazabilidad.

Además nos ayuda con el cálculo del impacto y el riesgo, acumulado, repercutido, potencial y residual. Este tema de titulación se lo realizó con un análisis cualitativo.

En la figura 22 se detalla la Herramienta Pilar en su versión 7.4.5.

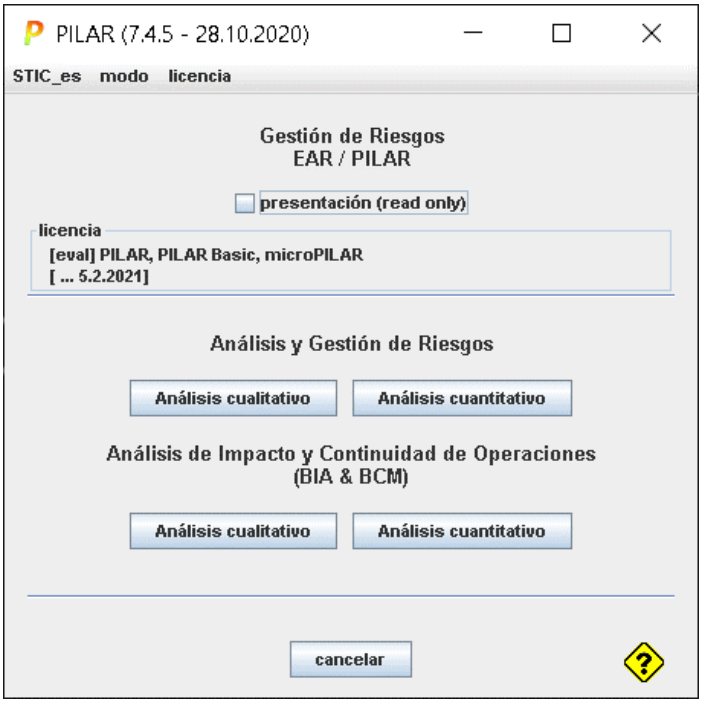


Figura 22 PILAR
Fuente: Pilar 7.4.5

Antes de formalizar las actividades establecidas en la tabla 5 se definió algunos aspectos que nos dice Magerit como son:

3.2 Roles y funciones

Dentro de la Gestión de riesgos hay que definir roles y funciones los cuales van a estar siendo responsables de que se cumpla las actividades, la matriz de la asignación de responsabilidades (RACI por las iniciales, en inglés, de los tipos de responsabilidad) se utiliza generalmente en la gestión de proyectos para relacionar actividades con recursos (individuos o equipos de trabajo). De esta manera se logra asegurar que cada una de las tareas esté asignada a un individuo o a un órgano colegiado, su descripción se detalla en la tabla 8. (MAGERIT, 2019)

Tabla 8 RACI

	Rol	Descripción
R	Responsable	Este rol realiza el trabajo y es responsable por su realización. Lo más habitual es que exista solo un R, si existe más de uno, entonces el trabajo debería ser subdividido a un nivel más bajo, usando para ello las matrices RACI. Es quien debe ejecutar las tareas.

A	Aprobador	Este rol se encarga de aprobar el trabajo finalizado y a partir de ese momento, se vuelve responsable por él. Sólo puede existir un A por cada tarea. Es quien debe asegurar que se ejecutan las tareas.
C	Consultado	Este rol posee alguna información o capacidad necesaria para terminar el trabajo. Se le informa y se le consulta información (comunicación bidireccional).
I	Informado	Este rol debe ser informado sobre el progreso y los resultados del trabajo. A diferencia del Consultado, la comunicación es unidireccional.

Fuente: Magerit 2019

Se definió las responsabilidades dentro de la organización como se detalla en la tabla 9.

Tabla 9 RACI Organización

Roles y Responsabilidades			
R	Responsable	Tesista	Realiza el trabajo
A	Aprobador	Gerente General	Aprueba la tarea
C	Consultado	Gerente de Servicios	Posee información y es experto en el tema
I	Informado	Gerente de Servicios	Es actualizado sobre el progreso del trabajo

Fuente: Propia

Y también se definió las responsabilidades dentro del equipo responsable de aprobar este trabajo de titulación de la Universidad Técnica del Norte como se detalla en la tabla 10.

Tabla 10 RACI UTN

Roles y Responsabilidades			
R	Responsable	Tesista	Realiza el trabajo
A	Aprobador	Tutor	Aprueba la tarea
C	Consultado	Asesores	Posee información y es experto en el tema
I	Informado	Tutor, Asesores	Es actualizado sobre el progreso del trabajo

Fuente: Propia

3.3 Contexto

El contexto se encuentra en el informe confidencial presentado a la Organización y es de tipo confidencial.

3.4 Alcance

Objetivo, alcance y usuarios

El objetivo de este documento es definir claramente los límites de la Gestión de Riesgos de Seguridad de la Información en la Organización.

Esto se aplica a toda la documentación y actividades dentro de la Gestión de Riesgos de Seguridad de la Información.

Los usuarios son los miembros de la Dirección de la Organización, los miembros del equipo responsable de la Seguridad de la Información en la Organización.

Definición del alcance de la Gestión de Riesgos

La organización necesita definir los límites de la Gestión de Riesgos de Seguridad de la Información para decidir qué información quiere proteger. Este tipo de información deberá ser protegida independientemente de si además es almacenada, procesada o transferida dentro o fuera del alcance de la Gestión de Riesgos de Seguridad de la Información. El hecho de que determinada información esté disponible fuera del alcance no significa que no se le aplicarán las medidas de seguridad; esto solamente implica que la responsabilidad por la aplicación de las medidas de seguridad será transferida a un tercero que administre esa información.

El alcance de la Gestión de Riesgos de Seguridad de la Información se define de acuerdo con los siguientes aspectos:

Procesos y servicios

Manejo de la Información de los Clientes de Consultoría.

Unidades organizativas

Departamento de Consultoría y Capacitación

Exclusiones del alcance

Los siguientes elementos no están incluidos en el alcance:

- Información que no sea clasificada como “Información de los Clientes de Consultoría”.
- Información de otros departamentos.

3.5 Metodología de análisis de riesgos

Magerit en su libro 1 nos brinda unos pasos pautados para ejecutar la gestión de riesgos que se detalla en la tabla 11.

Tabla 11 Tareas de análisis de riesgos

MAR - Método de Análisis de Riesgos
MAR.1 Caracterización de los activos
MAR.11 – Identificación de activos
MAR.12 – Valoración de los activos
MAR.2 Caracterización de las amenazas
MAR.21 – Identificación de las amenazas
MAR.22 – Valoración de las amenazas
MAR.3 Caracterización de las salvaguardas
MAR.31 – Identificación de las salvaguardas pertinentes
MAR.32 – Valoración de las salvaguardas
MAR.4 Estimación de riesgo
MAR.41 – Estimación de impacto
MAR.42 – Estimación del riesgo

Fuente: Magerit 2019

Pilar se enfoca en cumplir la metodología Magerit por lo cual nos da aspectos establecidos como se detalla en la figura 23.

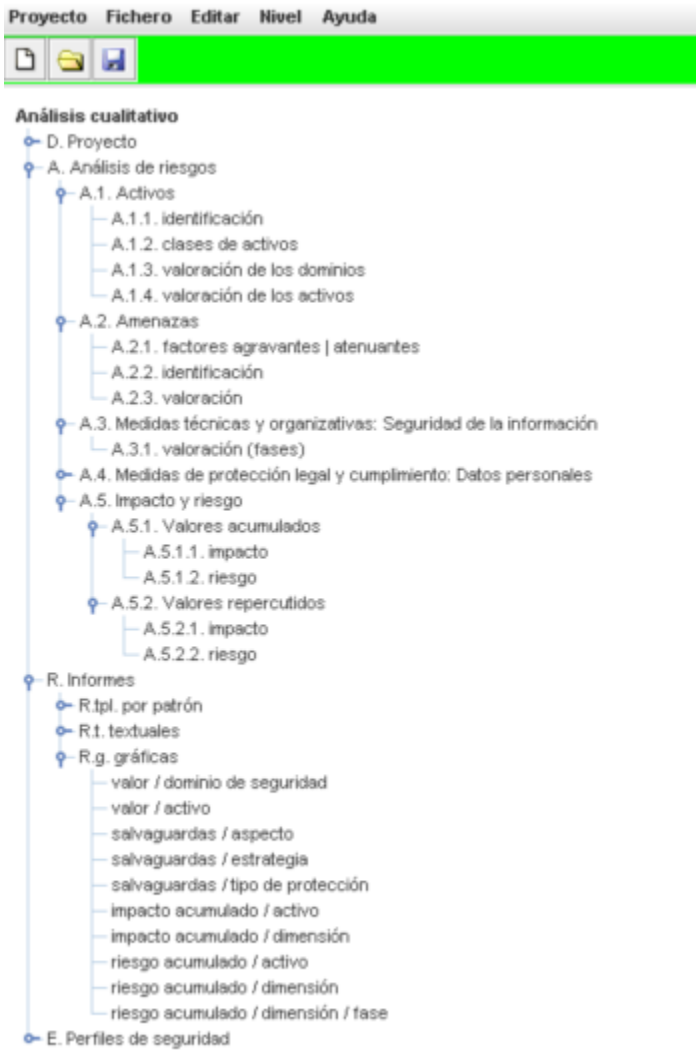


Figura 23 Pilar
Fuente: Pilar 7.4.5

3.5.1 MAR.11 Caracterización de los activos

Componente o funcionalidad de un sistema de información susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización. Incluye: información, datos, servicios, aplicaciones (software), equipos (hardware), comunicaciones, recursos administrativos, recursos físicos y recursos humanos.(Nacional, 2016)

En un sistema de información hay 2 cosas esenciales:

— la información que maneja

— y los servicios que presta.

Estos activos esenciales marcan los requisitos de seguridad para todos los demás componentes del sistema.

Subordinados a dicha esencia se pueden identificar otros activos relevantes:

— Datos que materializan la información.

— Servicios auxiliares que se necesitan para poder organizar el sistema.

— Las aplicaciones informáticas (software) que permiten manejar los datos.

— Los equipos informáticos (hardware) y que permiten hospedar datos, aplicaciones y servicios.

— Los soportes de información que son dispositivos de almacenamiento de datos.

— El equipamiento auxiliar que complementa el material informático.

— Las redes de comunicaciones que permiten intercambiar datos.

— Las instalaciones que acogen equipos informáticos y de comunicaciones.

— Las personas que explotan u operan todos los elementos anteriormente citados.

En la tabla 14 se presenta la identificación de los activos que cuenta la organización dentro del alcance establecido.

Tabla 14 Activos

No.	Código	Nombre del activo	Descripción	Tipo
1	HW-01	LPTP-GS-001	Laptop de uso diario de la Gerente General de la empresa, equipo usado para manejo de información de clientes, empleados.	Hardware
2	HW-02	LPTP-GS-002	Laptop de uso diario del Gerente de servicios, equipo usado para manejo de información de clientes e información importante.	Hardware
3	HW-03	LPTP-GS-003	Laptop de uso diario del consultor Jr, equipo usado para soporte técnico, manejo de información de contacto de clientes, manejo de documentación.	Hardware

4	HW-04	LPTP-GS-004	Laptop de uso diario del área de marketing, equipo usado para manejo de imagen, video y publicación de información del giro del negocio	Hardware
5	HW-05	Desktop-01	Equipo de escritorio de uso diario del área de Gerencia General, equipo usado para el manejo de información de contacto de clientes y proveedores.	Hardware
6	HW-06	Impresora HP Color LaserJet MFP M477fdw	Impresora	Hardware
7	Com-01	Teléfono Recepción	Teléfono Recepción	Comunicaciones
8	Com-02	Teléfono Gerencia de Servicios	Teléfono Gerencia de Servicios	Comunicaciones
9	Com-03	Teléfono área de ventas	Teléfono área de ventas	Comunicaciones
10	Com-04	Teléfono Gerencia General	Teléfono Gerencia General	Comunicaciones
11	Com-05	Teléfono área de capacitación	Teléfono área de capacitación	Comunicaciones
12	Com-06	Sistema Panasonic KX-TDA100D	Planta telefónica híbrida para conexiones de teléfono analógicas e IP	Comunicaciones
13	Com-07	Router CISCO 800 SERIES	Equipo utilizado para interconectar redes internas	Comunicaciones
14	Com-08	Router Linksys e900	Router inalámbrico	Comunicaciones
15	Com-09	ONT	Dispositivo Ont	Comunicaciones
16	Datos-01	Base de datos clientes (hubspot)	Base de datos de clientes.	Datos
17	Datos-02	Cotizaciones	Repositorio de cotizaciones para clientes nuevos y renovaciones de servicios.	Datos
18	Datos-03	Información Comercial	Repositorio de información comercial, servicios y productos comercializados.	Datos
19	Datos-04	Información personal de colaboradores	Repositorio de hojas de vida de colaboradores de la empresa	Datos
20	Datos-05	Información sobre clientes de auditoría	Información de clientes que se realiza auditoría	Datos

21	Datos-06	Información de clientes de consultoría	Información de clientes de consultoría	Datos
22	Datos-07	Base de datos clientes soporte (Freshdesk)	Información de clientes que solicitan soporte técnico	Datos
23	SW-01	Office 365	Herramienta de ofimática	Software
24	SW-02	FreshDesk	Mesa de servicios para la administración de solicitudes de soporte.	Software
25	SW-03	Hubspot	Desarrollador y comercializador de productos de software, ofrece una suite completa de herramientas de marketing, ventas y atención al cliente.	Software
26	Personal-01	Gerente de servicios	Gerente de servicios	Personal
27	Personal-02	Gerente General	Gerente general	Personal
28	Personal-03	Consultor Jr	Talento humano del área de consultoría	Personal
29	Personal-04	Analista de marketing digital	Talento humano del área de marketing	Personal
30	Personal-05	Asistente de gerencia	Asistente de gerencia	Personal

Fuente: Organización 2020

En la herramienta Pilar se detalla en la figura 24.

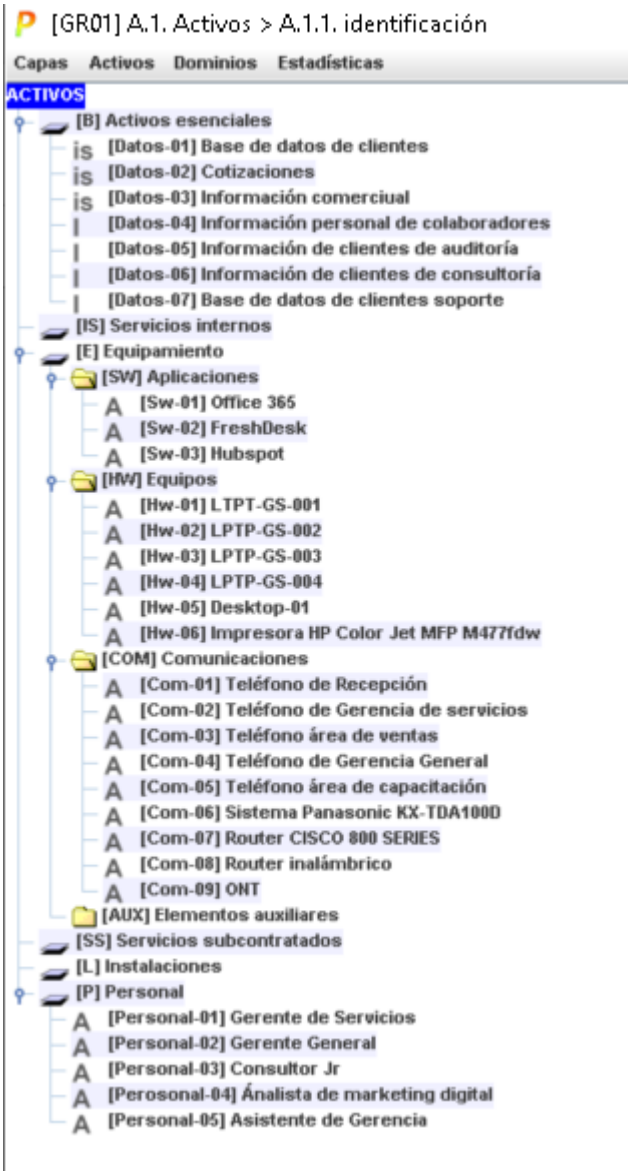


Figura 24 Activos
Fuente: Pilar 7.4.5

Una vez definido los activos Pilar nos permite definir estos a través de clases de activos es decir seleccionar aspectos preestablecidos que determinen a cada activo, a continuación, se detalla cómo queda cada activo con su clase correspondiente.

