DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN

CARRERA DE TECNOLOGÍA EN COMPUTACIÓN

MONOGRAFÍA: PREVIO A LA OBTENCIÓN DEL TÍTULO DE TECNÓLOGO EN COMPUTACIÓN

TEMA:

"APLICACIÓN DE LA METODOLOGÍA MAGERIT PARA EL ANÁLISIS DEL RIESGO INFORMÁTICO AL DEPARTAMENTO INFORMÁTICO DEL GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DEL CANTÓN LA LIBERTAD UTILIZANDO LA HERRAMIENTA PILAR"

AUTOR:

GUTIÉRREZ QUIRUMBAY, CINTHYA JOHANNA

DIRECTOR: ING. VINUEZA PAZ PATRICIO ENRIQUE

SANGOLQUÍ

2019

ESPE
UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN

CARRERA DE TECNOLOGÍA EN COMPUTACIÓN

CERTIFICACIÓN

Certifico que la monografía, **"APLICACIÓN DE LA METODOLOGÍA MAGERIT PARA EL ANÁLISIS DEL RIESGO INFORMÁTICO AL DEPARTAMENTO INFORMÁTICO DEL GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DEL CANTÓN LA LIBERTAD UTILIZANDO LA HERRAMIENTA PILAR"**, fue realizado por la señora Cinthya Johanna Gutiérrez Quirumbay, el mismo que ha sido revisado en su totalidad, analizado por la herramienta de verificación de similitud de contenido; por lo tanto cumple con los requisitos teóricos, científicos, técnicos, metodológicos y legales establecidos por la Universidad de las Fuerzas Armadas ESPE, razón por la cual me permito acreditar y autorizar para que lo sustente públicamente.

Sangolquí, 22 de mayo 2019.

Firma:

.....

Ing. Patricio Vinueza

Director

ESPE
UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN

CARRERA DE TECNOLOGÍA EN COMPUTACIÓN

AUTORÍA DE RESPONSABILIDAD

Yo, **GUTIÉRREZ QUIRUMBAY CINTHYA JOHANNA**, declaro que el contenido, ideas y criterios de la monografía, **"APLICACIÓN DE LA METODOLOGÍA MAGERIT PARA EL ANÁLISIS DEL RIESGO INFORMÁTICO AL DEPARTAMENTO INFORMÁTICO DEL GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DEL CANTÓN LA LIBERTAD UTILIZANDO LA HERRAMIENTA PILAR"**, es de mi autoría y responsabilidad, cumpliendo con los requisitos teóricos, científicos, técnicos, metodológicos y legales establecidos por la Universidad de Fuerzas Armadas ESPE, respetando los derechos intelectuales de terceros y referenciando las citas bibliográficas.

Consecuentemente el contenido de la investigación mencionada es veraz.

Sangolquí, 22 de mayo 2019.

.....

GUTIÉRREZ QUIRUMBAY CINTHYA JOHANNA

C.C. 0920707296

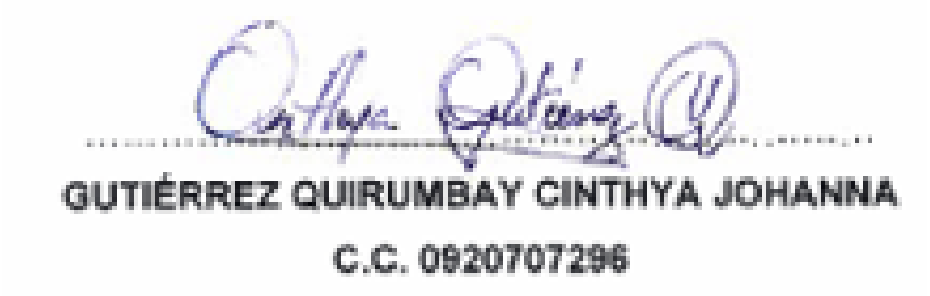
DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN

CARRERA DE TECNOLOGÍA EN COMPUTACIÓN

AUTORIZACIÓN

Yo, ***GUTIÉRREZ QUIRUMBAY CINTHYA JOHANNA***, autorizo a la Universidad de la Fuerzas Armadas ESPE publicar la monografía, **"APLICACIÓN DE LA METODOLOGÍA MAGERIT PARA EL ANÁLISIS DEL RIESGO INFORMÁTICO AL DEPARTAMENTO INFORMÁTICO DEL GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DEL CANTÓN LA LIBERTAD UTILIZANDO LA HERRAMIENTA PILAR",** en el Repositorio Institucional, cuyo contenido, ideas y criterios son de mi responsabilidad.