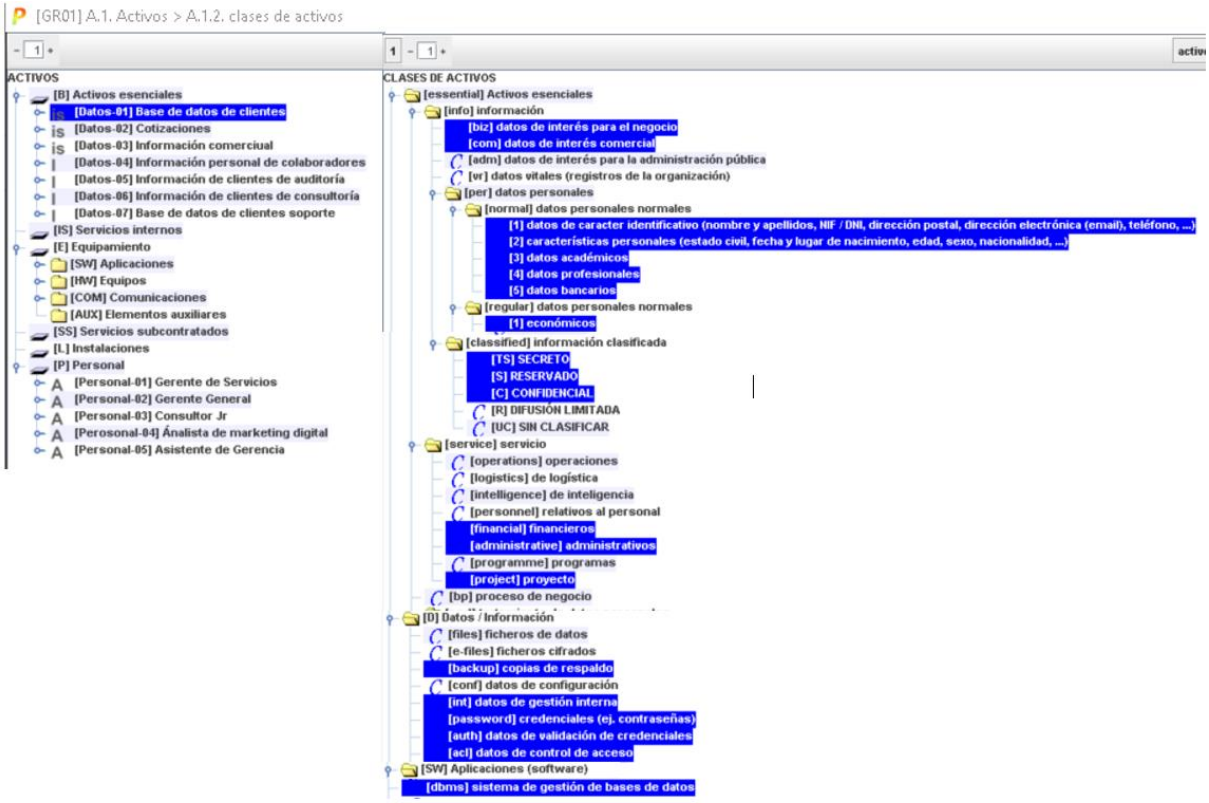


Figura 25 Clase de activo: Bdd de clientes
Fuente: Pilar 7.4.5

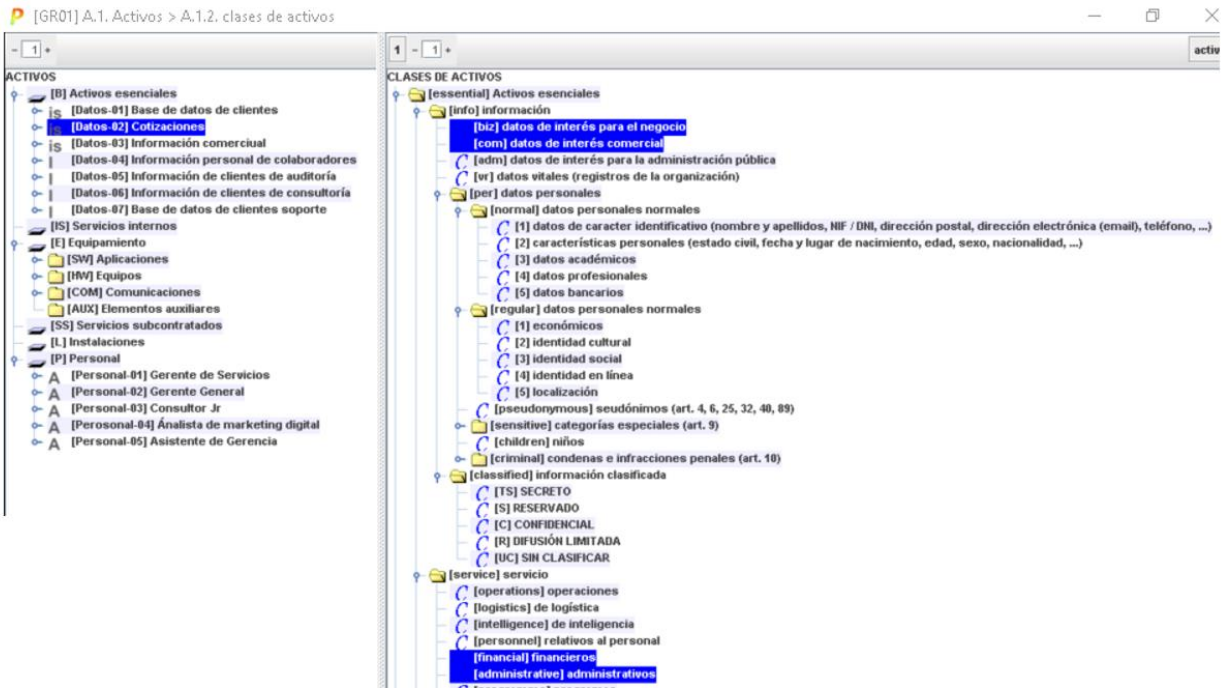


Figura 26 Clase de activo: Cotizaciones
Fuente: Pilar 7.4.5

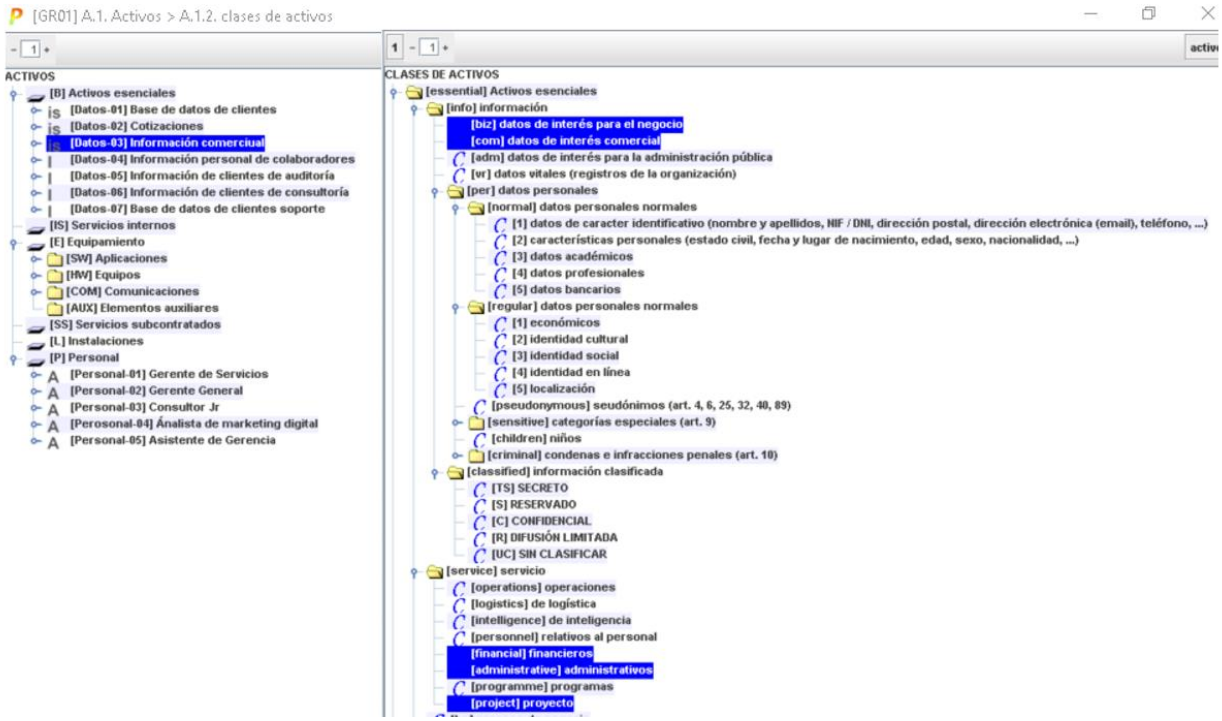


Figura 27 Clase de activos: Información comercial
Fuente: Pilar 7.4.5

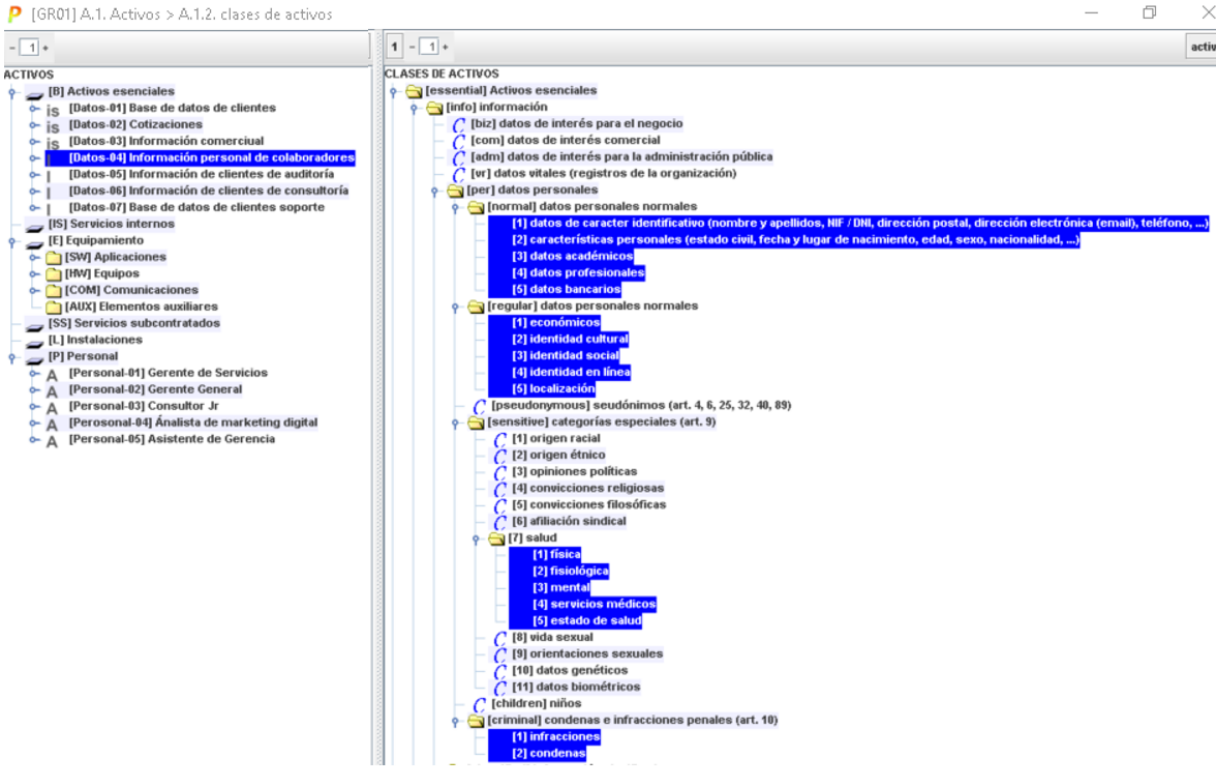


Figura 28 Clase de activos: Información personal de colaboradores
Fuente: Pilar 7.4.5

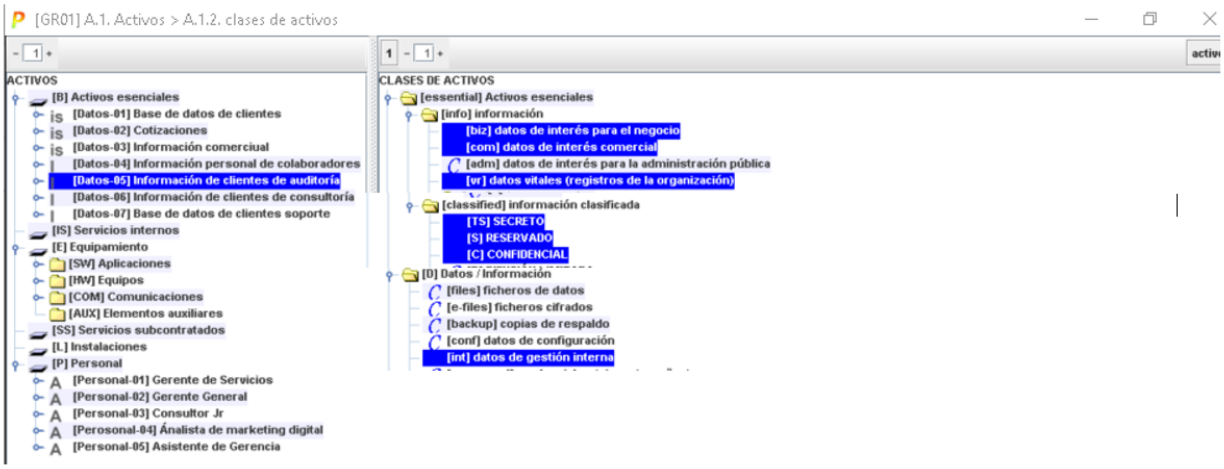


Figura 29 Clase de activos: Información de clientes de auditoría
Fuente: Pilar 7.4.5

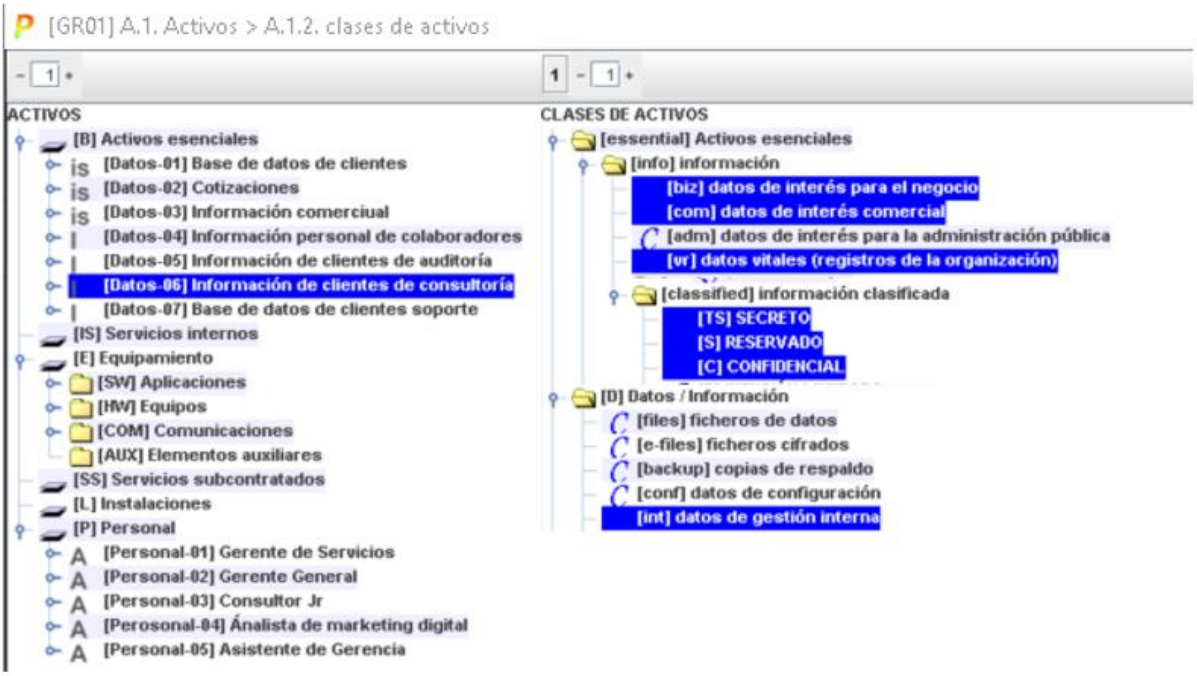


Figura 30 Clase de activos: Información de clientes de consultoría
Fuente: Pilar 7.4.5

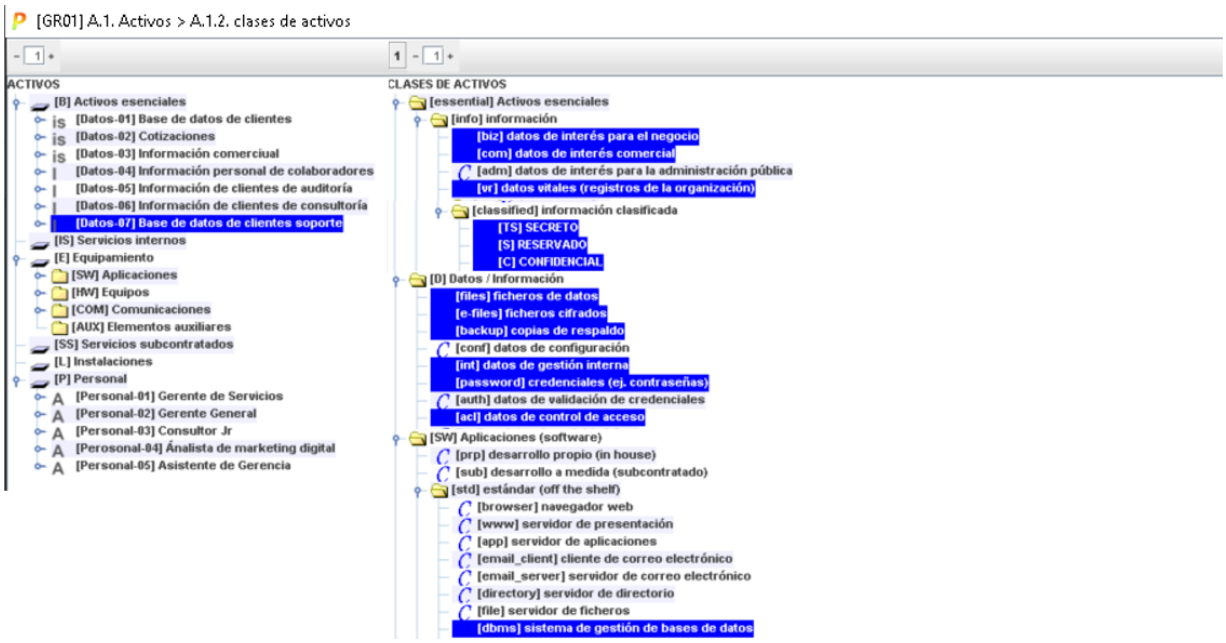


Figura 31 Clase de activos: Bdd de clientes soporte
Fuente: Pilar 7.4.5

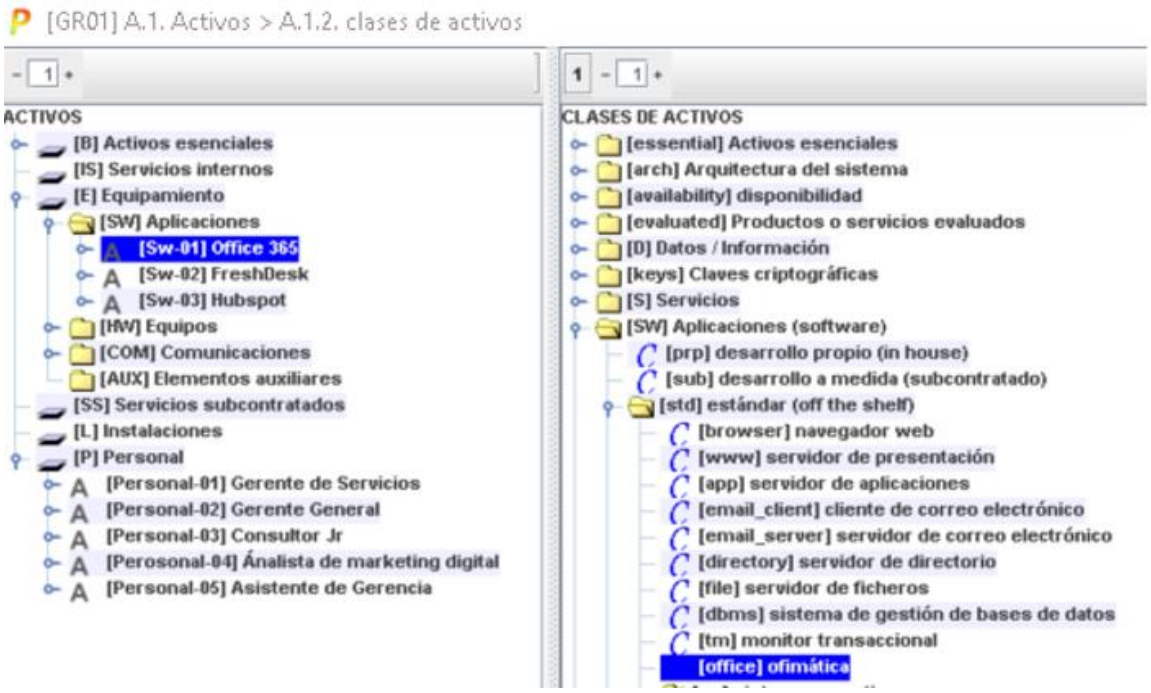


Figura 32 Clase de activos: Office 365
Fuente: Pilar 7.4.5

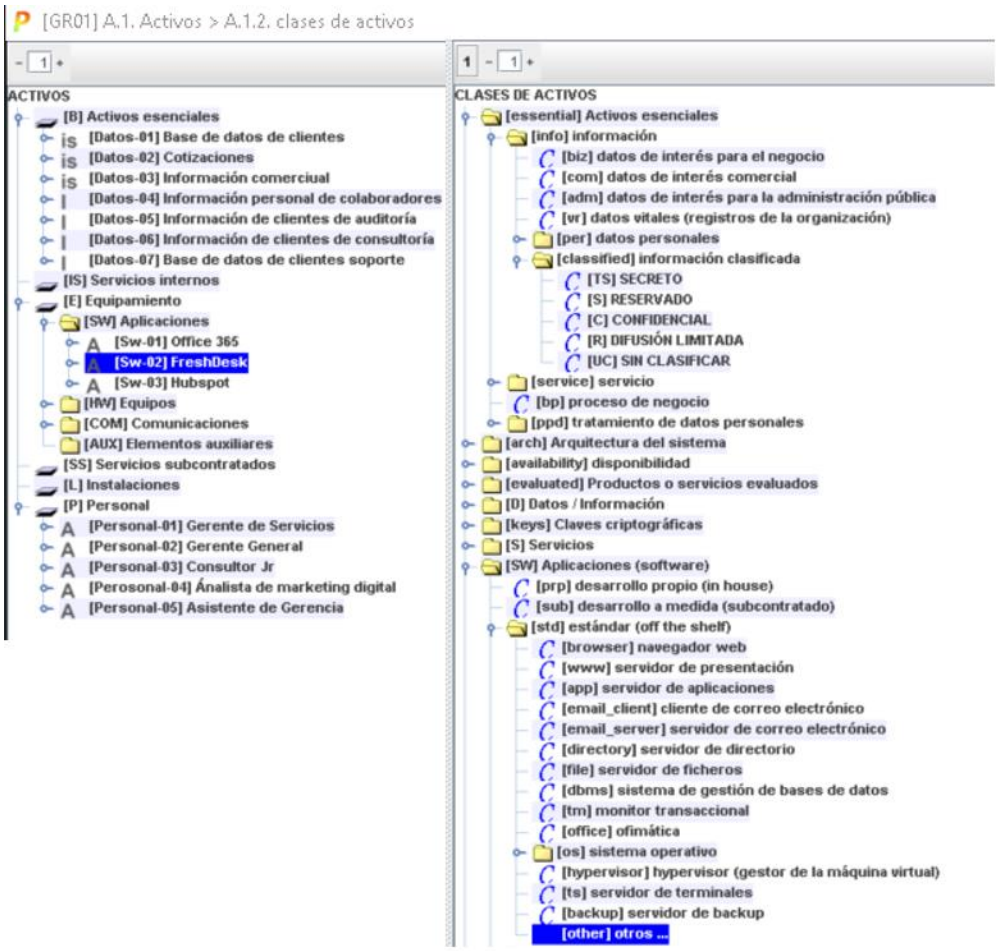


Figura 33 Clase de activos: FreshDesk
Fuente: Pilar 7.4.5

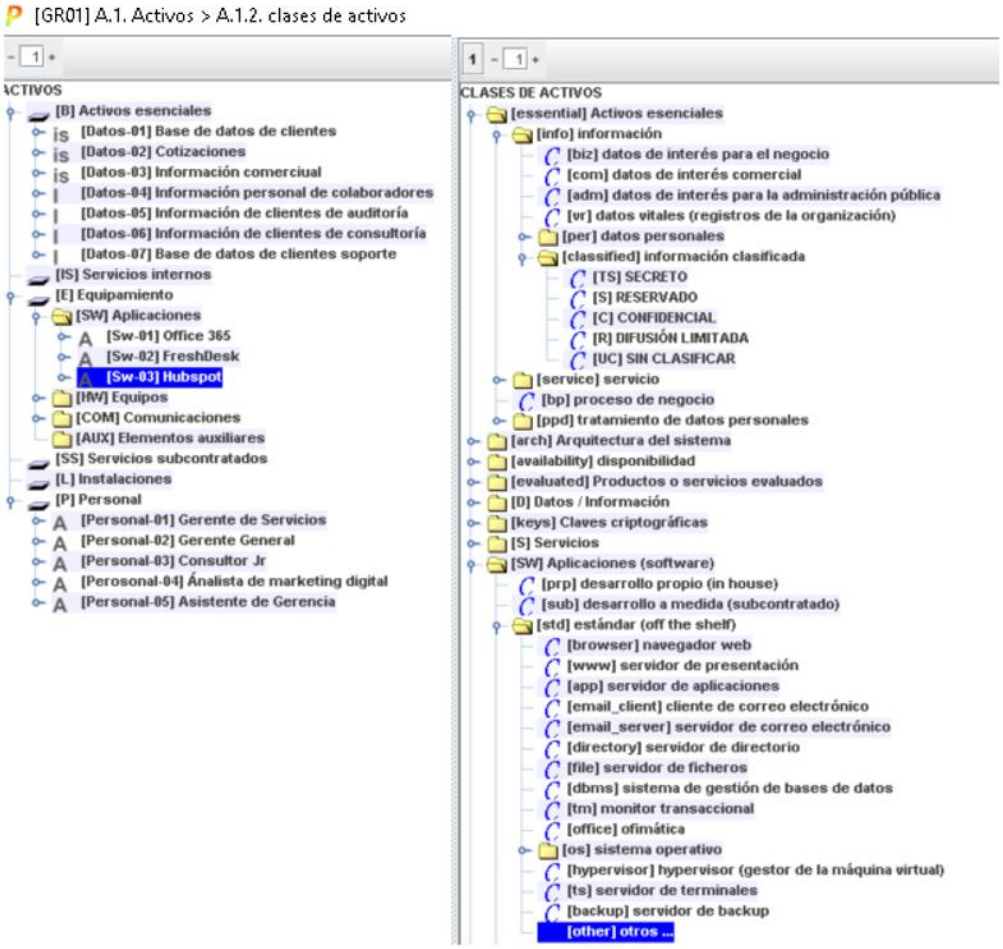


Figura 34 Clase de activos: Hubspot
Fuente: Pilar 7.4.5

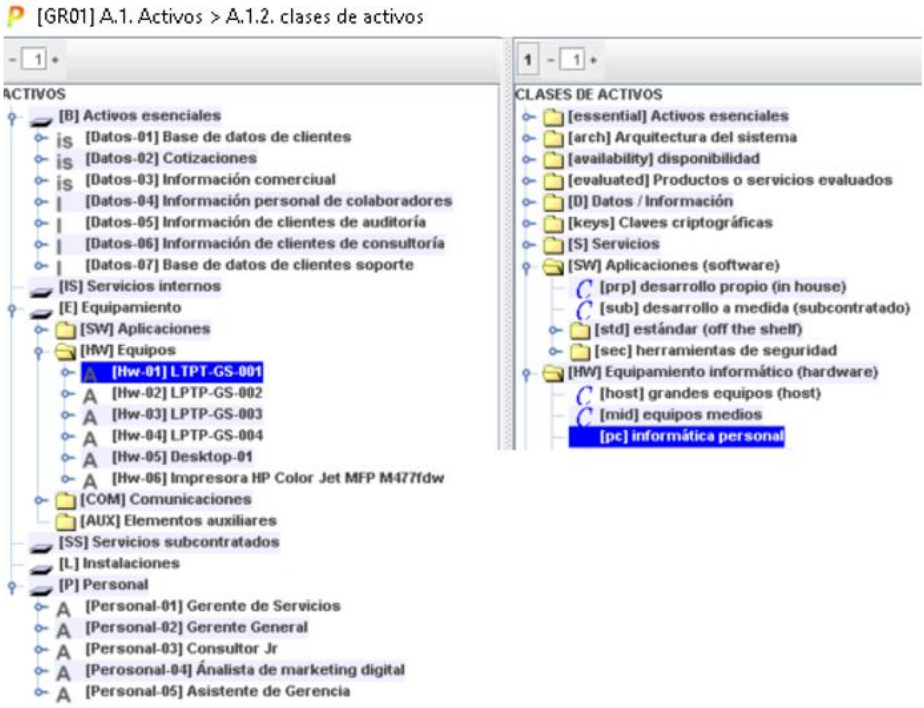


Figura 35 Clase de activos: LTPT-GS-001
Fuente: Pilar 7.4.5

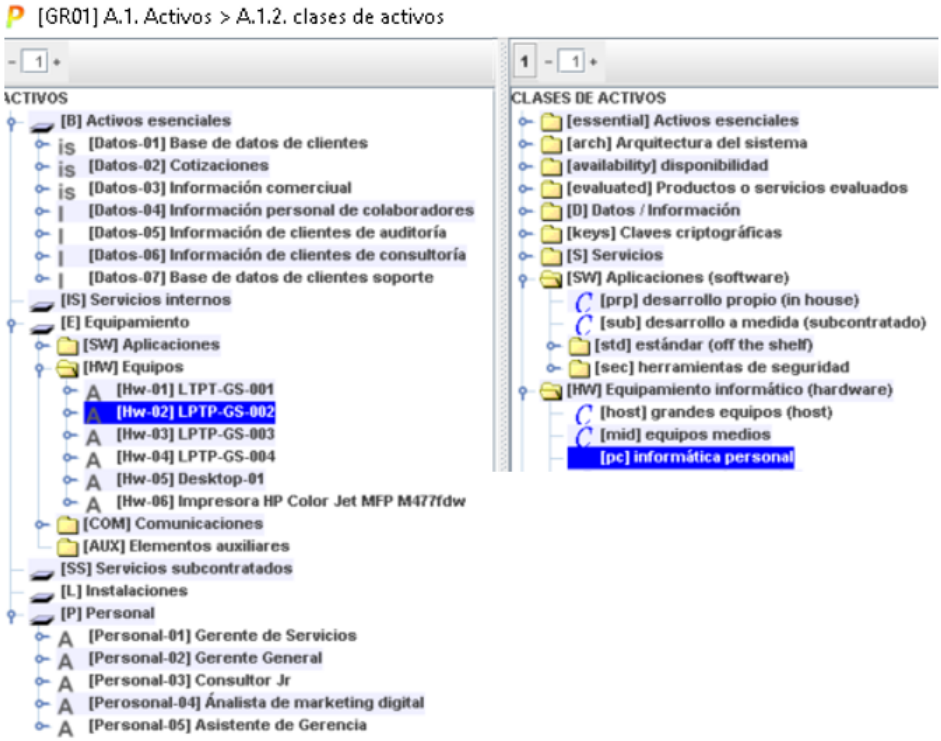


Figura 36 Clase de activos: LPTP-GS-002
Fuente: Pilar 7.4.5

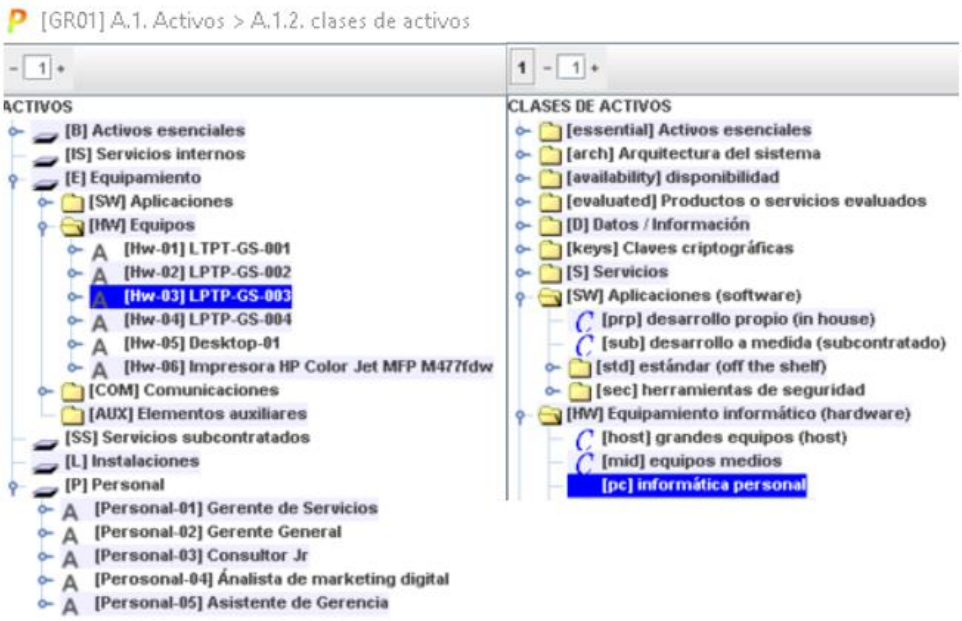


Figura 37 Clase de activos LPTP-GS-003
Fuente: Pilar 7.4.5

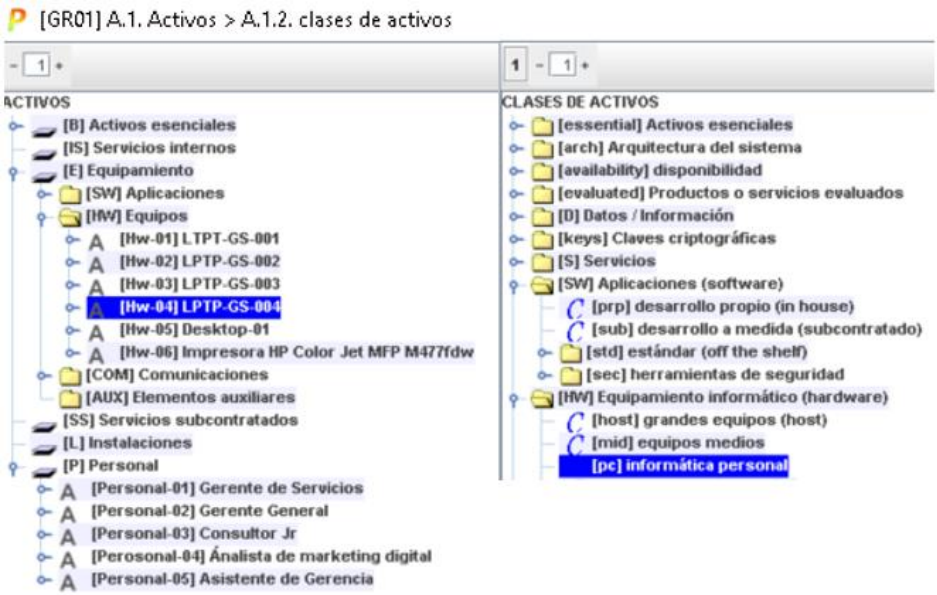


Figura 38 Clase de activos: LPTP-GS-004
Fuente: Pilar 7.4.5

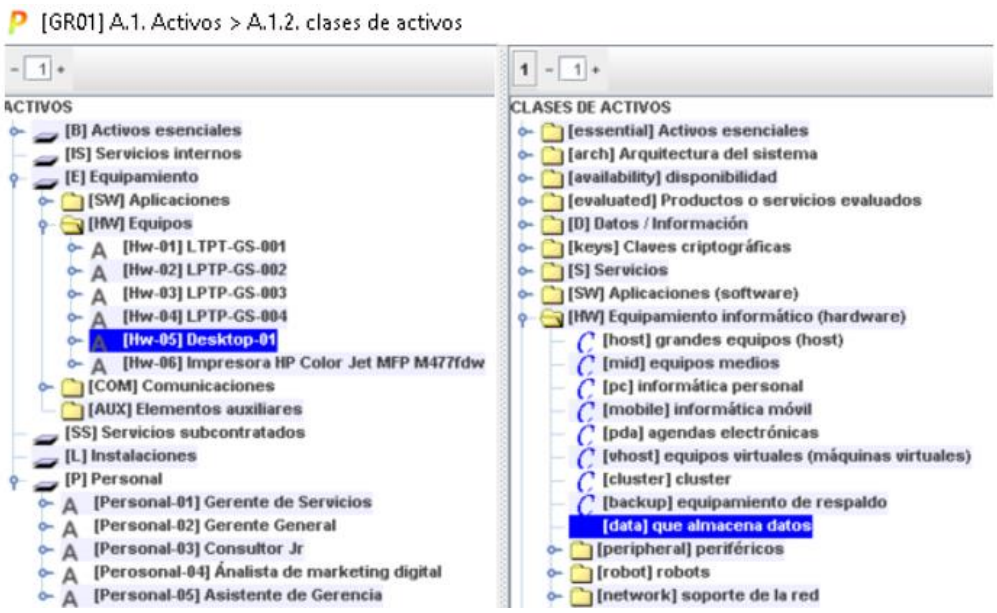


Figura 39 Clase de activos: Desktop-01
Fuente: Pilar 7.4.5

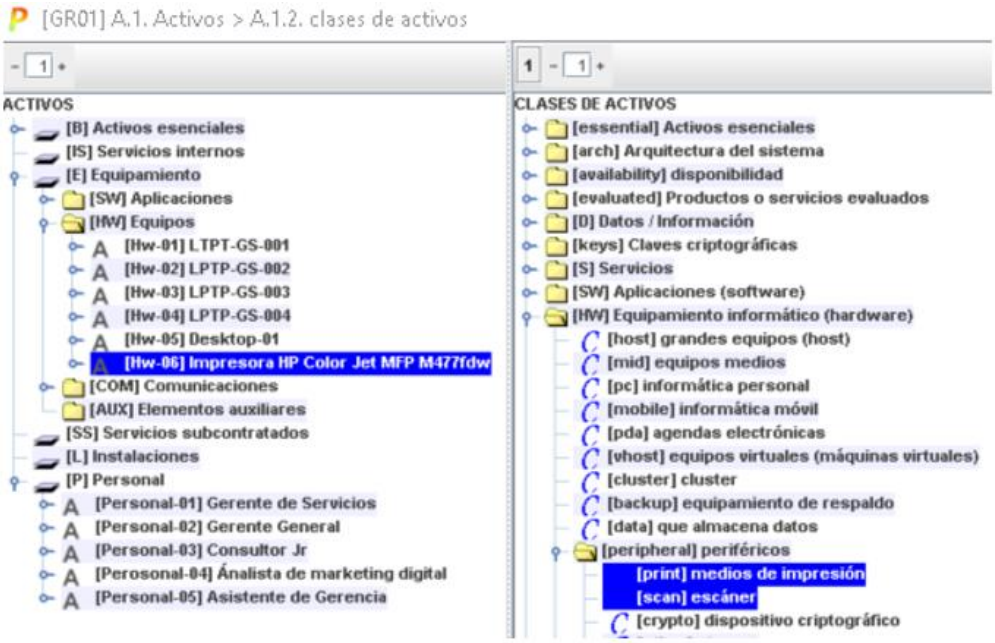


Figura 40 Clase de activos: Impresora HP Color MFP M47fdw
Fuente: Pilar 7.4.5

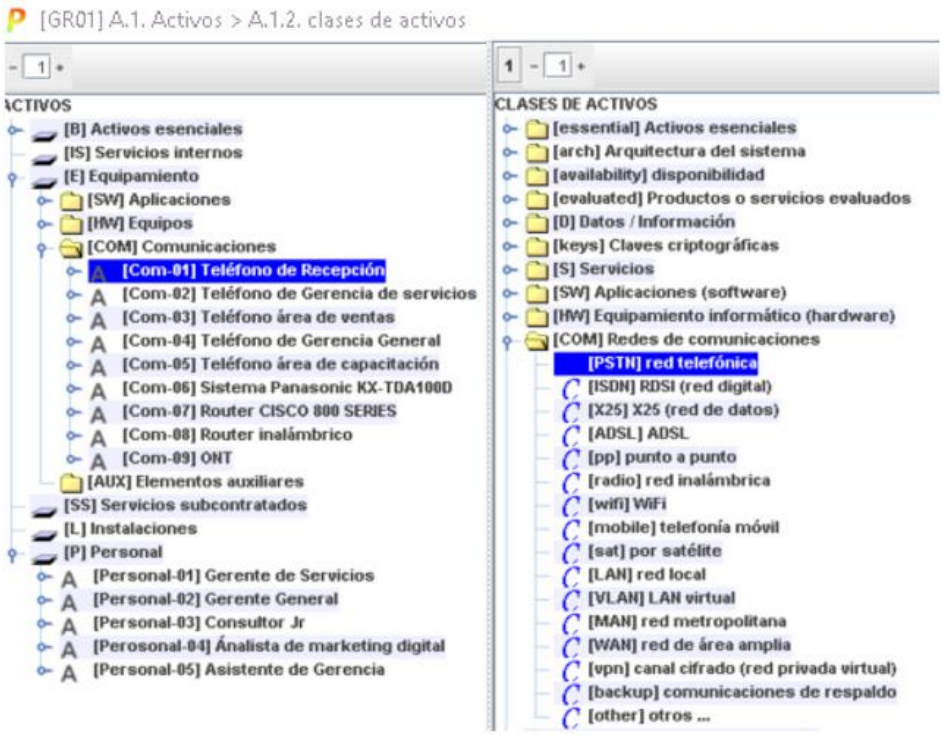


Figura 41 Clase de activos: Teléfono de recepción
Fuente: Pilar 7.4.5

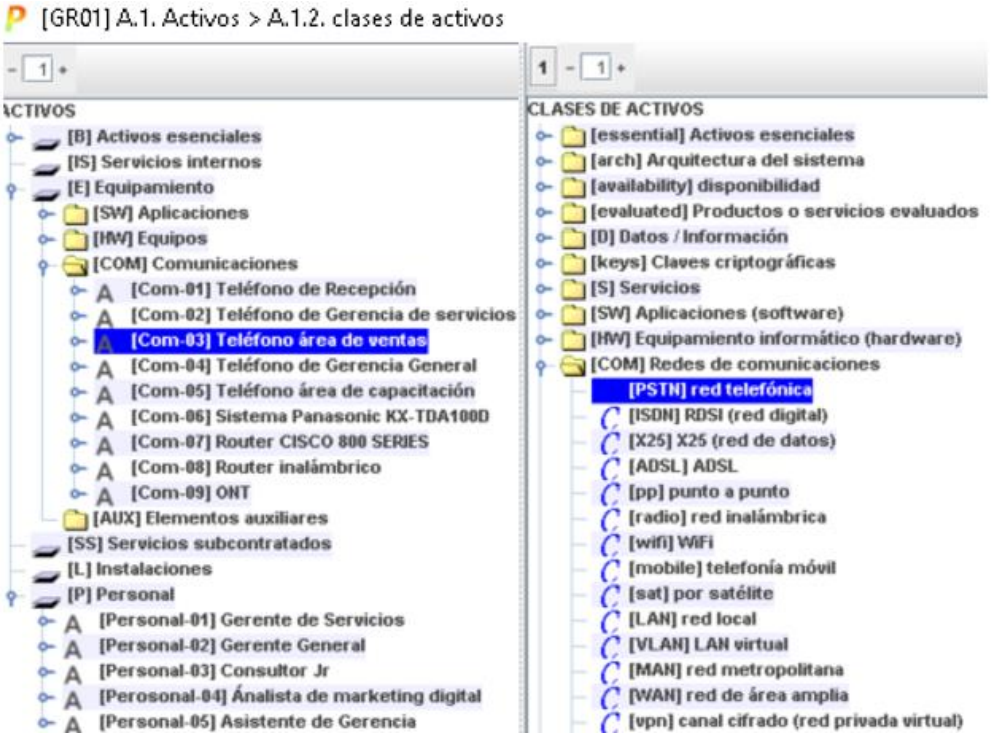


Figura 42 Clase de activos: Teléfono área de ventas
Fuente: Pilar 7.4.5

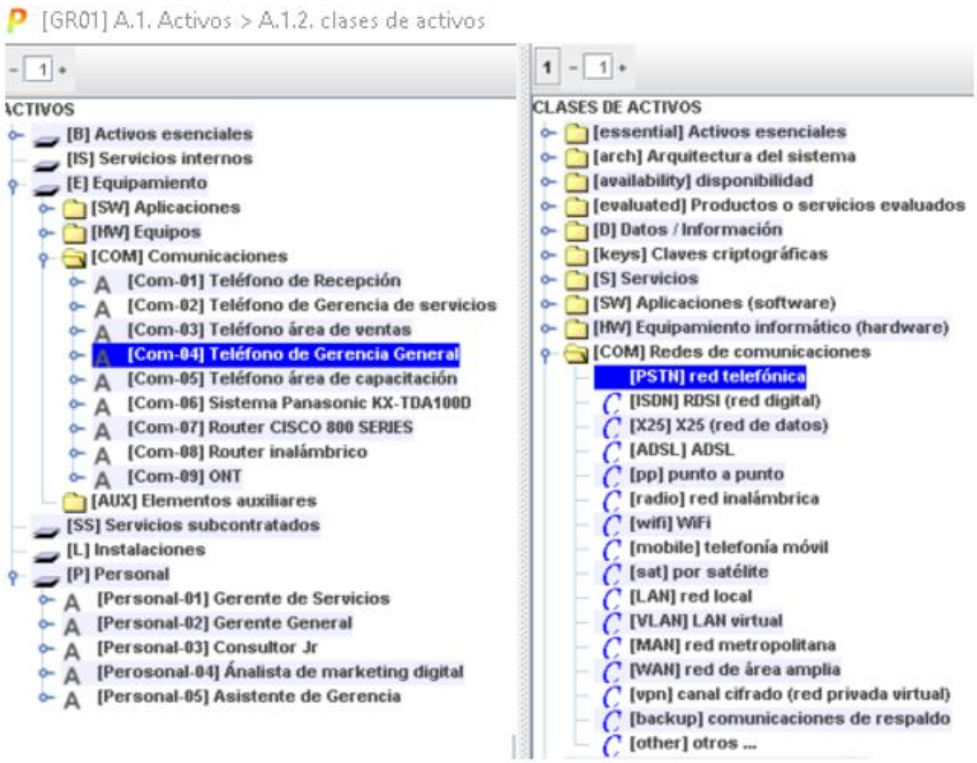


Figura 43 Clase de activos: Teléfono de Gerencia General
Fuente: Pilar 7.4.5

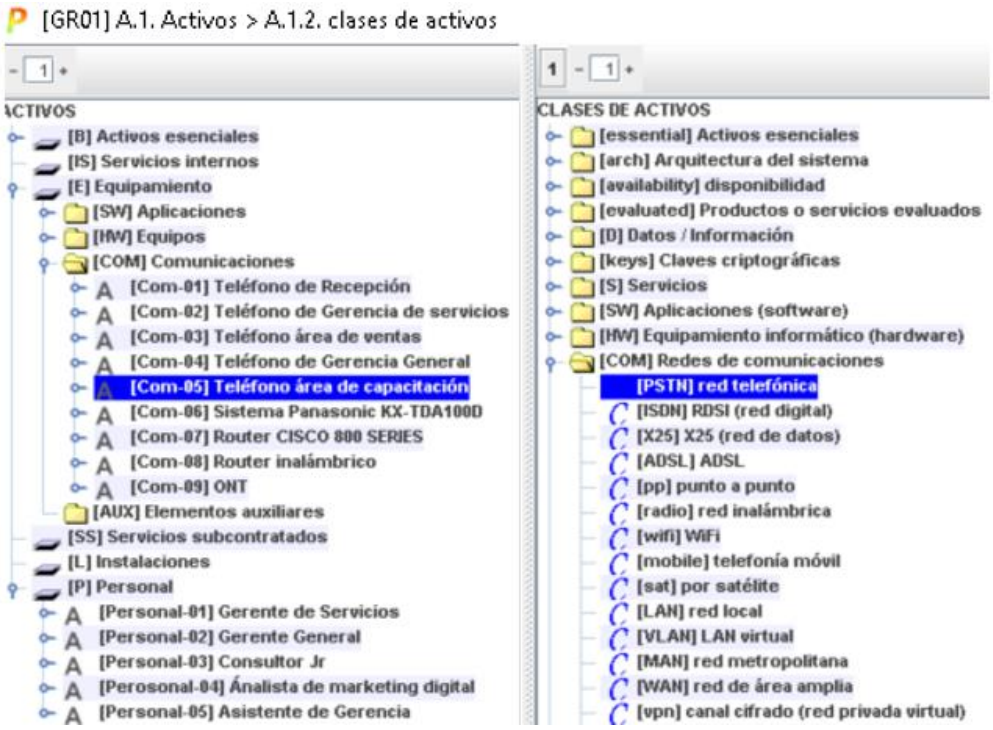


Figura 44 Clase de activos: Teléfono área de capacitación
Fuente: Pilar 7.4.5

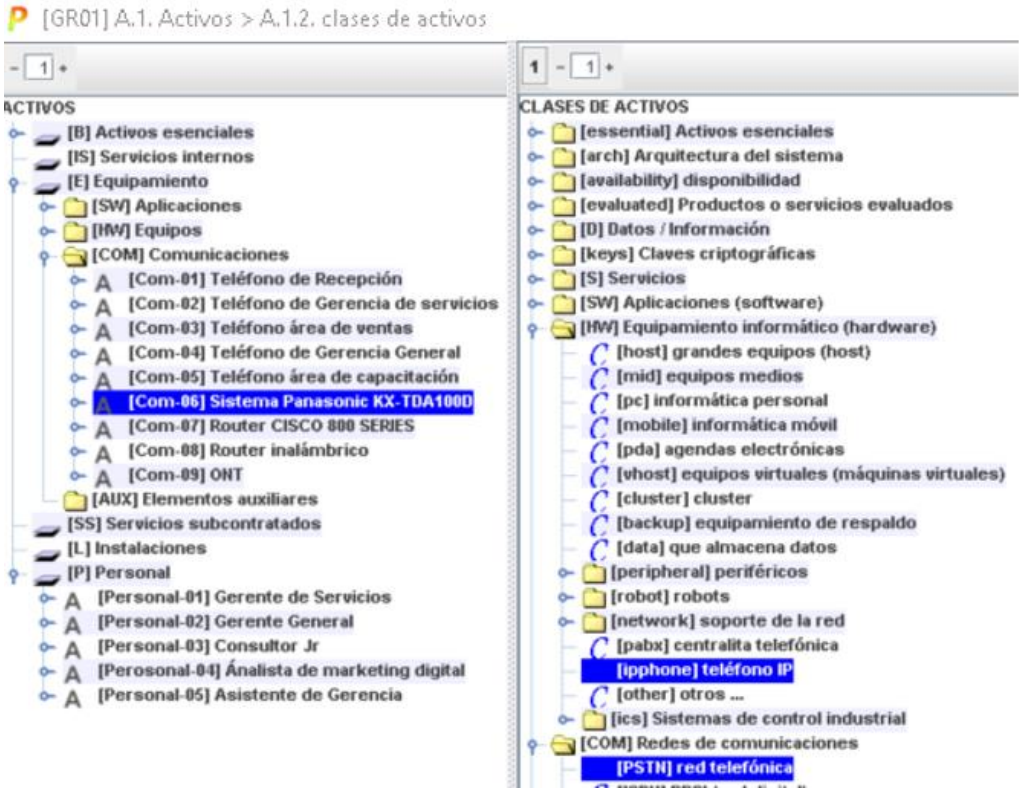


Figura 45 Clase de activos: Sistema Panasonic KX-TDA100D
Fuente: Pilar 7.4.5

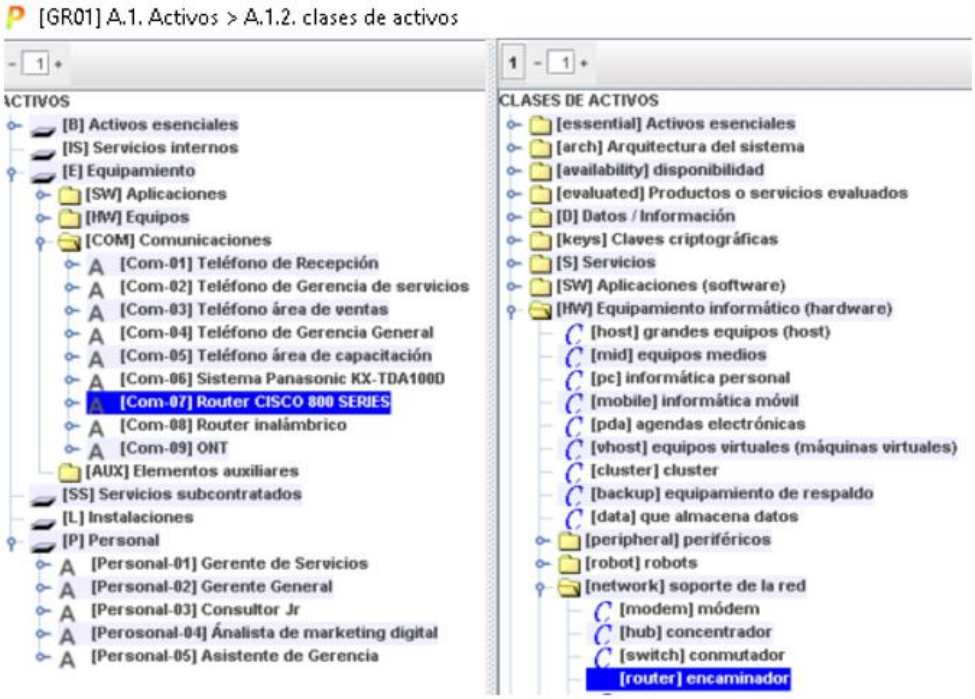


Figura 46 Clase de activos: Router Cisco 800 SERIES
Fuente: Pilar 7.4.5

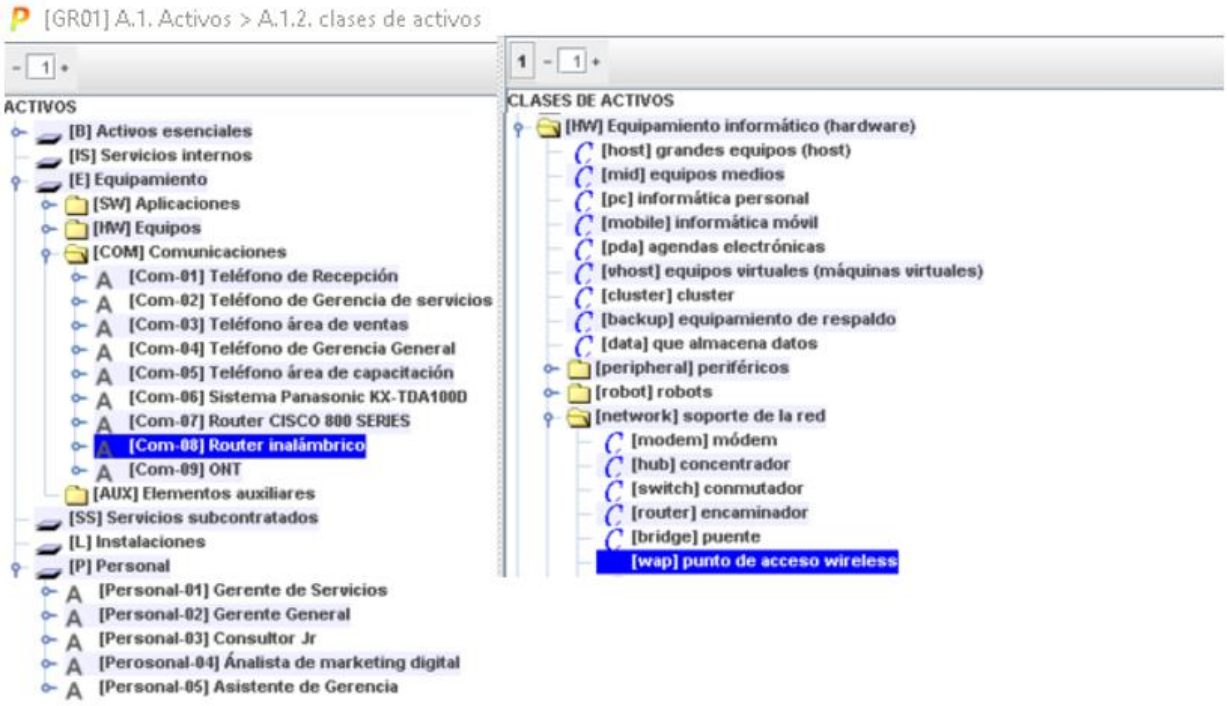


Figura 47 Clase de activos: Router inalámbrica
Fuente: Pilar 7.4.5

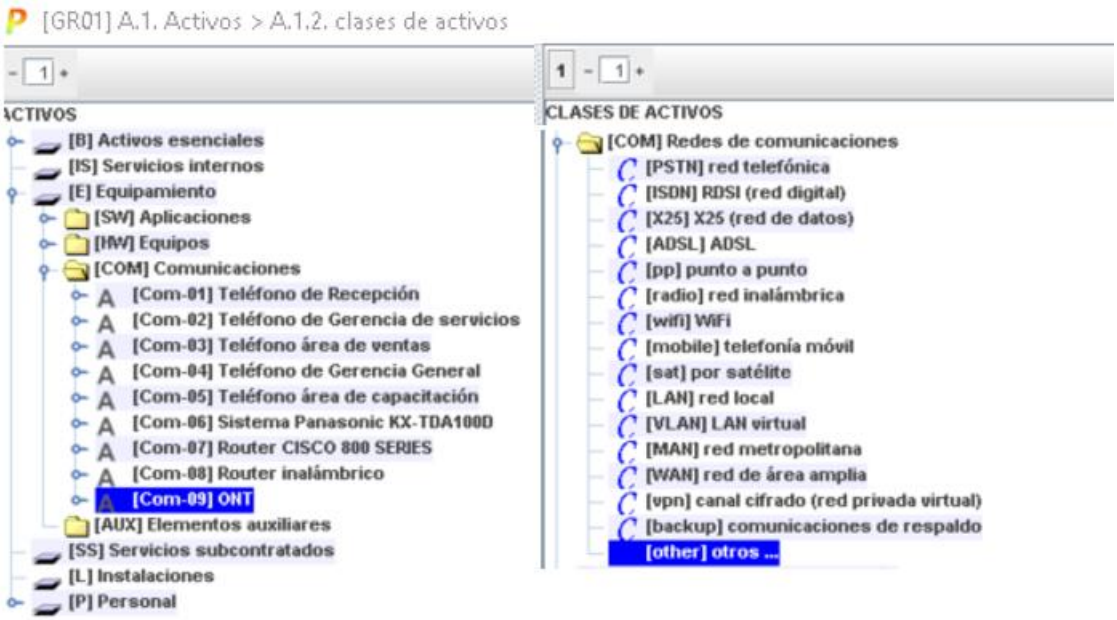


Figura 48 *Clase de activos: ONT*
Fuente: Pilar 7.4.5

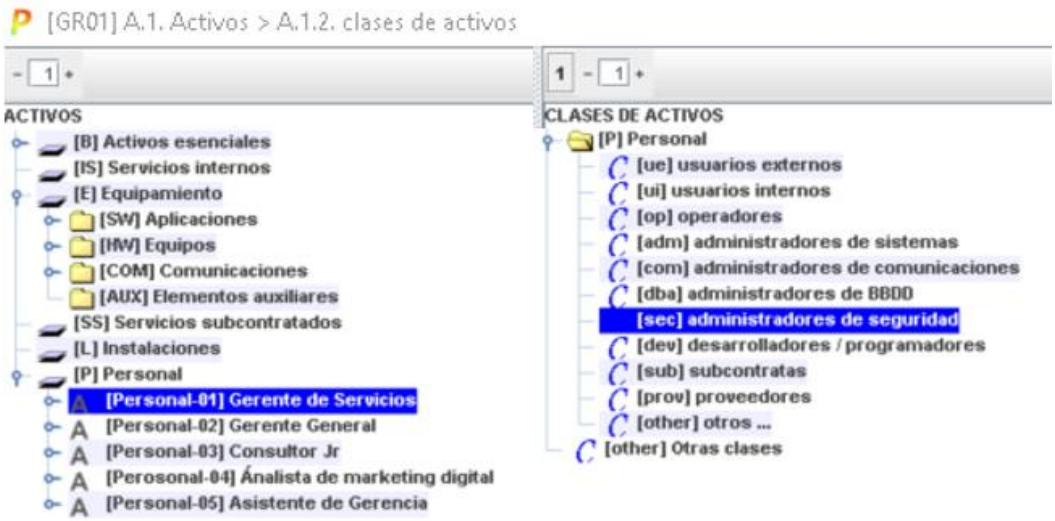


Figura 49 Clase de activos: Gerente de Servicios
Fuente: Pilar 7.4.5

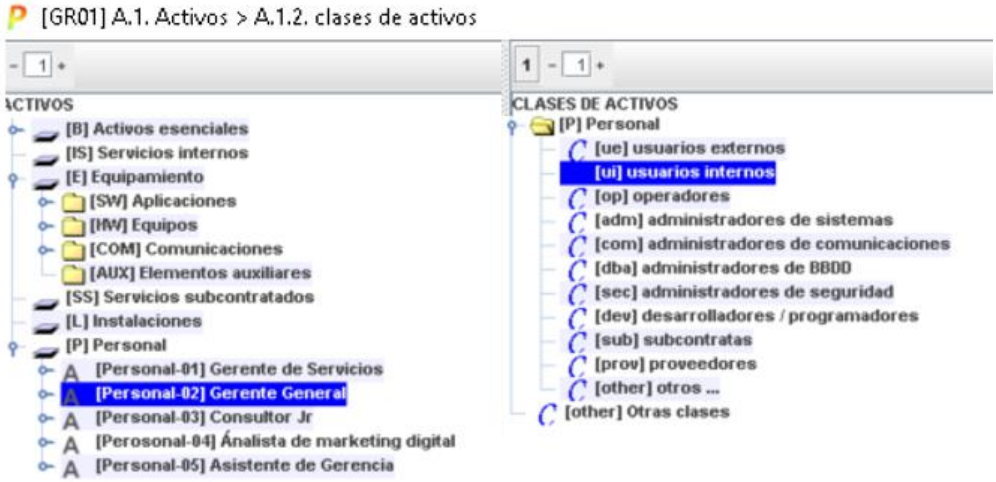