Sangolquí, 22 de mayo 2019.



GUTIÉRREZ QUIRUMBAY CINTHYA JOHANNA

C.C. 0920707296

DEDICATORIA

Éste trabajo de titulación se lo dedico a mis padres, hermanos, esposo y a mis dos hijos por su inmenso apoyo y amor incondicional.

CINTHYA

AGRADECIMIENTO

A Dios por encaminar mi vida y por darme las fuerzas necesarias en momentos difíciles y fortalecer mis ideales para continuar y culminar con ésta etapa de mi vida. A mis Padres, Dora y Juan por su apoyo y amor incondicional tanto en lo económico como emocional. A mi esposo Carlos y a mis dos hijos Isabella y Carlitos por su paciencia y comprensión. A mis hermanos que contribuyeron de algún modo en ésta etapa de mi vida.

CINTHYA

ÍNDICE DE CONTENIDOS

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

RESUMEN

El avance apresurado de las Tics (Tecnología de la Información y Comunicación) ha generado grandes oportunidades pero así mismo ha provocado la aparición de nuevas vulnerabilidades, amenazas y riesgos que si no son tratados a tiempo y de forma adecuada estas puedan materializarse y causar daño a las empresas. Se ha desarrollado un análisis de riesgo de la información de orden cualitativo aplicado al Departamento Informático del Gobierno Autónomo Descentralizado Municipal del Cantón La Libertad siguiendo la metodología MAGERIT versión 3. Se ha considerado para la evaluación del riesgo la herramienta PILAR, la cual soporta en análisis y gestión de los riesgos e impacto potencial, actual y objetivo. Se realizó el análisis de riesgo informático y se pudo identificar el nivel de riesgo en el que se encuentran los activos del departamento informático del GADMCLL mediante el nivel de madurez; resultados que nos proporcionó PILAR de acuerdo a las evaluaciones realizadas, mostrándonos que los activos cuentan con un alto índice de amenazas y riesgos que deben ser tratados de manera urgente; por lo que se presenta las salvaguardas con el fin de mitigar el riesgo. Finalmente se presenta propuesta de lineamiento y un Plan de seguridad de la información con el fin de incentivar al personal a seguir con las normas y procedimientos referentes a la seguridad de la información y estar atentos a cualquier evento que se pueda presentar.

PALABRAS CLAVE:

- **AMENAZAS**
- **MAGERIT**
- **PILAR**
- **SALVAGUARDAS**
- **RIESGOS.**

ABSTRACT

The rapid advance of TIC have generated great opportunities but also has caused emergence of new vulnerabilities, threats and risk that if they are not treated on time and properly, these can cause harm to companies.

A risk analysis of cualitative information has been developed, applied to the computer department of Gobierno Autónomo Descentralizado Municipal del Cantón La Libertad following the MARGERIT version 3 methodology. The PILAR tool Is considered for risk assessment, which supports risk analysis and management and potential impact, current and objective. We conducted the computer risk analysis and could identify the level of risk in which are the assets of the computer department of GADMCLL by the level of maturity; Results provided by PILAR according to the evaluations carried out, showing that the assets have a high rate of threats and risks that must be treated urgently; So the safeguards are presented in order to mitigate the risk. Finally it presents the proposal of guidelines and a Security Plan of information to encourage staff to continue with rules and procedures referring to the security of the information and be attentive to any event.

KEYWORDS:

- **THREATS**
- **MAGERIT**
- **PILAR**
- **SAFEGUARDS**
- **RISKS**

CAPÍTULO I
ASPECTOS GENERALES

1.1 Antecedentes

Durante mucho tiempo la información ha sido considerado un activo valioso, esto ha permitido que la seguridad informática sea un tema de interés en grandes y pequeñas empresas ya sean éstas públicas o privadas debido a que están expuestas a posibles amenazas por vulnerabilidades que si no son controladas y evaluadas a tiempo, pueden originar varios incidentes por el crecimiento de riesgos causando daño e impidiendo salvaguardar sus activos de información. La información es substancial para el Departamento Informático del GADMCLL y para todas las empresas que se encuentran involucradas con los cambios y desafíos tecnológicos que existe en la actualidad. La serie ISO 27001 es uno de los estándares a nivel mundial que tratan sobre la gestión de riesgo de la información, así como también existen metodologías y herramientas que ayudan a manejar información masiva para realizar un análisis de riesgo. Es por esta razón que es indispensable realizar un análisis de riesgo de la situación actual de la Institución y obtener resultados que servirán para elaborar propuesta de lineamiento de seguridad, para el Departamento Informático del Gobierno Autónomo Descentralizado Municipal del Cantón La Libertad.