Figura 50 Clase de activos: Gerente General
Fuente: Pilar 7.4.5

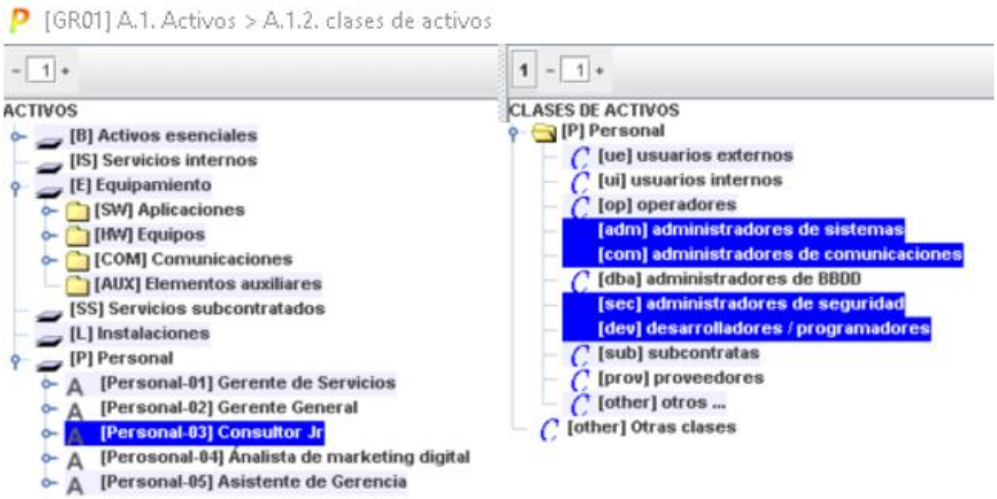


Figura 51 Clase de activos: Consultor Jr
Fuente: Pilar 7.4.5

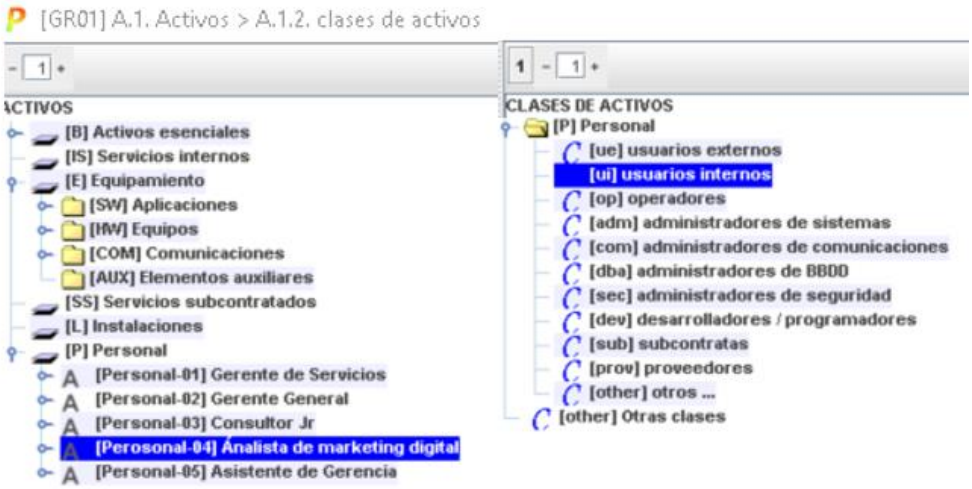


Figura 52 Clase de activos: Analista de marketing digital
Fuente: Pilar 7.4.5

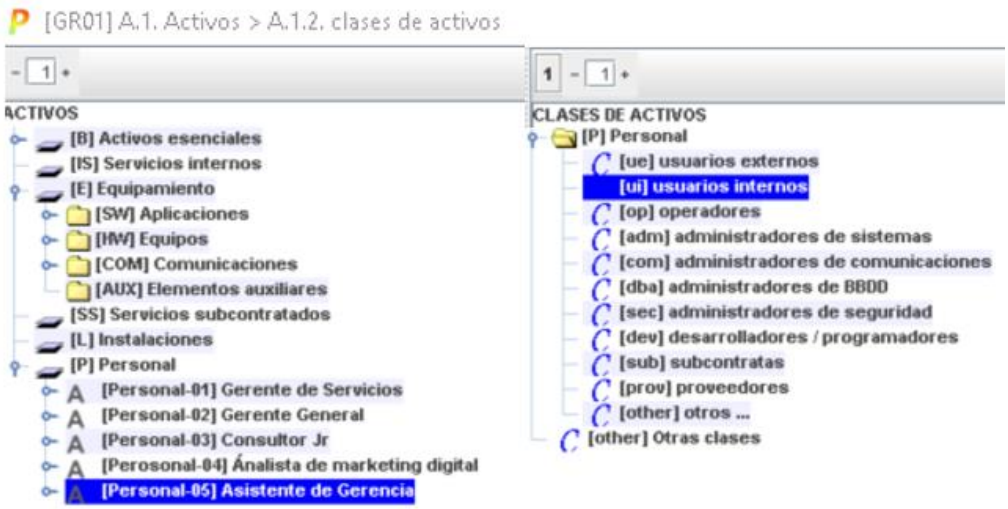


Figura 53 Clase de activos: Asistente de Gerencia
Fuente: Pilar 7.4.5

Pilar nos ofrece pasos a seguir basados en la Metodología escogida, el siguiente paso es valoración de los dominios, en este caso de estudio se creó un solo dominio enfocado en el alcance de este trabajo de titulación el cual es la Información de los clientes de consultoría, basados en esto se valoró los activos esenciales que conforman el dominio especificado.

La valoración se puede ver desde la perspectiva de la 'necesidad de proteger' pues cuanto más valioso es un activo, mayor nivel de protección requeriremos en la dimensión (o dimensiones) de seguridad que sean pertinentes (MAGERIT, 2019). En la tabla 12 se detalla los criterios de la valoración.

Tabla 12 Criterios de valoración

Nivel	Criterio
10	Muy alto
9	Alto (+)
8	Alto (-)
7	Alto
6	Medio (+)
5	Medio (-)
4	Medio
3	Bajo (+)
2	Bajo (-)
1	Bajo
0	Depreciable

Fuente: Pilar 7.4.5

Se realizó en las tres dimensiones principales por pedido especial de la organización estas se detalla en la tabla 13.

Tabla 13 Dimensiones

D	Disponibilidad
I	Integridad
C	Confidencialidad

Fuente: Pilar 7.4.5

La valoración se la realizó en base a la necesidad expresa de proteger ese activo dentro del alcance que se estableció, los valores son los establecidos en la tabla 13 y representados a la necesidad de proteger dicho domino abarcando los activos esenciales, como se detalla en la figura 54.

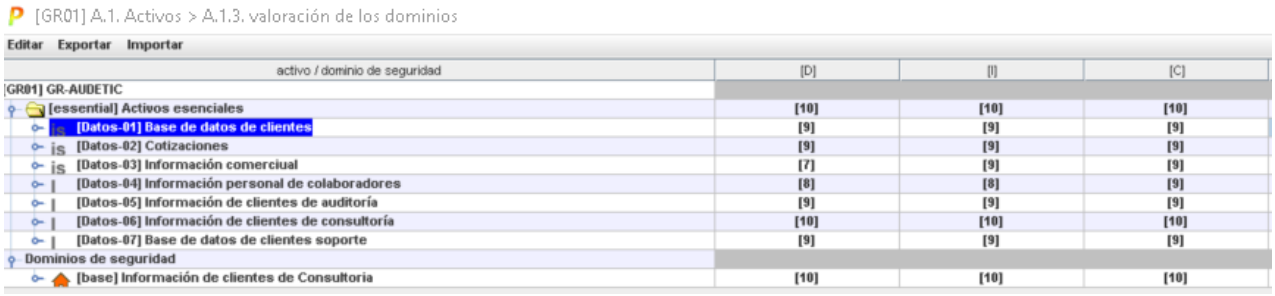


Figura 54 Valoración de dominios
Fuente: Pilar 7.4.5

El resultado de la valoración da como resultado que es demasiado importante proteger este dominio establecido.

El siguiente paso que nos da Magerit y Pilar es realizar la valoración de los activos estos están valorados de manera cualitativa, los criterios de valoración se detallan en la figura 55.

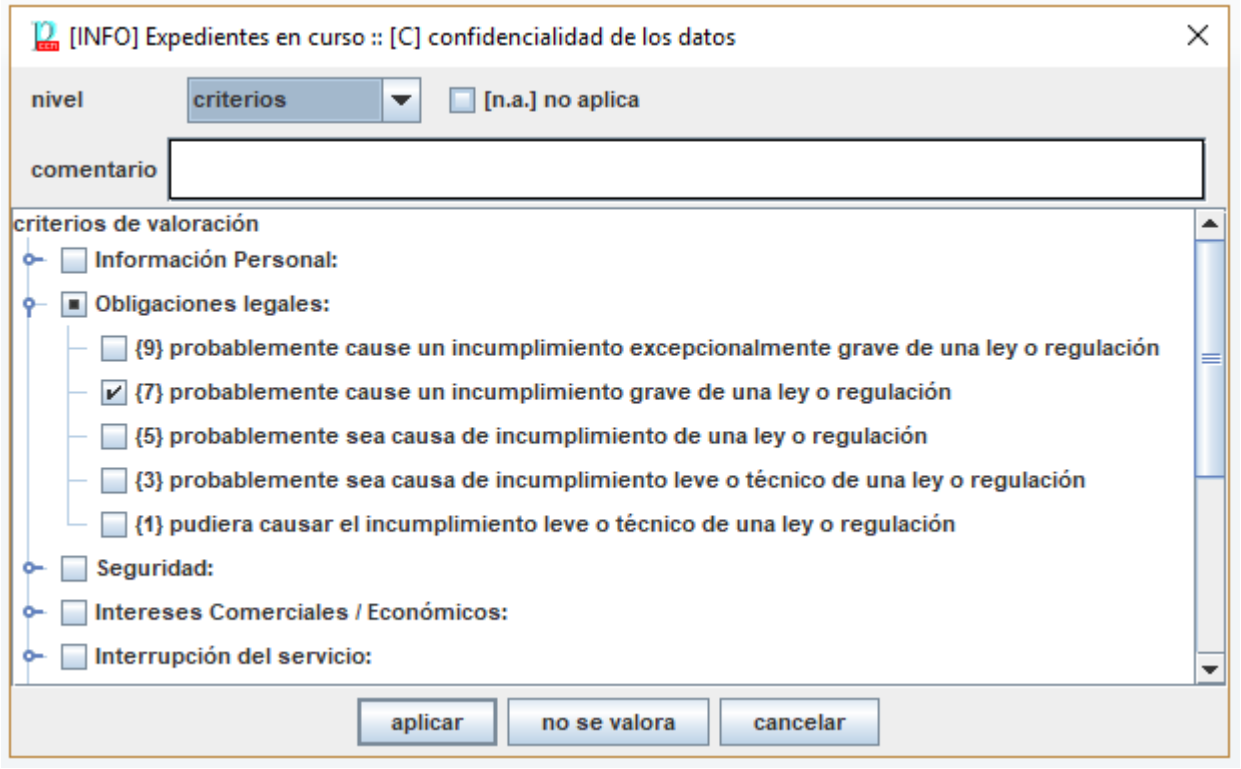


Figura 55 Criterios de valoración de los activos
Fuente: Pilar 7.4.5

Para un entendimiento mejor se estableció una tabla en donde se valoró los activos en referencia a la tabla 12 añadiendo colores para definir la criticidad de los activos.

Tabla 14 Criterios de valoración de activos

Criterio	Valor	
Daño muy grave a la organización	Muy Alto	10
Daño grave a la organización	Alto	7--9
Daño importante a la organización	Medio	4--6
Daño menor a la organización	Bajo	1--3
Irrelevante a efectos prácticos	Despreciable	0

Fuente: Propia

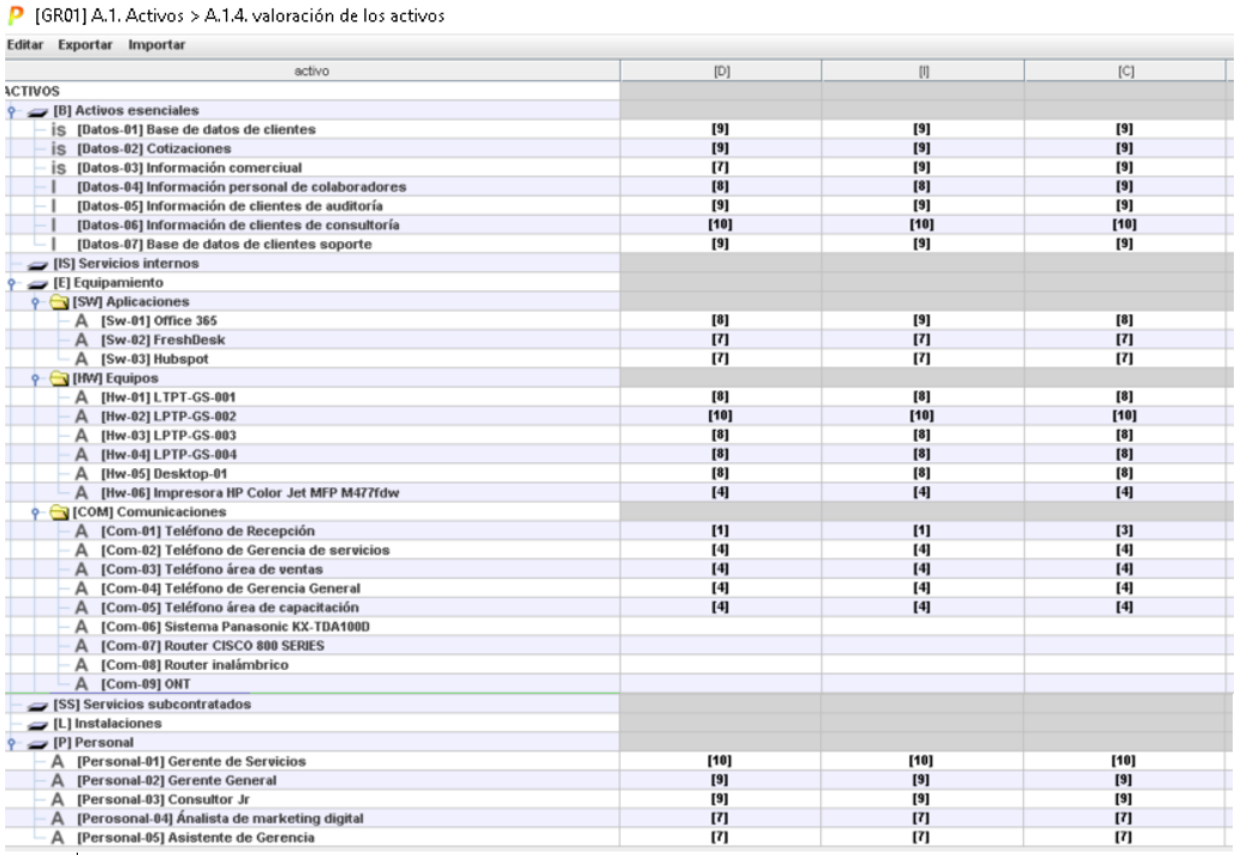
Dado los criterios para la valoración, se indica en la tabla 15 la valoración de activos como lo indica Magerit y lo acopla Pilar.

Tabla 15 Valoración de activos

Activos esenciales		C	D	I	Resultado
Datos-01	Base de datos de clientes	9	9	9	9
Datos-02	Cotizaciones	9	9	9	9
Datos-03	Información comercial	7	9	9	8
Datos-04	Información personal de colaboradores	8	8	9	8
Datos-05	Información de clientes de auditoría	9	9	9	9
Datos-06	Información de clientes de consultoría	10	10	10	10
Datos-07	Base de datos de clientes soporte	9	9	9	9
	Software				
Sw-01	Office 365	8	9	8	8
Sw-02	FreshDesk	7	7	7	7
Sw-03	HubSpot	7	7	7	7
	Hardware				
Hw-01	LPTP-GS-001	8	8	8	8
Hw-02	LPTP-GS-002	10	10	10	10
Hw-03	LPTP-GS-003	8	8	8	8
Hw-04	LPTP-GS-004	8	8	8	8
Hw-05	Desktop-01	8	8	8	8
Hw-06	Impresora HP Color Jet MFP M477fdw	4	4	4	4
	Comunicaciones				
Com-01	Teléfono de Recepción	1	1	3	2
Com-02	Teléfono de Gerencia de Servicios	4	4	4	4
Com-03	Teléfono área de ventas	4	4	4	4
Com-04	Teléfono de Gerencia General	4	4	4	4
Com-05	Teléfono área de capacitación	4	4	4	4
Com-06	Sistema Panasonic KX-TDA100D	4	4	4	4
Com-07	Router CISCO 800 SERIES	8	8	8	8
Com-08	Router inalámbrico	9	9	9	9
Com-09	ONT	4	4	4	4
	Personal				
Personal-01	Gerente de Servicios	10	10	10	10
Personal-02	Gerente General	9	9	9	9
Personal-03	Consultor Jr	9	9	9	9
Personal-04	Analista de marketing digital	7	7	7	7
Personal-05	Asiste de Gerencia	7	7	7	7

Fuente: Pilar 7.4.5

El resultado de esta valoración nos indica que activos son más importantes de proteger para la organización, expresada en colores como lo indica la tabla 9, también se indica la valoración realizada en Pilar en la figura 56.


[GR01] A.1. Activos > A.1.4. valoración de los activos

Editar Exportar Importar

activo	[D]	[I]	[C]
ACTIVOS			
[B] Activos esenciales			
[Datos-01] Base de datos de clientes	[9]	[9]	[9]
[Datos-02] Cotizaciones	[9]	[9]	[9]
[Datos-03] Información comerciual	[7]	[9]	[9]
[Datos-04] Información personal de colaboradores	[8]	[8]	[9]
[Datos-05] Información de clientes de auditoría	[9]	[9]	[9]
[Datos-06] Información de clientes de consultoría	[10]	[10]	[10]
[Datos-07] Base de datos de clientes soporte	[9]	[9]	[9]
[IS] Servicios internos			
[E] Equipamiento			
[SW] Aplicaciones			
[Sw-01] Office 365	[8]	[9]	[8]
[Sw-02] FreshDesk	[7]	[7]	[7]
[Sw-03] Hubspot	[7]	[7]	[7]
[HW] Equipos			
[Hw-01] LTPT-GS-001	[8]	[8]	[8]
[Hw-02] LPTP-GS-002	[10]	[10]	[10]
[Hw-03] LPTP-GS-003	[8]	[8]	[8]
[Hw-04] LPTP-GS-004	[8]	[8]	[8]
[Hw-05] Desktop-01	[8]	[8]	[8]
[Hw-06] Impresora HP Color Jet MFP M477fdw	[4]	[4]	[4]
[COM] Comunicaciones			
[Com-01] Teléfono de Recepción	[1]	[1]	[3]
[Com-02] Teléfono de Gerencia de servicios	[4]	[4]	[4]
[Com-03] Teléfono área de ventas	[4]	[4]	[4]
[Com-04] Teléfono de Gerencia General	[4]	[4]	[4]
[Com-05] Teléfono área de capacitación	[4]	[4]	[4]
[Com-06] Sistema Panasonic KX-TDA100D			
[Com-07] Router CISCO 800 SERIES			
[Com-08] Router inalámbrico			
[Com-09] ONT			
[SS] Servicios subcontratados			
[L] Instalaciones			
[P] Personal			
[Personal-01] Gerente de Servicios	[10]	[10]	[10]
[Personal-02] Gerente General	[9]	[9]	[9]
[Personal-03] Consultor Jr	[9]	[9]	[9]
[Perosonal-04] Ánalista de marketing digital	[7]	[7]	[7]
[Personal-05] Asistente de Gerencia	[7]	[7]	[7]

Figura 56 Valoración de activos
Fuente: Pilar 7.4.5

3.5.2 MAR.21 Caracterización de las amenazas

Dentro de la caracterización de las amenazas Pilar nos permite realizar una selección de factores agravantes que son una serie de calificativos al dominio que permiten establecer un perfil de vulnerabilidad, es decir ajustar el perfil de amenazas. En la tabla 16 se detalla los criterios.

Tabla 16 Factores agravantes

Criterios		
101		**Identificación del atacante**
	101.a	() público en general
	101.b	(5%) competidor comercial
	101.c	(5%) proveedor de servicios

	101.d	(5%) grupos de presión política / activistas / extremistas
	101.e	(5%) periodistas
	101.f	(8%) criminales / terroristas
	101.g	(10%) personal interno
	101.b	(10%) bandas criminales
	101.i	(10%) grupos terroristas
	101.j	(20%) servicios de inteligencia
		Motivación del atacante
102	102.a	(5%) económica (beneficios en dinero)
	102.b	(5%) beneficios comerciales
	102.c	(10%) personal propio con problemas de conciencia
	102.d	(10%) personal propio con problemas de intereses
	102.e	(30%) personal propio con pertenencia a un grupo extremista
	102.f	(5%) con ánimo destructivo
	102.g	(5%) con ánimo de causar daño
	102.h	(5%) con ánimo de provocar pérdidas
		Beneficio del atacante
103	103.a	(5%) moderadamente interesado
	103.b	(10%) muy interesado
	103.c	(20%) extremadamente interesado
		Atracción del objetivo
106	106.a	(-10%) objetivo muy poco atractivo
	106.b	(-5%) objetivo poco atractivo
	106.c	(5%) objetivo atractivo
	106.d	(10%) objetivo muy atractivo
	106.e	(15%) objetivo extremadamente atractivo
		Motivación del personal interno
104	104.a	(-10%) todo el personal está fuertemente motivado
	104.b	(5%) baja calificación personal / escasa formación
	104.c	(5%) sobrecargados de trabajo
	104.d	(10%) con problemas de conciencia
	104.e	(10%) con conflictos de interés
	104.f	(30%) personal asociado con grupos extremistas
		Permisos de los usuarios (derechos)
105	105.a	(10%) se permite el acceso al internet
	105.b	(20%) se permite la ejecución de programas sin autorización previa
	105.c	(30%) se permite la instalación de programas sin autorización previa
	105.d	(10%) se permite la conexión de dispositivos removibles
		Conectividad del sistema de información
111	111.a	(-20%) sistemas aislados

	111.b	() conectado con un conjunto reducido y controlado de redes
	111.c	(10%) conectado a un amplio colectivo de redes conocidas
	111.d	(30%) conectado a internet
		Ubicación del sistema de información
112	112.a	(-20%) dentro de una zona controlada
	112.b	(10%) en un área de acceso abierto
	112.c	(30%) de un entorno hostil
		Disponibilidad
301	301.l	(-90%) bajos requerimientos
	301.n	(-100%) ningún requisito
		Integridad
302	302.l	(-90%) bajos requerimientos
	302.n	(-100%) ningún requisito
		Confidencialidad
303	303.l	(-90%) bajos requerimientos
	303.n	(-100%) ningún requisito
		Autenticidad
304	304.l	(-90%) bajos requerimientos
	304.n	(-100%) ningún requisito
		Trazabilidad
305	305.l	(-90%) bajos requerimientos
	305.n	(-100%) ningún requisito

Fuente: Pilar 7.4.5

De los criterios de la tabla (16) se seleccionó los siguientes de acuerdo con el alcance y especificaciones de la organización que se observa en la tabla (17).

Tabla 17 Criterios seleccionados

Criterios seleccionados	
101.b	(5%) competidor comercial
101.g	(10%) personal interno
102.a	(5%) económica (beneficios en dinero)
102.b	(5%) beneficios comerciales
102.c	(10%) personal propio con problemas de conciencia
102.d	(10%) personal propio con problemas de intereses
102.f	(5%) con ánimo destructivo
102.g	(5%) con ánimo de causar daño
102.h	(5%) con ánimo de provocar pérdidas
103.b	(10%) muy interesado

106.d	(10%) objetivo muy atractivo
104.c	(5%) sobrecargados de trabajo
104.d	(10%) con problemas de conciencia
104.e	(10%) con conflictos de interés
105.a	(10%) se permite el acceso al internet
111.d	(30%) conectado a internet
112.a	(-20%) dentro de una zona controlada
301.l	(-90%) bajos requerimientos
302.l	(-90%) bajos requerimientos
303.l	(-90%) bajos requerimientos

Fuente: Pilar 7.4.5

En la herramienta Pilar se detalla en la figura 57.

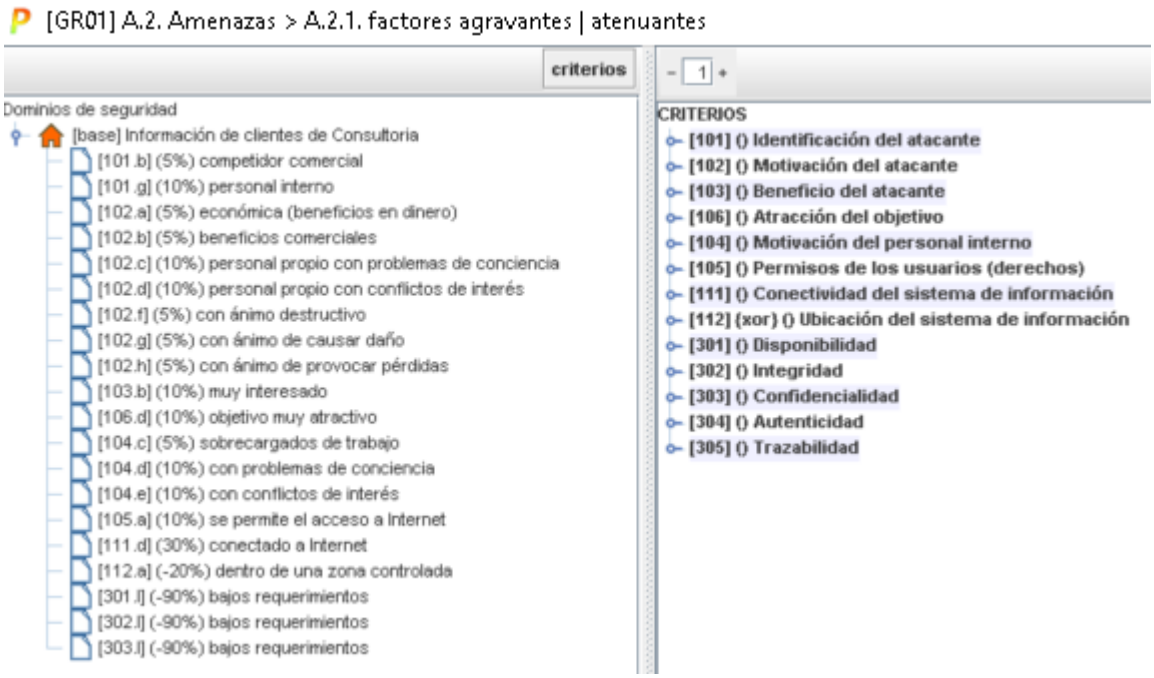


Figura 57 Factores agravantes
Fuente: Pilar 7.4.5

MAR.21 Identificación de las amenazas

El objetivo de esta tarea en específico es identificar las amenazas relevantes que atentan contra los activos, para esta tarea Pilar estandariza los criterios usados por Magerit y estos esta divididos en cinco grupos que son:

[N] Desastres naturales

[I] De origen industrial

[E] Errores y fallos no intencionados

[A] Ataques deliberados

[PR] Riesgos de privacidad

A continuación, en la tabla 18 se detalla cada activo con sus amenazas correspondientes.

Tabla 18 Identificación de las amenazas

Activos	Amenazas
Activos esenciales	
[Datos-01] Base de datos de clientes	[I.5] Avería de origen físico lógico [E.8] Difusión de software dañino [E.19] Fugas de información [E.20] Vulnerabilidades de los programas (software) [A.5] Suplantación de identidad [A.6] Abuso de privilegios de acceso [A.8] Difusión de software dañino [A.11] Acceso no autorizado [A.22] Manipulación de programas
[Datos-05] Información de clientes de auditoría	[E.19] Fugas de información [A.5] Suplantación de identidad [A.6] Abuso de privilegios de acceso [A.11] Acceso no autorizado
[Datos-06] Información de clientes de consultoría	[E.19] Fugas de información [A.5] Suplantación de identidad [A.6] Abuso de privilegios de acceso [A.11] Acceso no autorizado
[Datos-07] Base de datos de clientes soporte	[I.5] Avería de origen físico lógico [E.8] Difusión de software dañino [E.19] Fugas de información [E.20] Vulnerabilidades de los programas (software) [A.5] Suplantación de identidad [A.6] Abuso de privilegios de acceso [A.8] Difusión de software dañino [A.11] Acceso no autorizado [A.22] Manipulación de programas
[SW] Aplicaciones	
[Sw-01] Office 365	[I.5] Avería de origen físico lógico [E.8] Difusión de software dañino [E.20] Vulnerabilidades de los programas (software) [A.8] Difusión de software dañino [A.8] Difusión de software dañino
[Sw-02] FreshDesk	[E.19] Fugas de información

	[A.5] Suplantación de identidad
	[A.6] Abuso de privilegios de acceso
	[A.11] Acceso no autorizado
[Sw-03] Hubspot	[E.19] Fugas de información
	[A.5] Suplantación de identidad
	[A.6] Abuso de privilegios de acceso
	[A.11] Acceso no autorizado
[HW] Equipos	
[Hw-01] LPTP-GS-001	[N.1] Fuego
	[N.2] Daños por agua
	[N.*] Desastres naturales
	[I.1] Fuego
	[I.2] Daños por agua
	[I.*] Desastres industriales
	[I.3] Contaminación medioambiental
	[I.4] Contaminación electromagnética
	[I.5] Avería de origen físico o lógico
	[I.6] Corte de suministro eléctrico
	[I.7] Condiciones inadecuadas de temperatura o humedad
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)
	[E.24] Caída del sistema por agotamiento de recursos
	[E.25] Pérdida de equipos
	[A.7] Uso no previsto
	[A.11] Acceso no autorizado
	[A.23] Manipulación del hardware
	[A.24] Denegación de servicio
	[A.25] Robo de equipos
	[A.26] Ataque destructivo
[Hw-02] LPTP-GS-002	[N.1] Fuego
	[N.2] Daños por agua
	[N.*] Desastres naturales
	[I.1] Fuego
	[I.2] Daños por agua
	[I.*] Desastres industriales
	[I.3] Contaminación medioambiental
	[I.4] Contaminación electromagnética
	[I.5] Avería de origen físico o lógico
	[I.6] Corte de suministro eléctrico
	[I.7] Condiciones inadecuadas de temperatura o humedad
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)