1.2 Planteamiento del problema

En los dos últimos años el GADMCLL adquirió equipos y sistemas informáticos para mejorar sus funciones y servicios, se pudo observar que no cuenta con buenas

prácticas de seguridad informática que permitan resguardar sus activos. El activo informaciones de alta prioridad y de vital importancia para la Institución, es por esta razón que el departamento informático del GADMCLL pretende resguardar y proteger de ciertas amenazas que pueden causar eventos adversos a los procesos llegando hasta la pérdida de información; iniciando con un análisis de riesgo informático que nos muestre la situación actual del departamento informático del GADMCLL.

1.3 Importancia y Justificación.

La seguridad informática merece un alto nivel de importancia en todas las empresas y requiere una constante revisión, monitorización y aplicación de políticas, programas y estándares de protección permanentes ante las posibles amenazas que puedan afectar la confiabilidad, integridad y disponibilidad de la información.

Todas las Instituciones públicas, privadas, y de cualquier naturaleza identifican la vital importancia de mantener y conservar la información de manera segura; por lo que se busca proteger sus activos. Se ha tomado en cuenta el análisis del riesgo informático que forma parte de la primera fase del modelo PDCA (Plan, Do, Check, Act) de la Norma “ISO/IEC 27001 Norma internacional certificada”, genérica, única para la administración de la seguridad de la información y aplicable a todo tipo de organizaciones.

La herramienta elegida será PILAR, la misma que nos ayudará a analizar el riesgo informático aplicando la metodología Magerit; donde se ha tomado como referencia la Norma ISO 27001 y las buenas prácticas de la seguridad de la información de la Norma ISO 27002, estas nos permitirán realizar sugerencias y soluciones referente a la confidencialidad, integridad, autenticación y disponibilidad de la información. El Departamento Informático del GADMCLL será beneficiado porque se obtendrán resultados que muestren el estado actual.

1.4 Objetivo General

Efectuar un análisis del riesgo informático para el Departamento Informática del Gobierno Autónomo Descentralizado Municipal del Cantón La Libertad-GADMCLL utilizando la herramienta Pilar.

1.5 Objetivos Específicos

- ✓ Detectar los activos críticos informáticos del Departamento Informático del GADMCLL, mediante información proporcionada por el personal del departamento.
- ✓ Detectar las amenazas y vulnerabilidades en el Departamento Informático del GADMCLL, aplicando la metodología Magerit y la herramienta Pilar.
- ✓ Valoración de las amenazas
- ✓ Estimar el riesgo informático para sugerir mejoras de la seguridad de la información para el Departamento Informático del GADMCLL.

1.6 Alcance

El presente estudio centra su objeto de investigación y aplicación de los principios y fundamentos del estándar ISO 27001 y la ISO 27002, que serán de guía para realizar el análisis de riesgo de la información mediante la herramienta PILAR implementando la Metodología Magerit en el Departamento Informático del Gobierno Autónomo Descentralizado Municipal del Cantón La Libertad – GADMCLL, Posteriormente, mediante la herramienta Pilar se mostrará los resultados del análisis de riesgo y se planteará sugerencias o recomendaciones para la seguridad informática.

Cabe mencionar que se utilizará la herramienta PILAR en modo de evaluación y análisis en orden Cualitativo.

CAPÍTULO 2
MARCO TEÓRICO

2.1 CONCEPTOS Y DEFINICIONES GENERALES

Accesos autorizados: Autorizaciones concedidas a un usuario para la utilización de los diversos recursos.

Activo: Cualquier cosa que tenga valor para la organización.

Amenazas: Sinónimo de un evento interno o externo que pueden causar daño

Ataque: Evento, exitoso o no, que atenta sobre el buen funcionamiento del sistema.

Auditoria: Examinar de forma independiente los log´s del sistema y actividades para comprobar la eficiencia y controlar la integridad de los datos.

Autorización: Garantizar que todos los accesos a datos y/o transacciones que los utilicen, cumplan con los niveles de autorización correspondientes para su utilización y divulgación.

Autenticidad: La información es lo que dice ser o el transmisor de la información es quien dice ser.

Confidencialidad: Información solo disponible a personas autorizadas.

Control de acceso: Mecanismo que en función de la identificación ya autenticada permite acceder a datos o recursos.

Controles: Políticas o procedimientos que aplican a una vulnerabilidad.

Data Center: Es aquella ubicación donde se concentran los recursos necesarios para el procesamiento de la información de una organización.

Desastre o Contingencia: Interrupción de la capacidad de acceso a información y procesamiento de la misma a través de computadoras necesarias para la operación normal de un negocio.

Dependencias.- se refiere a la medida en que un activo superior se vería afectado por un incidente de seguridad en un activo inferior. (Omar, 2013)

Disponibilidad: Que la información esté disponible cuando se la necesite.

Dominios de la Norma: Estructura más general de la norma ISO27002, dentro de esta se encuentran los objetivos de control y los controles.

Gusanos (Worms): Son programas independientes (no necesitan insertarse en otros archivos) que se expandes a través de la red realizando distintas acciones como instalar virus, o atacar una PC como un intruso.

Hacker (pirata): Persona que goza alcanzando un conocimiento profundo sobre el funcionamiento interno de un sistema, de un ordenador o de una red de ordenadores.

Identificación: Procedimiento de reconocimiento de la identidad de un usuario.

IEC: International Electrotechnical Commission, Comisión Electrotécnica Internacional.

Impacto: Consecuencia de la materialización de una amenaza.

Integridad: Información va a estar completa y correcta.

ISO: International Organization for Standardization, Organización Internacional de Estandarización.

La infraestructura computacional: es una parte fundamental para el almacenamiento y gestión de la información, así como para el funcionamiento mismo de la organización. La función de la seguridad informática en esta área es velar por que los equipos funcionen adecuadamente y anticiparse en caso de fallos, robos, incendios, sabotajes, desastres

naturales, fallos en el suministro eléctrico y cualquier otro factor que atente contra la infraestructura informática.

Manual: Es el documento que contiene la descripción de actividades, normas que deben seguirse. Estos documentos deben de ser aprobados por la máxima autoridad.

Políticas: Un conjunto de reglas que sean comprensibles para toda la audiencia a quien va dirigido.

Propiedad: Asegurar que todos los derechos de propiedad sobre la información utilizada en el desarrollo de las tareas, estén adecuadamente establecidos a favor de sus propiedades. (Omar, 2013)

Proveedores: Persona que provee o abastece a otra persona de lo necesario o conveniente para un fin determinado. Empresa que se dedica a proveer o abastecer de productos necesarios a una persona o empresa.

Registro: Es una evidencia de que lo que se dice se ha cumplido, es un aval que permite presentar que se está cumpliendo con los acordado.

Riesgo: Es la probabilidad de que una amenaza sea explotada por las vulnerabilidades.

Salvaguardas.- protección que se les asigna a los activos informáticos para disminuir el impacto de las amenazas.

Seguridad de la información: Preservación de la confidencialidad, disponibilidad e integridad de la información.

SGSI: Sistema de Seguridad de la Información.

Sistemas de información: Conjunto de archivos automatizados, programas, soportes y equipos empleados para el almacenamiento y tratamiento de datos.

Software malicioso: (malware): Es un término común que se utiliza al referirse a cualquier programa malicioso o inesperado o a códigos móviles como virus, troyanos, gusanos o programas de broma.

Spam: Correo comercial no solicitado que se envía a través de Internet. El volumen y contenido del SPAM puede dificultar notablemente el uso de servicios de correo electrónico.

Riesgo Residual.- es el riesgo remanente que persiste después de que se hayan aplicado las medidas de seguridad recomendadas.

Terceros: Persona que es reconocida por ser independiente de las partes involucradas concerniente al tema en cuestión.

Trazabilidad: Poder asegurar en todo momento quien hizo y cuando lo hizo.

UPS: Sistema de alimentación ininterrumpida. Fuente ininterrumpida de energía. Es un dispositivo eléctrico que puede proporcionar energía eléctrica ante un apagón gracias a sus baterías internas que almacenan energía eléctrica.