	[E.24] Caída del sistema por agotamiento de recursos
	[E.25] Pérdida de equipos
	[A.7] Uso no previsto
	[A.11] Acceso no autorizado
	[A.23] Manipulación del hardware
	[A.24] Denegación de servicio
	[A.25] Robo de equipos
	[A.26] Ataque destructivo
[Hw-03] LPTP-GS-003	[N.1] Fuego
	[N.2] Daños por agua
	[N.*] Desastres naturales
	[I.1] Fuego
	[I.2] Daños por agua
	[I.*] Desastres industriales
	[I.3] Contaminación medioambiental
	[I.4] Contaminación electromagnética
	[I.5] Avería de origen físico o lógico
	[I.6] Corte de suministro eléctrico
	[I.7] Condiciones inadecuadas de temperatura o humedad
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)
	[E.24] Caída del sistema por agotamiento de recursos
	[E.25] Pérdida de equipos
	[A.7] Uso no previsto
	[A.11] Acceso no autorizado
	[A.23] Manipulación del hardware
	[A.24] Denegación de servicio
	[A.25] Robo de equipos
	[A.26] Ataque destructivo
[Hw-04] LPTP-GS-004	[N.1] Fuego
	[N.2] Daños por agua
	[N.*] Desastres naturales
	[I.1] Fuego
	[I.2] Daños por agua
	[I.*] Desastres industriales
	[I.3] Contaminación medioambiental
	[I.4] Contaminación electromagnética
	[I.5] Avería de origen físico o lógico
	[I.6] Corte de suministro eléctrico
	[I.7] Condiciones inadecuadas de temperatura o humedad
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)
	[E.24] Caída del sistema por agotamiento de recursos

	[E.25] Pérdida de equipos [A.7] Uso no previsto [A.11] Acceso no autorizado [A.23] Manipulación del hardware [A.24] Denegación de servicio [A.25] Robo de equipos [A.26] Ataque destructivo
[Hw-05] Desktop-01	[N.1] Fuego [N.2] Daños por agua [N.*] Desastres naturales [I.1] Fuego [I.2] Daños por agua [I.*] Desastres industriales [I.3] Contaminación medioambiental [I.4] Contaminación electromagnética [I.5] Avería de origen físico o lógico [I.6] Corte de suministro eléctrico [I.7] Condiciones inadecuadas de temperatura o humedad [E.23] Errores de mantenimiento / actualización de equipos (hardware) [E.24] Caída del sistema por agotamiento de recursos [E.25] Pérdida de equipos [A.7] Uso no previsto [A.11] Acceso no autorizado [A.23] Manipulación del hardware [A.24] Denegación de servicio [A.25] Robo de equipos [A.26] Ataque destructivo
[Hw-06] Impresora HP Color Jet MFP M477fdw	[N.1] Fuego [N.2] Daños por agua [N.*] Desastres naturales [I.1] Fuego [I.2] Daños por agua [I.*] Desastres industriales [I.3] Contaminación medioambiental [I.4] Contaminación electromagnética [I.5] Avería de origen físico o lógico [I.6] Corte de suministro eléctrico [I.7] Condiciones inadecuadas de temperatura o humedad [E.23] Errores de mantenimiento / actualización de equipos (hardware) [E.24] Caída del sistema por agotamiento de recursos [E.25] Pérdida de equipos

	[A.11] Acceso no autorizado
	[A.23] Manipulación del hardware
	[A.24] Denegación de servicio
	[A.25] Robo de equipos
	[A.26] Ataque destructivo
[COM] Comunicaciones	
[Com-01] Teléfono de Recepción	[I.8] Fallo de servicios de comunicaciones
	[E.2] Errores del administrador del sistema / de la seguridad
	[E.9] Errores de (re-)encaminamiento
	[E.10] Errores de secuencia
	[E.19] Fugas de información
	[E.24] Caída del sistema por agotamiento de recursos
	[A.5] Suplantación de identidad
	[A.7] Uso no previsto
	[A.9] (Re-)encaminamiento de mensajes
	[A.10] Alteración de secuencia
	[A.11] Acceso no autorizado
	[A.14] Interceptación de información (escucha)
	[A.15] Modificación de la información
	[A.18] Destrucción de la información
	[A.24] Denegación de servicio
[Com-02] Teléfono de Gerencia de servicios	[I.8] Fallo de servicios de comunicaciones
	[E.2] Errores del administrador del sistema / de la seguridad
	[E.9] Errores de (re-)encaminamiento
	[E.10] Errores de secuencia
	[E.19] Fugas de información
	[E.24] Caída del sistema por agotamiento de recursos
	[A.5] Suplantación de identidad
	[A.7] Uso no previsto
	[A.9] (Re-)encaminamiento de mensajes
	[A.10] Alteración de secuencia
	[A.11] Acceso no autorizado
	[A.14] Interceptación de información (escucha)
	[A.15] Modificación de la información
	[A.18] Destrucción de la información
	[A.24] Denegación de servicio
[Com-03] Teléfono área de ventas	[I.8] Fallo de servicios de comunicaciones
	[E.2] Errores del administrador del sistema / de la seguridad
	[E.9] Errores de (re-)encaminamiento
	[E.10] Errores de secuencia

	[E.19] Fugas de información [E.24] Caída del sistema por agotamiento de recursos [A.5] Suplantación de identidad [A.7] Uso no previsto [A.9] (Re-)encaminamiento de mensajes [A.10] Alteración de secuencia [A.11] Acceso no autorizado [A.14] Interceptación de información (escucha) [A.15] Modificación de la información [A.18] Destrucción de la información [A.24] Denegación de servicio
[Com-04] Teléfono de Gerencia General	[I.8] Fallo de servicios de comunicaciones [E.2] Errores del administrador del sistema / de la seguridad [E.9] Errores de (re-)encaminamiento [E.10] Errores de secuencia [E.19] Fugas de información [E.24] Caída del sistema por agotamiento de recursos [A.5] Suplantación de identidad [A.7] Uso no previsto [A.9] (Re-)encaminamiento de mensajes [A.10] Alteración de secuencia [A.11] Acceso no autorizado [A.14] Interceptación de información (escucha) [A.15] Modificación de la información [A.18] Destrucción de la información [A.24] Denegación de servicio
[Com-05] Teléfono área de capacitación	[I.8] Fallo de servicios de comunicaciones [E.2] Errores del administrador del sistema / de la seguridad [E.9] Errores de (re-)encaminamiento [E.10] Errores de secuencia [E.19] Fugas de información [E.24] Caída del sistema por agotamiento de recursos [A.5] Suplantación de identidad [A.7] Uso no previsto [A.9] (Re-)encaminamiento de mensajes [A.10] Alteración de secuencia [A.11] Acceso no autorizado [A.14] Interceptación de información (escucha) [A.15] Modificación de la información [A.18] Destrucción de la información [A.24] Denegación de servicio

[Com-06] Sistema Panasonic KX-TDA100D	[N.1] Fuego [N.2] Daños por agua [N.*] Desastres naturales [I.1] Fuego [I.2] Daños por agua [I.*] Desastres industriales [I.3] Contaminación medioambiental [I.4] Contaminación electromagnética [I.5] Avería de origen físico o lógico [I.6] Corte de suministro eléctrico [I.7] Condiciones inadecuadas de temperatura o humedad [I.8] Fallo de servicios de comunicaciones [E.2] Errores del administrador del sistema / de la seguridad [E.9] Errores de (re-)encaminamiento [E.10] Errores de secuencia [E.19] Fugas de información [E.23] Errores de mantenimiento / actualización de equipos (hardware) [E.24] Caída del sistema por agotamiento de recursos [E.25] Pérdida de equipos [A.5] Suplantación de identidad [A.7] Uso no previsto [A.9] (Re-)encaminamiento de mensajes [A.10] Alteración de secuencia [A.11] Acceso no autorizado [A.14] Interceptación de información (escucha) [A.15] Modificación de la información [A.18] Destrucción de la información [A.23] Manipulación del hardware [A.24] Denegación de servicio [A.25] Robo de equipos [A.26] Ataque destructivo
[Com-07] Router CISCO 800 SERIES	[N.1] Fuego [N.2] Daños por agua [N.*] Desastres naturales [L.1] Fuego [I.2] Daños por agua [I.*] Desastres industriales [I.3] Contaminación medioambiental [I.4] Contaminación electromagnética [I.5] Avería de origen físico o lógico [I.6] Corte de suministro eléctrico

	[I.7] Condiciones inadecuadas de temperatura o humedad
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)
	[E.24] Caída del sistema por agotamiento de recursos
	[E.25] Pérdida de equipos
	[A.7] Uso no previsto
	[A.11] Acceso no autorizado
	[A.23] Manipulación del hardware
	[A.24] Denegación de servicio
	[A.25] Robo de equipos
	[A.26] Ataque destructivo
[Com-08] Router inalámbrico	[N.1] Fuego
	[N.2] Daños por agua
	[N.*] Desastres naturales
	[I.1] Fuego
	[I.2] Daños por agua
	[I.*] Desastres industriales
	[I.3] Contaminación medioambiental
	[I.4] Contaminación electromagnética
	[I.5] Avería de origen físico o lógico
	[I.6] Corte de suministro eléctrico
	[I.7] Condiciones inadecuadas de temperatura o humedad
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)
	[E.24] Caída del sistema por agotamiento de recursos
	[E.25] Pérdida de equipos
	[A.7] Uso no previsto
	[A.11] Acceso no autorizado
	[A.23] Manipulación del hardware
	[A.24] Denegación de servicio
	[A.25] Robo de equipos
	[A.26] Ataque destructivo
[Com-09] ONT	[I.8] Fallo de servicios de comunicaciones
	[E.2] Errores del administrador del sistema / de la seguridad
	[E.9] Errores de (re-)encaminamiento
	[E.10] Errores de secuencia
	[E.19] Fugas de información
	[E.24] Caída del sistema por agotamiento de recursos
	[A.5] Suplantación de identidad
	[A.7] Uso no previsto
	[A.9] (Re-)encaminamiento de mensajes
	[A.10] Alteración de secuencia

	[A.11] Acceso no autorizado
	[A.14] Interceptación de información (escucha)
	[A.15] Modificación de la información
	[A.18] Destrucción de la información
	[A.24] Denegación de servicio
[P] Personal	
[Personal-01] Gerente de servicios	[E.15] Alteración de información
	[E.19] Fugas de información
	[A.15] Modificación de la información
	[A.18] Destrucción de la información
	[A.19] Revelación de información
	[A.28] Indisponibilidad del personal
	[A.29] Extorsión
	[A.30] Ingeniería social
[Personal-02] Gerente General	[E.15] Alteración de información
	[E.19] Fugas de información
	[E.28] Indisponibilidad del personal
	[A.15] Modificación de la información
	[A.18] Destrucción de la información
	[A.19] Revelación de información
	[A.28] Indisponibilidad del personal
	[A.29] Extorsión
	[A.30] Ingeniería social
[Personal-03] Consultor Jr	[E.15] Alteración de información
	[E.19] Fugas de información
	[E.28] Indisponibilidad del personal
	[A.15] Modificación de la información
	[A.18] Destrucción de la información
	[A.19] Revelación de información
	[A.28] Indisponibilidad del personal
	[A.29] Extorsión
	[A.30] Ingeniería social
[Personal-04] Analista de marketing digital	[E.15] Alteración de información
	[E.19] Fugas de información
	[E.28] Indisponibilidad del personal
	[A.15] Modificación de la información
	[A.18] Destrucción de la información
	[A.19] Revelación de información
	[A.28] Indisponibilidad del personal
	[A.29] Extorsión
	[A.30] Ingeniería social
Asistente de Gerencia	[E.15] Alteración de información
	[E.19] Fugas de información

	[E.28] Indisponibilidad del personal
	[A.15] Modificación de la información
	[A.18] Destrucción de la información
	[A.19] Revelación de información
	[A.28] Indisponibilidad del personal
	[A.29] Extorsión
	[A.30] Ingeniería social

Fuente: Pilar 7.4.5

En la herramienta Pilar se describe como se detalla en la figura 58.

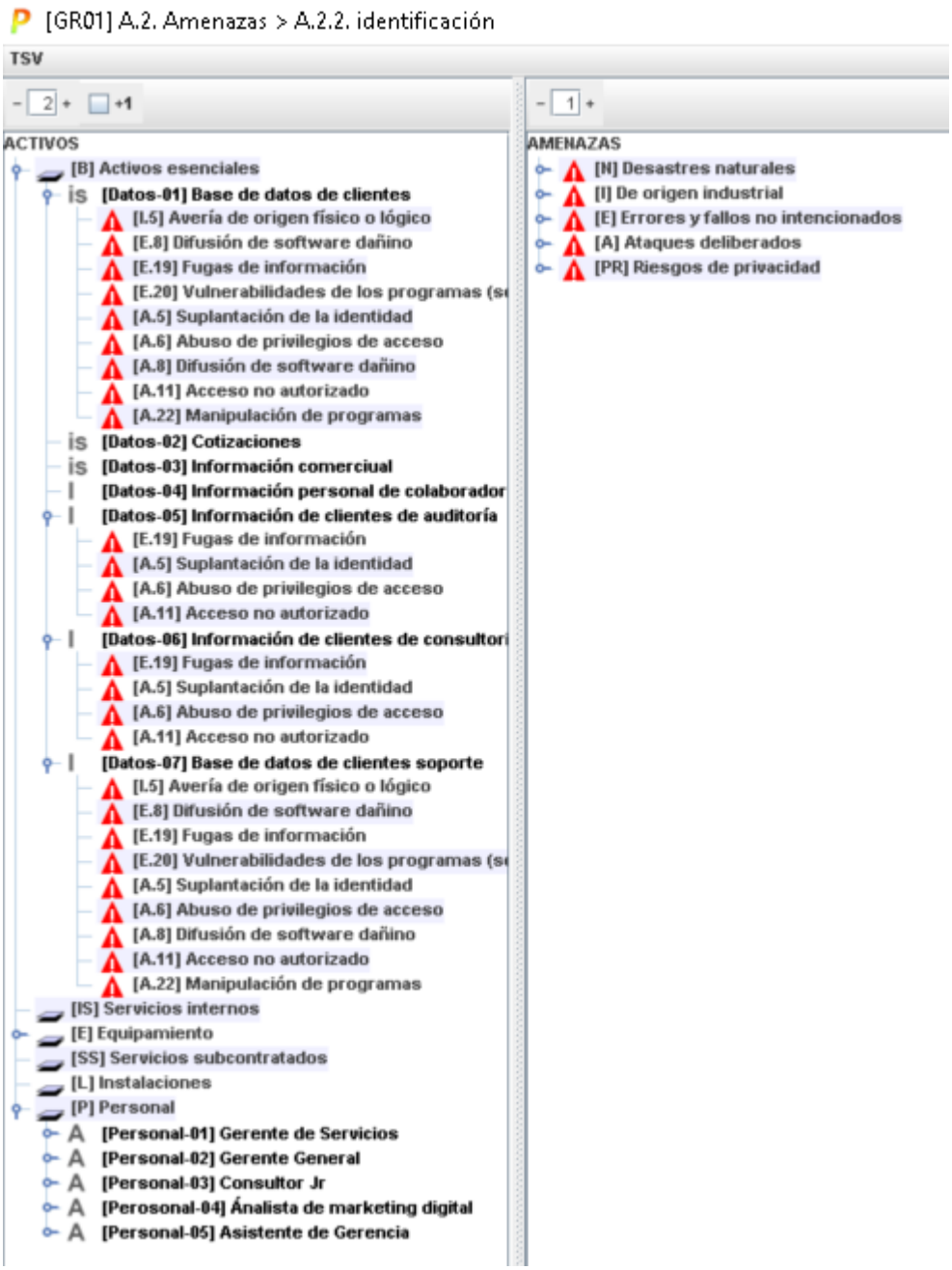


Figura 58 Identificación de amenazas
Fuente: Pilar 7.4.5

MAR.22 – Valoración de las amenazas

Una vez identificado las amenazas que pueden afectar a los activos de la organización se procedió a realizar la valoración de las amenazas basados en una escala nominal que son:

Evaluar la probabilidad de ocurrencia de cada amenaza concerniente a cada activo.

Estimar la degradación que causaría la amenaza en cada dimensión del activo si llegara a materializarse.

Para valorar las amenazas de cada activo se han tomado en cuenta la degradación de valor en la cual sus criterios se detalla en la tabla 19 y la probabilidad de ocurrencia que se detalla en la tabla 20.

Tabla 19 Degradación del valor

MA	MUY ALTA
A	ALTA
M	MEDIA
B	BAJA
MB	MUY BAJA

Fuente: Pilar 7.4.5

Tabla 20 Probabilidad de ocurrencia

CS	CASI SEGURO
MA	MUY ALTO
P	POSIBLE
PP	POCO PROBABLE
MB	SIGLOS
MR	MUY RARA

Fuente: Pilar 7.4.5

A continuación, se detalla en la tabla 21 la valoración de las amenazas.

Tabla 21 Valoración de amenazas

Activos	Amenazas	P	D	I	C
Activos esenciales					
[Datos-01] Base de datos de clientes	[I.5] Avería de origen físico lógico	P	M	−	B
	[E.8] Difusión de software dañino	P	B	B	B
	[E.19] Fugas de información	P	−	−	B
	[E.20] Vulnerabilidades de los programas (software)	P	−	B	M
	[A.5] Suplantación de identidad	MA	−	B	M
	[A.6] Abuso de privilegios de acceso	CS	−	B	M
	[A.8] Difusión de software dañino	P	M	M	M
	[A.11] Acceso no autorizado	CS	−	B	M
	[A.22] Manipulación de programas	MA	M	M	M
[Datos-05] Información de clientes de auditoría	[E.19] Fugas de información	P	−	−	B
	[A.5] Suplantación de identidad	MA	−	B	M
	[A.6] Abuso de privilegios de acceso	CS	−	B	M
	[A.11] Acceso no autorizado	CS	−	B	M
[Datos-06] Información de clientes de consultoría	[E.19] Fugas de información	P	−	−	B
	[A.5] Suplantación de identidad	MA	−	B	M
	[A.6] Abuso de privilegios de acceso	CS	−	B	M
	[A.11] Acceso no autorizado	CS	−	B	M
[Datos-07] Base de datos de clientes soporte	[I.5] Avería de origen físico lógico	P	M	−	−
	[E.8] Difusión de software dañino	P	B	B	B
	[E.19] Fugas de información	P	−	−	B
	[E.20] Vulnerabilidades de los programas (software)	P	−	B	B
	[A.5] Suplantación de identidad	MA	−	B	M
	[A.6] Abuso de privilegios de acceso	CS	−	B	M
	[A.8] Difusión de software dañino	P	M	M	M
	[A.11] Acceso no autorizado	CS	−	B	M
	[A.22] Manipulación de programas	MA	M	M	M
[SW] Aplicaciones					
[Sw-01] Office 365	[I.5] Avería de origen físico lógico	P	M	−	−
	[E.8] Difusión de software dañino	P	B	B	B
	[E.20] Vulnerabilidades de los programas (software)	P		B	B
	[A.8] Difusión de software dañino	P	M	M	M
	[A.8] Difusión de software dañino	MA	M	M	M
[Sw-02] FreshDesk	[E.19] Fugas de información	P	−	−	B
	[A.5] Suplantación de identidad	MA	−	B	M
	[A.6] Abuso de privilegios de acceso	CS	−	B	M
	[A.11] Acceso no autorizado	CS	−	B	M
[Sw-03] Hubspot	[E.19] Fugas de información	P	−		B
	[A.5] Suplantación de identidad	MA	−	B	M
	[A.6] Abuso de privilegios de acceso	CS	−	B	M
	[A.11] Acceso no autorizado	CS	−	B	M
[HW] Equipos					

[Hw-01] LPTP-GS-001	[N.1] Fuego	PP	M	–	–
	[N.2] Daños por agua	PP	M	–	–
	[N.*] Desastres naturales	PP	M	–	–
	[I.1] Fuego	P	M	–	–
	[I.2] Daños por agua	P	M	–	–
	[I.*] Desastres industriales	P	M	–	–
	[I.3] Contaminación medioambiental	PP	M	–	–
	[I.4] Contaminación electromagnética	P	B	–	–
	[I.5] Avería de origen físico o lógico	P	M	–	–
	[I.6] Corte de suministro eléctrico	P	M	–	–
	[I.7] Condiciones inadecuadas de temperatura o humedad	P	M	–	–
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	P	B	–	–
	[E.24] Caída del sistema por agotamiento de recursos	MA	M	–	–
	[E.25] Pérdida de equipos	MA		–	B
	[A.7] Uso no previsto	MA	B	–	B
	[A.11] Acceso no autorizado	P	B	B	M
	[A.23] Manipulación del hardware	P	M	–	M
	[A.24] Denegación de servicio	MA	M	–	–
	[A.25] Robo de equipos	MA	–	–	B
	[A.26] Ataque destructivo	P	M	–	–
[Hw-02] LPTP-GS-002	[N.1] Fuego	PP	M	–	–
	[N.2] Daños por agua	PP	M	–	–
	[N.*] Desastres naturales	PP	M	–	–
	[I.1] Fuego	P	M	–	–
	[I.2] Daños por agua	P	M	–	–
	[I.*] Desastres industriales	P	M	–	–
	[I.3] Contaminación medioambiental	PP	M	–	–
	[I.4] Contaminación electromagnética	P	B	–	–
	[I.5] Avería de origen físico o lógico	P	M	–	–
	[I.6] Corte de suministro eléctrico	P	M	–	–
	[I.7] Condiciones inadecuadas de temperatura o humedad	P	M	–	–
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	P	B	–	–
	[E.24] Caída del sistema por agotamiento de recursos	MA	M	–	–
	[E.25] Pérdida de equipos	MA	–	–	B
	[A.7] Uso no previsto	MA	B	–	B
	[A.11] Acceso no autorizado	P	B	B	M
	[A.23] Manipulación del hardware	P	M	–	M
	[A.24] Denegación de servicio	MA	M	–	–
	[A.25] Robo de equipos	MA	–	–	B
	[A.26] Ataque destructivo	P	M	–	–
[Hw-03] LPTP-GS-003	[N.1] Fuego	PP	M	–	–
	[N.2] Daños por agua	PP	M	–	–