Usuario: Sujeto o proceso autorizado para acceder a datos o recursos.

Virus: El tipo más conocido de código malicioso. Programa que se copia dentro de otros programas e intenta reproducirse el mayor número de veces posible. Aunque no siempre es así, la mayoría de las veces el virus, además de copiarse, altera o destruye la información de los sistemas en los que se ejecuta.

Vulnerabilidad: Es una debilidad, una falencia que podría atacar a las amenazas. (Seguridad Informatica, 2010)

2.2 SEGURIDAD INFORMÁTICA

Es la disciplina que se ocupa de diseñar las normas, procedimientos, métodos y técnicas destinados a conseguir un sistema de información seguro y confiable. Es decir, se enfoca en la protección de la infraestructura computacional que comprende el Software (base de datos, metadatos, archivos), Hardware, redes computacionales y todo lo que la organización valore y considere que esté en riesgo (información privilegiada).

Es importante mencionar que no existen sistemas completamente seguros por lo tanto cualquier sistema puede ser comprometido ya sea por error de software, hardware, causas naturales o con un ataque con suficiente recurso y conocimiento.

La Seguridad Informática es un proceso continuo y requiere participación universal.(Cartaya, 2014)

2.2.1 VULNERABILIDADES

Las Vulnerabilidades son los puntos débiles, son los elementos que, al ser explotados por amenazas, afectan la confidencialidad, disponibilidad e integridad de la información de un individuo o una empresa.

Es decir, son una puerta abierta para posibles ataques y violación a la información privada.Las vulnerabilidades son muy variadas y al igual que las amenazas tienen una clasificación, tal como se indica en la Tabla 1.

Tabla 1
Vulnerabilidades

VULNERABILIDADES

Clasificación	Definición
Física	Las debilidades que puede tener el entorno físico donde se encuentran los activos. Ejemplo instalaciones inadecuadas del espacio de trabajo, ausencia de identificación entre otras.
Natural	Vulnerabilidades que tienen que ver con que el sistema pueda ser dañado en caso que ocurra algún desastre natural o ambiental. Ejemplo, la falta de salidas de emergencia, que el data center no esté ubicado en una zona climatológicamente adecuada, etc.
De Hardware	Vulnerabilidades con los dispositivos y equipos. Ejemplo, el no darles el mantenimiento adecuado.
De Software	Debilidades en los programas instalado (Universidad Internacional de Valencia, 2014)s.
De Red	Vulnerabilidades que existen en las conexiones de red. Ejemplo, la no limitación de acceso.
Humana	Falta de capacitación para ejecución de las actividades diarias. Falta de conciencia de seguridad para las actividades de rutinas, etc.

Fuente: (Universidad Internacional de Valencia, 2014)

2.2.2. AMENAZAS

Las amenazas son agentes capaces de explotar los fallos de seguridad y, como consecuencia de ello, causar pérdidas o daños a los activos de una empresa y poner en riesgo la integridad, confidencialidad y disponibilidad de la información.

- ✓ Amenazas Internas: pueden ser más serias que las externas porque los usuarios y personal técnico conocen la red, tienen acceso y saben cuál es su funcionamiento.

Quedan imposibilitados los sistemas de prevención de intrusos y firewalls ante amenazas externas.

- ✓ Amenazas Externas: son las que se originan fuera de la red, pero logran ingresar a través de la red a través del Internet siendo las empresas las más afectadas. (Cartaya, 2014)

2.3 SEGURIDAD DE LA INFORMACIÓN

La información es un Activo importante que necesita ser protegido adecuadamente.

2.3.1 DEFINICIÓN

Es el conjunto de medidas preventivas y reactivas de las organizaciones y de los sistemas tecnológicos que permiten resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de datos. Se logra implementando un adecuado conjunto de controles: políticas, procesos, procedimientos, estructuras organizacionales y funciones de software y hardware, los cuales deben realizarse de manera constante *retroalimentación* con el fin de cumplir con el objetivo de seguridad planteado en conjunto con otros procesos de gestión del organismo.(Wikipedia, 2018)

2.3.2 IMPORTANCIA

Para el sector público como privado es importante la seguridad de la información ya que es prioridad la protección de sus activos en infraestructuras críticas. El

intercambio de fuentes de información mediante la interconexión de redes públicas y privadas debilita el control de acceso.

La mayoría de sistemas de información no han sido diseñados para ser seguros y la seguridad que se puede lograr es limitada, por tal razón es necesario el apoyo de la gestión y los procedimientos adecuados y requiere como mínimo la participación de los diferentes grupos de interés (proveedores, terceros, clientes, asesoría especializada de organizaciones externas).

"Dentro de la organización el tema de la seguridad de la información es un capítulo muy importante que requiere dedicarle tiempo y recursos.

La organización debe plantearse un Sistema de Gestión de la Seguridad de la Información (SGSI).El objetivo de un SGSI es proteger la información y para ello lo primero que debe hacer es identificar los "activos de información" que deben ser protegidos y en qué grado. Luego debe aplicarse el plan PDCA ('PLAN – DO – CHECK – ACT'), es decir Planificar, Hacer, Verificar, Actuar y volver a repetir el ciclo. Se entiende la seguridad como un proceso que nunca termina ya que los riesgos nunca se eliminan, pero se pueden gestionar. De los riesgos se desprende que los problemas de seguridad no son únicamente de naturaleza tecnológica, y por ese motivo nunca se eliminan en su totalidad. Un SGSI siempre cumple cuatro niveles repetitivos que comienzan por Planificar y terminan en Actuar, consiguiendo así mejorar la seguridad.

PLANIFICAR (Plan): consiste en establecer el contexto en él se crean las políticas de seguridad, se hace el análisis de riesgos, se hace la selección de controles y el estado de aplicabilidad

HACER (Do): consiste en implementar el sistema de gestión de seguridad de la información, implementar el plan de riesgos e implementar los controles.

VERIFICAR (Check): consiste en monitorear las actividades y hacer auditorías internas.

ACTUAR (Act): consiste en ejecutar tareas de mantenimiento, propuestas de mejora, acciones preventivas y acciones correctivas". Tal como se indica en la Figura 1.(Bernal, 2017)

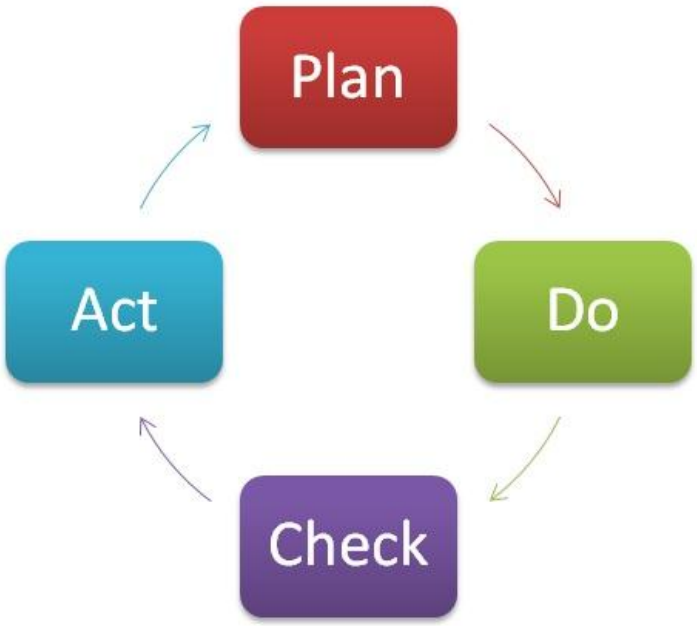


Figura 1Pasos para adaptarse a la Norma ISO 27001

Fuente: (Bernal, 2017)

2.3.3 CONFIDENCIALIDAD

Se garantiza que la información sea accesible sólo y únicamente a las personas autorizadas. Toda la información no debe ser vista por todos los usuarios. Por esa razón las empresas seleccionan y proporcionan a sus empleados de acuerdo a sus funciones

los accesos correspondientes, adicional se aseguran de que la información que van a manejar no la puedan revelar mediante clausulas establecidas en sus contratos con el fin de garantizar su información. (SGSI, 2018)

2.3.4 INTEGRIDAD

Se salvaguarda la exactitud y totalidad de la información y los métodos de procesamiento; es decir que la información no haya sido borrada, copiada o alterada desde su origen a su destino, brindando la confianza de estar seguros de que la información no haya sufrido alguna alteración. (SGSI, 2018)

2.3.5 DISPONIBILIDAD

Se refiere a que los usuarios autorizados tienen acceso a la información cuando lo requieren; es decir proporcionar la información en el momento adecuado, oportuno y preciso cuando se acceda al sistema el mismo que debe mantenerse operativo y enfrentar posibles eventualidades. (SGSI, 2018)

2.3.6 AUTENTICACIÓN

Son los mecanismos de seguridad que tienen los equipos que se manejan para la comunicación y verificación si el origen de los datos es el correcto; es decir la Criptografía que se encarga de mantener la legitimidad de los mensajes, quien los envía y cuando fueron enviados y recibidos.