	[N.*] Desastres naturales	PP	M	–	–
	[I.1] Fuego	P	M	–	–
	[I.2] Daños por agua	P	M	–	–
	[I.*] Desastres industriales	P	M	–	–
	[I.3] Contaminación medioambiental	PP	M	–	–
	[I.4] Contaminación electromagnética	P	B	–	–
	[I.5] Avería de origen físico o lógico	P	M	–	–
	[I.6] Corte de suministro eléctrico	P	M	–	–
	[I.7] Condiciones inadecuadas de temperatura o humedad	P	M	–	–
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	P	B	–	–
	[E.24] Caída del sistema por agotamiento de recursos	MA	M	–	–
	[E.25] Pérdida de equipos	MA	–	–	B
	[A.7] Uso no previsto	MA	B	–	B
	[A.11] Acceso no autorizado	P	B	B	M
	[A.23] Manipulación del hardware	P	M	–	M
	[A.24] Denegación de servicio	MA	M	–	–
	[A.25] Robo de equipos	MA	–	–	B
	[A.26] Ataque destructivo	P	M	–	–
[Hw-04] LPTP-GS-004	[N.1] Fuego	PP	M	–	–
	[N.2] Daños por agua	PP	M	–	–
	[N.*] Desastres naturales	PP	M	–	–
	[I.1] Fuego	P	M	–	–
	[I.2] Daños por agua	P	M	–	–
	[I.*] Desastres industriales	P	M	–	–
	[I.3] Contaminación medioambiental	PP	M	–	–
	[I.4] Contaminación electromagnética	P	B	–	–
	[I.5] Avería de origen físico o lógico	P	M	–	–
	[I.6] Corte de suministro eléctrico	P	M	–	–
	[I.7] Condiciones inadecuadas de temperatura o humedad	P	M	–	–
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	P	B	–	–
	[E.24] Caída del sistema por agotamiento de recursos	MA	M	–	–
	[E.25] Pérdida de equipos	MA	–	–	B
	[A.7] Uso no previsto	MA	B	–	B
	[A.11] Acceso no autorizado	P	B	B	M
	[A.23] Manipulación del hardware	P	M	–	M
	[A.24] Denegación de servicio	MA	M	–	–
	[A.25] Robo de equipos	MA	–	–	B
	[A.26] Ataque destructivo	P	M	–	–
[Hw-05] Desktop-01	[N.1] Fuego	PP	M	–	–
	[N.2] Daños por agua	PP	M	–	–
	[N.*] Desastres naturales	PP	M	–	–
	[I.1] Fuego	P	M	–	–

	[I.2] Daños por agua	P	M	–	–
	[I.*] Desastres industriales	P	M	–	–
	[I.3] Contaminación medioambiental	PP	M	–	–
	[I.4] Contaminación electromagnética	P	B	–	–
	[I.5] Avería de origen físico o lógico	P	M	–	–
	[I.6] Corte de suministro eléctrico	P	M	–	–
	[I.7] Condiciones inadecuadas de temperatura o humedad	P	M	–	–
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	P	B	–	–
	[E.24] Caída del sistema por agotamiento de recursos	MA	M	–	–
	[E.25] Pérdida de equipos	P	M	–	M
	[A.6] Abuso de privilegios de acceso	MA	B	M	M
	[A.7] Uso no previsto	MA	B	B	M
	[A.11] Acceso no autorizado	P	B	M	M
	[A.24] Denegación de servicio	MA	M	–	–
	[A.25] Robo de equipos	P	M	–	M
	[A.26] Ataque destructivo	P	M	–	–
[Hw-06] Impresora HP Color Jet MFP M477fdw	[N.1] Fuego	PP	M	–	–
	[N.2] Daños por agua	PP	M	–	–
	[N.*] Desastres naturales	PP	M	–	–
	[I.1] Fuego	P	M	–	–
	[I.2] Daños por agua	P	M	–	–
	[I.*] Desastres industriales	P	M	–	–
	[I.3] Contaminación medioambiental	PP	M	–	–
	[I.4] Contaminación electromagnética	P	B	–	–
	[I.5] Avería de origen físico o lógico	P	M	–	–
	[I.6] Corte de suministro eléctrico	P	M	–	–
	[I.7] Condiciones inadecuadas de temperatura o humedad	P	M	–	–
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	P	B	–	–
	[E.24] Caída del sistema por agotamiento de recursos	MA	M	–	–
	[E.25] Pérdida de equipos	P	M	–	M
	[A.11] Acceso no autorizado	P	B	B	M
	[A.23] Manipulación del hardware	P	M	–	M
	[A.24] Denegación de servicio	MA	M	–	–
	[A.25] Robo de equipos	P	M	–	M
	[A.26] Ataque destructivo	P	M	–	–
	[COM] Comunicaciones				
[Com-01] Teléfono de Recepción	[I.8] Fallo de servicios de comunicaciones	P	M	–	B
	[E.2] Errores del administrador del sistema / de la seguridad	P	B	B	B
	[E.9] Errores de (re-)encaminamiento	P	–	–	–
	[E.10] Errores de secuencia	P	–	B	B
	[E.19] Fugas de información	P	–	–	–
	[E.24] Caída del sistema por agotamiento de recursos	P	M	–	M

	[A.5] Suplantación de identidad	P	−	B	B
	[A.7] Uso no previsto	MA	B	B	B
	[A.9] (Re-)encaminamiento de mensajes	P	−	−	−
	[A.10] Alteración de secuencia	P	−	B	M
	[A.11] Acceso no autorizado	P	−	B	B
	[A.14] Interceptación de información (escucha)	P	−	−	−
	[A.15] Modificación de la información	P	−	B	−
	[A.18] Destrucción de la información	P	M	−	−
	[A.24] Denegación de servicio	CS	M	−	−
[Com-02] Teléfono de Gerencia de servicios	[I.8] Fallo de servicios de comunicaciones	P	M	−	−
	[E.2] Errores del administrador del sistema / de la seguridad	P	B	B	B
	[E.9] Errores de (re-)encaminamiento	P	−	−	B
	[E.10] Errores de secuencia	P	−	B	−
	[E.19] Fugas de información	P	−	−	B
	[E.24] Caída del sistema por agotamiento de recursos	P	M	−	−
	[A.5] Suplantación de identidad	MA		B	M
	[A.7] Uso no previsto	P	B	B	B
	[A.9] (Re-)encaminamiento de mensajes	P	−	−	B
	[A.10] Alteración de secuencia	P	−	B	−
	[A.11] Acceso no autorizado	P	−	B	M
	[A.14] Interceptación de información (escucha)	P	−	−	B
	[A.15] Modificación de la información	P	−	B	−
	[A.18] Destrucción de la información	P	M	−	−
	[A.24] Denegación de servicio	CS	M	−	−
[Com-03] Teléfono área de ventas	[I.8] Fallo de servicios de comunicaciones	P	M	−	−
	[E.2] Errores del administrador del sistema / de la seguridad	P	B	B	B
	[E.9] Errores de (re-)encaminamiento	P	−	−	B
	[E.10] Errores de secuencia	P	−	B	−
	[E.19] Fugas de información	P	−	−	B
	[E.24] Caída del sistema por agotamiento de recursos	P	M	−	−
	[A.5] Suplantación de identidad	MA	−	B	M
	[A.7] Uso no previsto	P	B	B	B
	[A.9] (Re-)encaminamiento de mensajes	P	−	−	B
	[A.10] Alteración de secuencia	P	−	B	
	[A.11] Acceso no autorizado	P	−	B	M
	[A.14] Interceptación de información (escucha)	P	−	−	B
	[A.15] Modificación de la información	P	−	B	−
	[A.18] Destrucción de la información	P	M	−	−
	[A.24] Denegación de servicio	CS	M	−	−
[Com-04] Teléfono de Gerencia General	[I.8] Fallo de servicios de comunicaciones	P	M	−	−
	[E.2] Errores del administrador del sistema / de la seguridad	P	B	B	B
	[E.9] Errores de (re-)encaminamiento	P	−	−	B
	[E.10] Errores de secuencia	P	−	B	−
	[E.19] Fugas de información	P	−	−	B
	[E.24] Caída del sistema por agotamiento de recursos	P	M	−	−

	[A.5] Suplantación de identidad	MA	−	B	M
	[A.7] Uso no previsto	P	B	B	B
	[A.9] (Re-)encaminamiento de mensajes	P	−	−	B
	[A.10] Alteración de secuencia	P	−	B	−
	[A.11] Acceso no autorizado	P	−	B	M
	[A.14] Interceptación de información (escucha)	P	−	−	B
	[A.15] Modificación de la información	P	−	B	−
	[A.18] Destrucción de la información	P	M	−	−
	[A.24] Denegación de servicio	CS	M	−	−
[Com-05] Teléfono área de capacitación	[I.8] Fallo de servicios de comunicaciones	P	M	−	−
	[E.2] Errores del administrador del sistema / de la seguridad	P	B	B	B
	[E.9] Errores de (re-)encaminamiento	P	−	−	B
	[E.10] Errores de secuencia	P	−	B	
	[E.19] Fugas de información	P	−	−	B
	[E.24] Caída del sistema por agotamiento de recursos	P	M	−	−
	[A.5] Suplantación de identidad	MA	−	B	M
	[A.7] Uso no previsto	P	B	B	B
	[A.9] (Re-)encaminamiento de mensajes	P	−	−	B
	[A.10] Alteración de secuencia	P	−	B	−
	[A.11] Acceso no autorizado	P	−	B	M
	[A.14] Interceptación de información (escucha)	P	−	−	B
	[A.15] Modificación de la información	P	−	B	−
	[A.18] Destrucción de la información	P	M	−	−
	[A.24] Denegación de servicio	CS	M	−	−
[Com-06] Sistema Panasonic KX-TDA100D	[N.1] Fuego	PP	M	−	−
	[N.2] Daños por agua	PP	M	−	−
	[N.*] Desastres naturales	PP	M	−	−
	[I.1] Fuego	P	M	−	−
	[I.2] Daños por agua	P	M	−	−
	[I.*] Desastres industriales	P	M	−	−
	[I.3] Contaminación medioambiental	PP	M	−	−
	[I.4] Contaminación electromagnética	P	B	−	−
	[I.5] Avería de origen físico o lógico	P	M	−	−
	[I.6] Corte de suministro eléctrico	P	M	−	−
	[I.7] Condiciones inadecuadas de temperatura o humedad	P	M	−	−
	[I.8] Fallo de servicios de comunicaciones	P	M	−	−
	[E.2] Errores del administrador del sistema / de la seguridad	P	B	B	B
	[E.9] Errores de (re-)encaminamiento	P	−	−	B
	[E.10] Errores de secuencia	P		B	−
	[E.19] Fugas de información	P	−	−	B
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	P	B	−	−
	[E.24] Caída del sistema por agotamiento de recursos	MA	M	−	−
	[E.25] Pérdida de equipos	P	M	−	M
	[A.5] Suplantación de identidad	P	−	B	M

[Com-07] Router CISCO 800 SERIES	[A.7] Uso no previsto	MA	B	B	B
	[A.9] (Re-)encaminamiento de mensajes	P	−	−	B
	[A.10] Alteración de secuencia	P	−	B	−
	[A.11] Acceso no autorizado	P	B	B	M
	[A.14] Interceptación de información (escucha)	P	−	−	B
	[A.15] Modificación de la información	P	−	B	−
	[A.18] Destrucción de la información	P	M	−	−
	[A.23] Manipulación del hardware	P	M	−	M
	[A.24] Denegación de servicio	CS	M	−	−
	[A.25] Robo de equipos	P	M	−	M
	[A.26] Ataque destructivo	P	M	−	−
	[N.1] Fuego	PP	M	−	−
	[N.2] Daños por agua	PP	M	−	−
	[N.*] Desastres naturales	PP	M	−	−
	[I.1] Fuego	P	M	−	−
	[I.2] Daños por agua	P	M	−	−
	[I.*] Desastres industriales	P	M	−	−
	[I.3] Contaminación medioambiental	PP	M	−	−
	[I.4] Contaminación electromagnética	P	B	−	−
	[I.5] Avería de origen físico o lógico	P	M	−	−
	[I.6] Corte de suministro eléctrico	P	M	−	−
	[I.7] Condiciones inadecuadas de temperatura o humedad	P	M	−	−
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	P	B	−	−
	[E.24] Caída del sistema por agotamiento de recursos	MA	M	−	−
	[E.25] Pérdida de equipos	P	B	−	M
	[A.7] Uso no previsto	MA	B	−	B
	[A.11] Acceso no autorizado	P	B	B	M
	[A.23] Manipulación del hardware	P	M	−	M
	[A.24] Denegación de servicio	MA	M	−	−
	[A.25] Robo de equipos	P	B	−	M
	[A.26] Ataque destructivo	P	M	−	−
[Com-08] Router inalámbrico	[N.1] Fuego	PP	M	−	−
	[N.2] Daños por agua	PP	M	−	−
	[N.*] Desastres naturales	PP	M	−	−
	[I.1] Fuego	P	M	−	−
	[I.2] Daños por agua	P	M	−	−
	[I.*] Desastres industriales	P	M	−	−
	[I.3] Contaminación medioambiental	PP	M	−	−
	[I.4] Contaminación electromagnética	P	B	−	−
	[I.5] Avería de origen físico o lógico	P	M	−	−
	[I.6] Corte de suministro eléctrico	P	M	−	−
	[I.7] Condiciones inadecuadas de temperatura o humedad	P	M	−	−

	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	P	B	–	–
	[E.24] Caída del sistema por agotamiento de recursos	MA	M	–	–
	[E.25] Pérdida de equipos	P	B	–	M
	[A.7] Uso no previsto	MA	B	–	B
	[A.11] Acceso no autorizado	P	B	B	M
	[A.23] Manipulación del hardware	P	M	–	M
	[A.24] Denegación de servicio	MA	M	–	–
	[A.25] Robo de equipos	P	B	–	M
	[A.26] Ataque destructivo	P	M	–	–
[Com-09] ONT	[I.8] Fallo de servicios de comunicaciones	P	M	–	–
	[E.2] Errores del administrador del sistema / de la seguridad	P	B	B	B
	[E.9] Errores de (re-)encaminamiento	P	–	–	B
	[E.10] Errores de secuencia	P	–	B	–
	[E.19] Fugas de información	P	–	–	B
	[E.24] Caída del sistema por agotamiento de recursos	P	M	–	–
	[A.5] Suplantación de identidad	P	–	B	M
	[A.7] Uso no previsto	MA	B	B	B
	[A.9] (Re-)encaminamiento de mensajes	P	–	–	B
	[A.10] Alteración de secuencia	P	–	B	
	[A.11] Acceso no autorizado	P	–	B	M
	[A.14] Interceptación de información (escucha)	P	–	–	B
	[A.15] Modificación de la información	P	–	B	–
	[A.18] Destrucción de la información	P	M	–	–
	[A.24] Denegación de servicio	CS	M	–	–
	[P] Personal				
[Personal-01] Gerente de servicios	[E.15] Alteración de información	P	–	B	–
	[E.19] Fugas de información	P	–	–	B
	[A.15] Modificación de la información	P	–	M	–
	[A.18] Destrucción de la información	P	B	–	–
	[A.19] Revelación de información	MA	–	–	M
	[A.28] Indisponibilidad del personal	P	B	–	–
	[A.29] Extorsión	P	M	M	M
	[A.30] Ingeniería social	P	M	M	M
[Personal-02] Gerente General	[E.15] Alteración de información	P	–	B	–
	[E.19] Fugas de información	P	–	–	B
	[E.28] Indisponibilidad del personal	P	B	–	–
	[A.15] Modificación de la información	P	–	M	–
	[A.18] Destrucción de la información	P	B	–	–
	[A.19] Revelación de información	MA	–	–	B
	[A.28] Indisponibilidad del personal	P	M	–	–
	[A.29] Extorsión	P	B	B	B
	[A.30] Ingeniería social	P	B	B	B
[Personal-03] Consultor Jr	[E.15] Alteración de información	P	–	B	–

	[E.19] Fugas de información	P	–	–	B
	[E.28] Indisponibilidad del personal	P	B	–	–
	[A.15] Modificación de la información	P	–	M	–
	[A.18] Destrucción de la información	P	B	–	–
	[A.19] Revelación de información	MA	–	–	M
	[A.28] Indisponibilidad del personal	P	B	–	–
	[A.29] Extorsión	P	M	M	M
	[A.30] Ingeniería social	P	M	M	M
[Personal-04] Analista de marketing digital	[E.15] Alteración de información	P	–	B	–
	[E.19] Fugas de información	P	–	–	B
	[E.28] Indisponibilidad del personal	P	B	–	–
	[A.15] Modificación de la información	P	–	M	–
	[A.18] Destrucción de la información	P	B	–	–
	[A.19] Revelación de información	MA	–	–	B
	[A.28] Indisponibilidad del personal	P	M	–	–
	[A.29] Extorsión	P	B	B	B
	[A.30] Ingeniería social	P	B	B	B
Asistente de Gerencia	[E.15] Alteración de información	P	–	B	–
	[E.19] Fugas de información	P	–	–	B
	[E.28] Indisponibilidad del personal	P	B	–	–
	[A.15] Modificación de la información	P	–	M	–
	[A.18] Destrucción de la información	P	B	–	–
	[A.19] Revelación de información	MA	–	–	B
	[A.28] Indisponibilidad del personal	P	M	–	–
	[A.29] Extorsión	P	B	B	B
	[A.30] Ingeniería social	P	B	B	B

Fuente: Pilar 7.4.5

3.5.3 MAR.3- Caracterización de las salvaguardas

Según la Metodología (Magerit V3 Libro 1, 2019) es tomada la siguiente información.

Se definen las salvaguardas o contra medidas como aquellos procedimientos o mecanismos tecnológicos que reducen el riesgo. Hay amenazas que se conjuran simplemente organizándose adecuadamente, otras requieren elementos técnicos (programas o equipos), otra seguridad física y, por último, está la política de personal.

Magerit y Pilar definen aspectos para clasificar las salvaguardas como se detalla en la tabla 22.

Tabla 22 Aspectos de las salvaguardas

G	para Gestión
T	para Técnico
F	para seguridad Física
P	para gestión del Personal

Fuente: Pilar 7.4.5

También Magerit y Pilar definen los tipos de protección que se definen a continuación.

Tipo de protección

Esta aproximación a veces resulta un poco simplificadora, pues es habitual hablar de diferentes tipos de protección prestados por las salvaguardas:

[PR] prevención Diremos que una salvaguarda es preventiva cuando reduce las oportunidades de que un incidente ocurra. Si la salvaguarda falla y el incidente llega a ocurrir, los daños son los mismos.

[DR] disuasión Diremos que una salvaguarda es disuasoria cuando tiene un efecto tal sobre los atacantes que estos no se atreven o se lo piensan dos veces antes de atacar. Son salvaguardas que actúan antes del incidente, reduciendo las probabilidades de que ocurra; pero que no tienen influencia sobre los daños causados caso de que el atacante realmente se atreva.

[EL] eliminación Diremos que una salvaguarda elimina un incidente cuando impide que éste tenga lugar. Son salvaguardas que actúan antes de que el incidente se haya producido. No reducen los daños caso de que la salvaguarda no sea perfecta y el incidente llegue a ocurrir.

[IM] minimización del impacto / limitación del impacto Se dice que una salvaguarda minimiza o limita el impacto cuando acota las consecuencias de un incidente.

[CR] corrección Diremos que una salvaguarda es correctiva cuando, habiéndose producido un daño, lo repara. Son salvaguardas que actúan después de que el incidente se haya producido y por tanto reducen los daños.

[RC] recuperación Diremos que una salvaguarda ofrece recuperación cuando permite regresar al estado anterior al incidente. Son salvaguardas que no reducen las probabilidades del incidente, pero acotan los daños a un periodo de tiempo.

[MN] monitorización Son las salvaguardas que trabajan monitorizando lo que está ocurriendo o lo que ha ocurrido. Si se detectan cosas en tiempo real, podemos reaccionar atajando el incidente para limitar el impacto; si se detectan cosas a posteriori, podemos aprender del incidente y mejorar el sistema de salvaguardas de cara al futuro.

[DC] detección Diremos que una salvaguarda funciona detectando un ataque cuando informa de que el ataque está ocurriendo. Aunque no impide el ataque, sí permite que entren en operación otras medidas que atajen la progresión del ataque, minimizando daños.

[AW] concienciación Son las actividades de formación de las personas anexas al sistema que pueden tener una influencia sobre él. La formación reduce los errores de los usuarios, lo cual tiene un efecto preventivo. También mejora las salvaguardas de todo tipo pues los que las operan lo hacen con eficacia y rapidez, potenciando su efecto o, al menos, no menoscabándolo por una mala operación.

[AD] administración Se refiere a las salvaguardas relacionadas con los componentes de seguridad del sistema. Una buena administración evita el desconocimiento de lo que hay y por tanto impide que haya puertas desconocidas por las que pudiera tener éxito un ataque. En general pueden considerarse medidas de tipo preventivo.

La tabla 22 relaciona cada uno de estos tipos de protección con el modelo anterior de reducción de la degradación y de la probabilidad:

Tabla 23 Tipos de salvaguardas

Efecto	Tipo
Preventivas: reducen la probabilidad	[PR] preventivas [DR] disuasorias [EL] eliminatorias
Acotan la degradación	[IM] minimizadoras [CR] correctivas [RC] recuperativas

Consolidan el efecto de las demás	[MN] de monitorización [DC] de detección [AW] de concienciación [AD] administrativas

Fuente: Magerit 2019

Eficacia de la protección se establece en rangos de madurez actuales y rangos objetivos que se definen en la tabla 24.

Tabla 24 Madurez de las salvaguardas

L0 - inexistente	No se cuenta dentro de la organización
L1 - inicial	En fase inicial, empezando
L2 - Reproducible, pero intuitivo	En mejora continua
L3 - Proceso definido	Documentado
L4 - Gestionado y medible	Aplicable y medible
L5 - Optimizado	Revisado y comprobado

Fuente: Magerit 2019

Teniendo en cuenta todos estos aspectos se obtuvo la información de la organización indicando las salvaguardas con su respectiva valoración en madurez como se detalla en la tabla 25.