2.4 RIESGO INFORMÁTICO

"Es la probabilidad de que una amenaza se materialice, utilizando la vulnerabilidad existente de un activo o grupo de activos, generándoles pérdidas o daños".(Riesgos Informático, 2014)

Se utiliza la siguiente fórmula para calcular el riesgo informático:

$$R = I * P$$

Fórmula 1

Dónde en la fórmula 1 se tiene:

R= Riesgo

I= Impacto

P= Probabilidad

Todos los sistemas informáticos están bajo amenazas y cada día aparecen nuevas vulnerabilidades y la probabilidad de que sean explotadas también es alta al igual que el impacto. Toda organización está expuesta a los riesgos informáticos y la forma para salvaguardar la información y reducir el riesgo es priorizar la seguridad informática dándole la importancia necesaria, implementando el análisis y gestión del riesgo.

2.4.1 ANÁLISIS DEL RIESGO INFORMÁTICO

Es un proceso donde se estudia las causas de las posibles amenazas y la probabilidad de taques no deseados y el impacto que pueda tener.

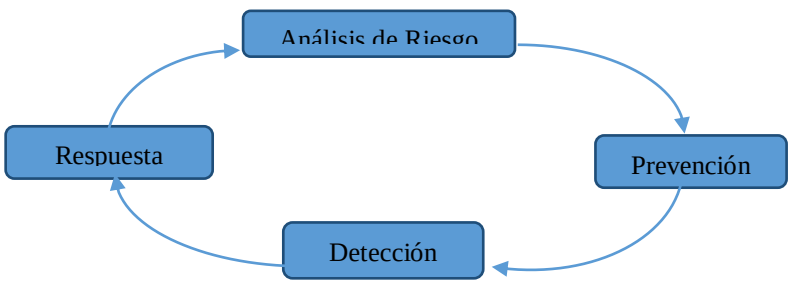


Figura 2. Modelo de proceso de la seguridad.

En la prevención, en la fase inicial del sistema, se debe configurar adecuadamente el sistema, los servicios y entender las herramientas de detección y respuesta de los posibles ataques.

En la detección, es la fase en la cual se está pendiente para detectar y reaccionar a posibles ataques. Cuando el sistema se pone en marcha y pasa a producción se comienza una fase crítica que es la fase de monitorización continua del sistema que se trata de comprobar que el objetivo cumple las expectativas consideradas de acuerdo a las políticas de seguridad. En esta etapa que determinada si hay que evaluar nuevamente el sistema de acuerdo a la situación actual o nuevas vulnerabilidades encontradas. En la etapa de respuesta, en el caso de que exista un ataque se comienza con el tratamiento del ataque. Se trata de restablecer lo antes posible los servicios y el tiempo en que se tome va a depender de la fase previa es decir de que herramientas se haya instalado y de que estén bien configuradas y de la información que se disponga para averiguar lo que realmente ha ocurrido ya que no se trata de recuperar el funcionamiento normal del sistema si no garantizar que el atacante no vuelva atacar la misma vulnerabilidad. Una vez que el sistema esté en funcionamiento hay que aprovechar este hecho para aprender todo lo posible y volver a evaluar el riesgo, las herramientas y analizar nuevos riesgos que se presentan. (Seguridad Informatica, 2010)

2.4.2 GESTIÓN DEL RIESGO INFORMÁTICO

Son actividades coordinadas para dirigir y controlar una organización en lo que concierne al riesgo. Usualmente incluye la evaluación de riesgo, el tratamiento de riesgos, la aceptación de riesgos y la comunicación de riesgos.