Tabla 25 Valoración de las salvaguardas

SALVAGUARDAS	Descripción	Actual	Objetivo
[IA] Identificación y autenticación	Se dispone de una normativa de identificación, autenticación junto a sus procedimientos.	L3 - Proceso definido	L4 - Gestionado y medible
[AC] Control de acceso lógico	Política que asegure el acceso lógico a sus sistemas, pc, oficinas, etc.	L3 - Proceso definido	L4 - Gestionado y medible
[D] Protección de la Información	Política que asegure la información de la organización.	L1 - inicial	L4 - Gestionado y medible
[K] Protección de claves criptográficas	Política que exija el uso de claves criptográficas.	L0 - inexistente	L4 - Gestionado y medible
[S] Protección de los Servicios	Política que proteja los servicios de Consultoría.	L0 - inexistente	L4 - Gestionado y medible
[HW] Protección de los Equipos Informáticos (HW)	Hardware existente para proteger los equipos informáticos.	L1 - inicial	L4 - Gestionado y medible
[COM] Protección de las Comunicaciones	Hardware existente para proteger los equipos de comunicación.	L1 - inicial	L4 - Gestionado y medible
[IP] Sistema de protección de frontera lógica	Firewalls, etc.	L0 - inexistente	L4 - Gestionado y medible
[PPE] Protección física de los equipos	Política que regule el uso de protección física al hardware que contenga la información de consultoría.	L1 - inicial	L4 - Gestionado y medible
[L] Protección de las Instalaciones	Implementos físicos para la protección de las oficinas de la organización.	L1 - inicial	L4 - Gestionado y medible
[PPS] Protección del perímetro físico	Alarmas, etc.	L0 - inexistente	L4 - Gestionado y medible
[PS] Gestión del Personal	Política que regule el acceso del personal a la información de Consultoría.	L1 - inicial	L4 - Gestionado y medible

[IR] Gestión de incidentes	Política que gestione los incidentes informáticos relacionados con la información de Consultoría.	L0 - inexistente	L4 - Gestionado y medible
[tolos] Herramientas de seguridad	Herramientas para proteger la información de Consultoría.	L0 - inexistente	L4 - Gestionado y medible
[V] Gestión de vulnerabilidades	Implementación de gestión de vulnerabilidades.	L0 - inexistente	L4 - Gestionado y medible
[A] Registro y auditoría	Gestión de riesgos informáticos y auditoría.	L1 - inicial	L4 - Gestionado y medible
[BC] Continuidad del negocio	Plan de continuidad del negocio.	L0 - inexistente	L4 - Gestionado y medible

Fuente: Pilar 7.4.5

En la herramienta Pilar se detalla en la figura 59.

[GR01] A.3. Medidas técnicas y o ... > A.3.1. valoración (fases)

Editar Expandir Ver Exportar Importar Estadísticas

[base] Información de clientes de Consultoria

	aspecto	tdp	recomend...			current	target	PILAR
					SALVAGUARDAS	L0-L3	L4	L2-L5
	G	EL	9		[IA] Identificación y autenticación	L3	L4	L2-L5
	T	EL	7		[AC] Control de acceso lógico	L3	L4	L2-L4
	G	PR	7		[D] Protección de la Información	L1	L4	L2-L4
	G	EL			[K] Protección de claves criptográficas	L0	L4	n.a.
	G	PR			[S] Protección de los Servicios	L0	L4	n.a.
	G	PR	7		[SW] Protección de las Aplicaciones Informáticas (SW)	L1	L4	L2-L4
	G	PR	7		[HW] Protección de los Equipos Informáticos (HW)	L1	L4	L2-L4
	G	PR	8		[COM] Protección de las Comunicaciones	L1	L4	L2-L5
	G	PR			[IP] Sistema de protección de frontera lógica	L0	L4	n.a.
	G	PR			[MP] Protección de los Soportes de Información	n.a.	n.a.	n.a.
	G	PR	5		[AUX] Elementos Auxiliares	n.a.	n.a.	L2-L3
	F	EL	5		[PPE] Protección física de los equipos	L1	L4	L3
	F	PR			[L] Protección de las Instalaciones	L1	L4	n.a.
	F	EL			[PPS] Protección del perímetro físico	L0	L4	n.a.
	P	PR	6		[PS] Gestión del Personal	L1	L4	L2-L4
	G	PR			[PDS] Servicios potencialmente peligrosos	n.a.	n.a.	n.a.
	G	CR	6		[IR] Gestión de incidentes	L0	L4	L2-L4
	T	PR	8		[tools] Herramientas de seguridad	L0	L4	L2-L5
	G	CR	6		[V] Gestión de vulnerabilidades	L0	L4	L2-L4
	T	MN			[A] Registro y auditoría	L1	L4	n.a.
	G	RC	5		[BC] Continuidad del negocio	L0	L4	L2-L3
	G	AD	5		[G] Organización	n.a.	n.a.	L2-L3
	G	AD	6		[E] Relaciones Externas	n.a.	n.a.	L3-L4

Figura 59 Valoración de las salvaguardas
Fuente: Pilar 7.4.5

En la herramienta Pilar se identificó los activos, se valorizo dichos activos, se identificó las amenazas, se valorizó, se identificó las salvaguardas y por último se las valorizó encontrando así que el siguiente paso en la herramienta Pilar es el impacto y le riesgo a los que se encuentran sometidos los activos de la organización.

3.5.4 MAR.4- Estimación del estado del riesgo

Impacto repercutido

Es el calculado sobre un activo teniendo en cuenta su valor propio y las amenazas a que están expuestos los activos de los que depende El impacto repercutido se calcula para cada activo, por cada amenaza y en cada dimensión de valoración, siendo una función del valor propio y de la degradación causada. El impacto es tanto mayor cuanto mayor es el valor propio de un activo. El impacto es tanto mayor cuanto mayor sea la degradación del activo atacado. El impacto es tanto mayor cuanto mayor sea la dependencia del activo atacado. El impacto repercutido, al calcularse sobre los activos que tienen valor propio, permite determinar las consecuencias de las incidencias técnicas sobre la misión del sistema de información. Es pues una presentación gerencial que ayuda a tomar una de las decisiones críticas de un análisis de riesgos: aceptar un cierto nivel de riesgo.

Pilar nos define unos criterios basados en colores que se observan en la figura para la respectiva presentación del impacto repercutido en la figura 60.

Figura 60 Leyenda de impacto repercutido
Fuente: Pilar 7.4.5

El valor repercutido del impacto es el que se detalla en la figura 61.

[GR01] A.5.2. Valores repercutid ... > A.5.2.1. impacto

Exportar

potencial | current | target | PILAR

activo	[D]	[I]	[C]
ACTIVOS	[7]	[10]	[10]
[Datos-01] Base de datos de clientes	[6]	[9]	[9]
[Datos-02] Cotizaciones	[6]	[9]	[9]
[Datos-03] Información comerciual	[4]	[9]	[9]
[Datos-04] Información personal de colaboradores	[5]	[8]	[9]
[Datos-05] Información de clientes de auditoría	[6]	[9]	[9]
[Datos-06] Información de clientes de consultoría	[7]	[10]	[10]
[Datos-07] Base de datos de clientes soporte	[6]	[9]	[9]
[Sw-01] Office 365	[5]	[6]	[5]
[Sw-02] FreshDesk		[1]	[3]
[Sw-03] Hubspot		[1]	[3]
[Hw-01] LTPT-GS-001	[5]	[2]	[4]
[Hw-02] LPTP-GS-002	[7]	[4]	[6]
[Hw-03] LPTP-GS-003	[5]	[2]	[4]
[Hw-04] LPTP-GS-004	[5]	[2]	[4]
[Hw-05] Desktop-01	[5]	[5]	[5]
[Hw-06] Impresora HP Color Jet MFP M477fdw	[1]	[0]	[0]
[Com-01] Teléfono de Recepción	[0]	[0]	[0]
[Com-02] Teléfono de Gerencia de servicios	[0]	[0]	[0]
[Com-03] Teléfono área de ventas	[0]	[0]	[0]
[Com-04] Teléfono de Gerencia General	[0]	[0]	[0]
[Com-05] Teléfono área de capacitación	[0]	[0]	[0]
[Com-06] Sistema Panasonic KX-TDA100D	[1]	[0]	[0]
[Com-07] Router CISCO 800 SERIES	[5]	[2]	[4]
[Com-08] Router inalámbrico	[6]	[3]	[5]
[Com-09] ONT	[0]	[0]	[0]
[Personal-01] Gerente de Servicios	[6]	[7]	[7]
[Personal-02] Gerente General	[5]	[5]	[4]
[Personal-03] Consultor Jr	[5]	[6]	[6]
[Perosonal-04] Ánalista de marketing digital	[3]	[3]	[2]
[Personal-05] Asistente de Gerencia	[3]	[3]	[2]

Figura 61 *Impacto repercutido*
Fuente: Pilar 7.4.5

Riesgo repercutido

Es el calculado sobre un activo teniendo en cuenta el impacto repercutido sobre un activo debido a una amenaza y la probabilidad de la amenaza El riesgo repercutido se calcula para cada activo, por cada amenaza y en cada dimensión de valoración, siendo una función del valor propio, la degradación causada y la probabilidad de la amenaza. El riesgo repercutido, al calcularse sobre los activos que tienen valor propio, permite determinar las consecuencias de las incidencias técnicas sobre la misión del sistema de información. Es pues una presentación gerencial que ayuda a tomar una de las decisiones críticas de un análisis de riesgos: aceptar un cierto nivel de riesgo. (MAGERIT, 2019)

Dícese del calculado tomando en consideración únicamente el valor propio de un activo. Este valor se combina con la degradación causada por una amenaza y la frecuencia estimada de la misma, medidas ambas sobre activos de los que depende.(MAGERIT, 2019)

Pilar define unos niveles de criticidad como se detalla en la figura 62 para interpretar el riesgo repercutido.

Figura 62 *Niveles de criticidad*
Fuente: Pilar 7.4.5

El valor repercutido del riesgo se detalla en la figura 63.

[GR01] A.5.2. Valores repercutid ... > A.5.2.2. riesgo

Exportar

potencial | current | target | PILAR

activo	[D]	[I]	[C]
ACTIVOS	{6,5}	{8,2}	{8,2}
[Datos-01] Base de datos de clientes	{5,9}	{7,6}	{7,6}
[Datos-02] Cotizaciones	{5,9}	{7,6}	{7,6}
[Datos-03] Información comerciual	{4,7}	{7,6}	{7,6}
[Datos-04] Información personal de colaboradores	{5,3}	{7,0}	{7,6}
[Datos-05] Información de clientes de auditoría	{5,9}	{7,6}	{7,6}
[Datos-06] Información de clientes de consultoría	{6,5}	{8,2}	{8,2}
[Datos-07] Base de datos de clientes soporte	{5,9}	{7,6}	{7,6}
[Sw-01] Office 365	{4,3}	{5,0}	{4,4}
[Sw-02] FreshDesk		{3,7}	{5,0}
[Sw-03] Hubspot		{3,7}	{5,0}
[Hw-01] LTPT-GS-001	{4,7}	{2,6}	{3,8}
[Hw-02] LPTP-GS-002	{5,9}	{3,7}	{5,0}
[Hw-03] LPTP-GS-003	{4,7}	{2,6}	{3,8}
[Hw-04] LPTP-GS-004	{4,7}	{2,6}	{3,8}
[Hw-05] Desktop-01	{4,7}	{4,4}	{4,4}
[Hw-06] Impresora HP Color Jet MFP M477fdw	{2,3}	{0,84}	{1,4}
[Com-01] Teléfono de Recepción	{0,92}	{0,52}	{0,97}
[Com-02] Teléfono de Gerencia de servicios	{2,4}	{0,87}	{1,4}
[Com-03] Teléfono área de ventas	{2,4}	{0,87}	{1,4}
[Com-04] Teléfono de Gerencia General	{2,4}	{0,87}	{1,4}
[Com-05] Teléfono área de capacitación	{2,4}	{0,87}	{1,4}
[Com-06] Sistema Panasonic KX-TDA100D	{2,9}	{0,87}	{1,4}
[Com-07] Router CISCO 800 SERIES	{4,7}	{2,6}	{3,8}
[Com-08] Router inalámbrico	{5,3}	{3,2}	{4,4}
[Com-09] ONT	{2,4}	{0,87}	{1,4}
[Personal-01] Gerente de Servicios	{4,9}	{5,5}	{5,9}
[Personal-02] Gerente General	{4,1}	{4,4}	{4,6}
[Personal-03] Consultor Jr	{4,3}	{4,9}	{5,3}
[Perosonal-04] Ánalista de marketing digital	{2,9}	{3,2}	{3,4}
[Personal-05] Asistente de Gerencia	{2,9}	{3,2}	{3,4}

Figura 63 *Riesgo repercutido*
Fuente: Pilar 7.4.5

Interpretación de los resultados

Para la interpretación de resultados se tomó en cuenta todas las actividades realizadas anteriormente, la figura 64 indica el nivel de criticidad encontrado en los activos proporcionados por la organización.

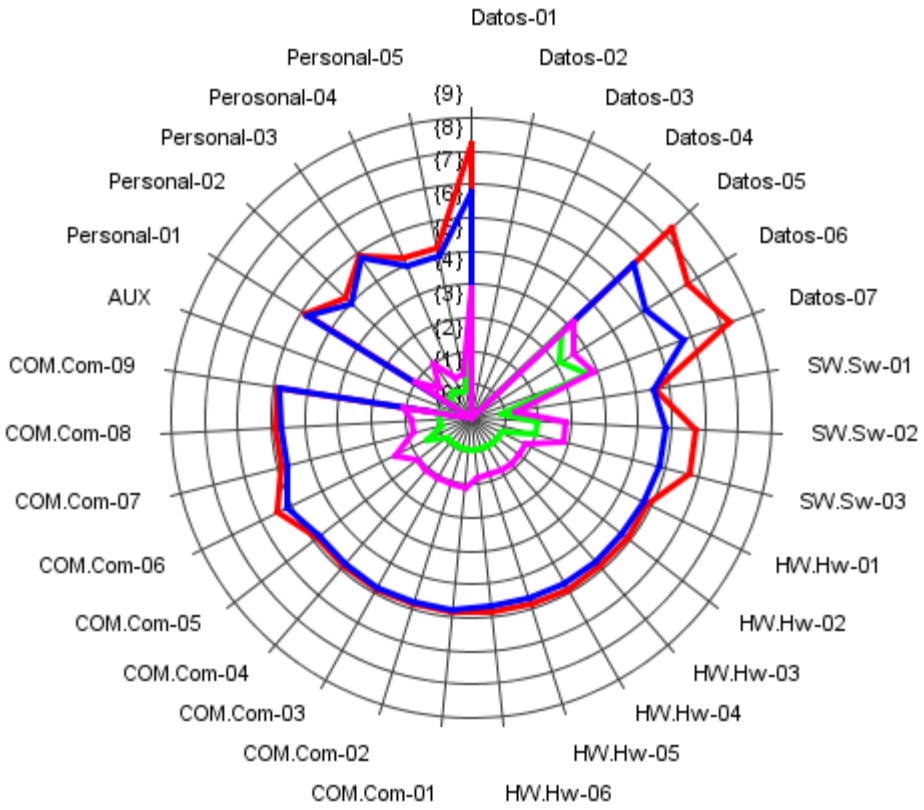


Figura 64 *Resultados*
Fuente: Pilar 7.4.5

La figura 64 explica claramente los activos en color rojo que son lo más vulnerables y a los cuales se les debe prestar más atención para que se aplique el respectivo plan de mitigación que la organización debe ejecutar con los respectivos resultados obtenidos.

Conclusiones

- El marco teórico resultó ser una visión muy abierta para poder entender y encaminar este trabajo permitiéndome tener una visión clara de los conceptos que engloba la Gestión de Riesgos de la Seguridad de la Información en entidades que están implicadas en la seguridad, así como también los tipos de riesgos e impactos que pueden afectar a los activos en las organizaciones.

- Gracias a la metodología Magerit se logró seguir una serie de pasos muy estructurados para el análisis y gestión de riegos tecnológicos, dicha metodología fue la base fundamental para la aplicación en esta organización dedicada a la Seguridad de la información.

- El software Pilar fue fundamental y de gran ayuda para la ejecución de este trabajo pues permitió realizar la valoración de activos, amenazas y salvaguardas con el objetivo de obtener los niveles de impacto y/o riesgo

.

- La información obtenida es un punto de partida para que la Organización cree políticas y procedimientos de seguridad de la información para que las amenazas que afectan a los activos sean mitigados o controlados a partir de las salvaguardas.

Recomendaciones

- Se recomienda que haya una revisión continua de las amenazas y riesgos realizando una búsqueda de las nuevas brechas que pueden aparecer ya que se ha identificado que existen activos que están muy afectados y esto se debe a que la tecnología está cambiando de manera constante y deben ser contralados para evitar problemas futuros

- Se sugiere a la Organización destinar el personal correspondiente que se ocupe expresamente de la Seguridad de la Información, este personal debe crear políticas y hacer cumplir las mismas para que se asegure la confidencialidad, integridad y disponibilidad de los activos.

- Enfocarse en los activos esenciales donde el riesgo llegue a niveles de criticidad (6,7,8,9) y crear salvaguardas que ayuden a mitigar dichos activos.

- Es importante que en las organizaciones el análisis y gestión de riesgos debe ser entendido por la parte gerencial pero no como un tema aislado sino como parte de los procesos primordiales de la organización.

- Se recomienda seguir realizando futuros temas de tesis referentes al análisis y gestión de riesgos tecnológicos pues este trabajo demostró que este campo no ha recibido la relevancia suficiente en las organizaciones públicas y privadas.

Bibliografía

Almeida, A. C. G. (2017). *Tesis_Ix81_Martinez Y Molina*.

Andrés, A., & Gómez, L. (2019). *Guía de aplicación de la Norma UNE-ISO / IEC 27001 sobre seguridad en sistemas de información para pymes*. 1–135. Retrieved from www.aenor.es

Arévalo, F. M., & Moscoso, I. P. C. S. A. (2017). *Agile Methodology for Computer Risk Management*. *1*(2), 31–42.

Calder, A., & Watkins, S. (2018). *Guide to Data Security and ISO 27001/ISO 27002*.

Cañas, L. (2019). Desarrollo e Implementación de Sistemas de Gestión de Riesgos. *Banco Central de Reserva de El Salvador Documentos Ocasionales No. 2009-01*, (1813–6494), 39. Retrieved from http://www.bcr.gob.sv/bcrsite/uploaded/content/category/790395247.pdf

Castillo, J., Cisneros, A., Méndez, P., & Jácome, D. (2018). Modelo para la reducción de riesgos de seguridad informática en servicios web. *Revista Cumbres*, *4*(2), 12. Retrieved from https://dialnet.unirioja.es/servlet/articulo?codigo=6836549

CCN-CERT. (2020). *EAR/PILAR - Herramientas para el Análisis de Riesgos*. Retrieved from http://www.ar-tools.com/es/index.html

Ealde Business School. (2020). *Metodologías en Gestión de Riesgos - EALDE Business School*. Retrieved from https://www.ealde.es/metodologias-gestion-riesgos/

Imbaquingo, D., Pusdá, M., & Jácome, J. (2017). *Fundamentos de Auditoría informática Basada en Riesgos*.

INCIBE. (2015). *Guia de Gestion de Riesgos*. *1205*(Imc), 528. https://doi.org/10.1017/CBO9781107415324.004

INCIBE. (2020). *Protege tu empresa*. Retrieved from https://www.incibe.es/protege-tu-empresa

INSTITUTO NACIONAL DE CIBERSEGURIDAD. (2016). Gestión de Riesgos. *INSTITUTO NACIONAL DE CIBERSEGURIDAD*, 3–5. Retrieved from https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_ciberseguridad_gestion_riesgos_metad.pdf%0Afile:///F:/TFM/gra_ficha_AGO_16.pdf

Instituto Nacional de Tecnologías de la Comunicación. (2016). *Implantación de un SGSI en la empresa*. Retrieved from https://www.incibe.es/extfrontinteco/img/File/intecocert/sgsi/img/Guia_apoyo_SGSI.pdf

ISO/IEC 27001. (2017). *Norma Española Técnicas de seguridad Sistemas de Gestión de la Seguridad de la Información Requisitos*.

ISOTools. (2016). *ISO 27001 - Software ISO 27001 de Sistemas de Gestión*. Retrieved from https://www.isotools.org/normas/riesgos-y-seguridad/iso-27001%0Ahttps://www.isotools.org/normas/riesgos-y-seguridad/iso-27001/

Kowask Bezerra, E., Alcántara Lima, F., Motta, A. C., & Piccolini, J. D. B. (2016). *Gestión del riesgo de las TI NTC 27005*. 217.

Llorente Pozo, Pérez Gutiérrez, S. R. (2017). *No Title*.

MAGERIT. (2019). MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I - Método. *Ministerio de Hacienda y Administraciones Públicas*, *2006*(630-12-171–8), 127.

Mariño, D. C. M. (2017). *GESTIÓN DE RIESGOS INFORMÁTICOS PARA LA PROTECCIÓN DE LOS SISTEMAS DE INFORMACIÓN EN LA COOPERATIVA DE AHORRO Y CREDITO CAMPESINA COOPAC.* (Vol. 66).

MINTIC. (2019).

Mora, H. (2020). Seguridad de Instalaciones. Retrieved from 2020 website: http://epn.gov.co/elearning/distinguidos/SEGURIDAD/bibliografa.html

Morales, A. (2019). Información. *2019*.

Nacional, C. C. (2016). *Guía de Seguridad CCN-STIC-401*.

Okoli, C., & Pawlowski, S. D. (2004). The Delphi method as a research tool: An example, design considerations and applications. *Information and Management*, *42*(1), 15–29. https://doi.org/10.1016/j.im.2003.11.002

Ortega, J. (2018). *SEGURIDAD INFORMÁTICA*.

Ponemon, L., & Whitemore, W. (2017). Know the Odds: The Cost of a Data Breach in 2017. *IBM Security Intelligence*, pp. 1–9. Retrieved from https://securityintelligence.com/know-the-odds-the-cost-of-a-data-breach-in-2017/

Posada, E. (2016). *Cul Es La Situacion Actual De Las*.

Quiroz Zambrano, S., & Macías Valencia, D. (2017). Seguridad en informática: consideraciones. *Dominio de Las Ciencias*, *3*(3), 676–688.

SAMPIERI, Hernández Roberto. (2018).

Secretaría Nacional de Planificación y Desarrollo. (2017). *Plan Nacional de Desarrollo 2017-2021-Toda una Vida*. 84. Retrieved from http://www.planificacion.gob.ec/wp-content/uploads/downloads/2017/10/PNBV-26-OCT-FINAL_0K.compressed1.pdf

Torrado Fonseca, M. R. Á. M. (2016). El método Delphi. *REIRE. Revista d'Innovació y Recerca En Educación*, *9*(9 (1)), 0–2. https://doi.org/10.1344/reire2016.9.1916

United Nations. (2017). Objetivos y metas de desarrollo sostenible - Desarrollo Sostenible. *Web Page*, p. 1. Retrieved from https://www.un.org/sustainabledevelopment/es/objetivos-de-desarrollo-sostenible/

Urbina, G. B. (2016). *Introducción a la Seguridad Informática* (Primera Ed). Mexico.

Vanegas, A. C. C. (2016). UNIVERSIDAD DE CUENCA - TESIS.pdf. *Articulo Ecuador*, *1*(5), 1–127.