Cabe mencionar que en mi caso de estudio se utilizará la herramienta PILAR que toma como referencia los perfiles de seguridad de la ISO 27002:2013 con la cual sólo se va a trabajar. (Riesgos Informáticos, 2009)

2.4 NORMAS DE LA SEGURIDAD DE LA INFORMACIÓN

Las normas ISO son un modelo, un patrón, ejemplo o criterio a seguir. La finalidad de las normas ISO es orientar, simplificar y unificar los usos para conseguir menores costes y efectividad. (Intef, 2018)

Actualmente se encuentra con estándares internacionales que proporcionan mecanismos de seguridad que deberían ser implementados por todas las organizaciones relacionadas a las tecnologías de la información. A continuación se mencionan algunas de ellas en la siguiente Tabla 2.

2.5.1 CONCEPTOS

Tabla 2

Normas de Seguridad Informática

NORMA	DESCRIPCIÓN
ISO/IEC 27000	Es una visión general de las normas que componen la serie 27000 sólo en inglés
ISO/IEC 27001	Sistema de Gestión de la Seguridad de la Información: Esta norma fue en octubre de 2005, dejando obsoleta a la ISO-17799. Norma certificable y es la que establece todos los requerimientos de un SGSI.
ISO/IEC 27002	Código o Guía de buenas prácticas para la Seguridad de la Información, fue publicado el 15 de junio del 2005 y detalla los 133 controles reunidos en 11 grupos, más 39 “Objetivos de control”
ISO/IEC 27003	Guía de Implementación. Describe los aspectos a tener en cuenta para la implantación de un SGSI, fue publicada en febrero de 2009 y aún no existe traducción al español
ISO/IEC 27004	Describe todos los aspectos de métricas, indicadores y mediciones que deben realizarse sobre un SGSI. Se publicó en diciembre de 2009.
ISO/IEC 27005	Trata los aspectos relacionados a la “Gestión de riesgos” tema de suma importancia en toda esta familia.
ISO/IEC 27007	Guía para auditoría de un SGSI
ISO/IEC 27008	Guía para auditoría de los controles de un SGSI.
ISO/IEC 27010	Guía para la gestión de la seguridad de Sistemas de Información entre organizaciones.
ISO/IEC 27011	Guía de implementación de un SGSI para el sector de Telecomunicaciones.
ISO/IEC 27012	SGSI para el sector de e-administración.
ISO/IEC 27013	Integración con ISO-20000
ISO/IEC 27014	Gobierno corporativo de un SGSI.
ISO/IEC 27015	Sector financiero.
ISO/IEC 27031	Directrices para la preparación de las TIC en la Continuidad de Negocio, de reciente publicación, orientada a aspectos específicos de las Tics, en particular hacia el Plan de Continuidad de Negocio.
ISO/IEC 27032	Ciberseguridad.

Fuente:(ISO27000.es, 2013)

2.5.2 NORMA ISO 27001:2013

La norma ISO 27002, usa la expresión “shall”, otro término convencional, en este caso para expresar mandato u obligación.

La ISO 27001 especifica los requisitos para establecer un plan de seguridad constituido por un Sistema de Gestión de Seguridad de la Información, SGSI dentro del contexto de los riegos totales en negocios de una empresa.

La norma ISO 27001:2013 no sólo establece cambios en el contenido sino también en la estructura, lo que verá reflejado en otros documentos que forman parte de la familia ISO 27000.

La norma ISO 27001:2013 ha sido desarrollada con base al Anexo SL, en la que se proporciona un formato y un conjunto de alineamiento que siguen el desarrollo documental de un Sistema de Gestión sin que le importe el enfoque empresarial, se alinean bajo la misma estructura todos los documentos que se relaciona con el Sistema de Gestión de Seguridad de la Información y así se evitan problemas de integración con otros marcos de referencia. Además, la nueva estructura queda así: (ISO27000.es, 2013)

2.5.3 Introducción

En la norma ISO 27001:2013 el cambio más significativo es la eliminación de la sección “Enfoque del proceso” que sí contenía la versión 2005, donde se describía el modelo PHVA, considerándose el corazón del Sistema de Gestión de Seguridad de la Información (SGSI).

1. Alcance

2. Referencias normativas

3. Términos y definiciones

4. Contexto de la organización

5. Liderazgo

6. Planeación

7. Soporte

8. Operación

9. Evaluación del desempeño

10. Mejora

2.5.4 NORMA ISO 27002:2013

ISO/IEC 27002:2013 proporciona directrices para las normas de seguridad de la información organizacional y las prácticas de gestión de la seguridad de la información, incluida la selección, implementación y gestión de controles teniendo en cuenta los entornos de riesgo de seguridad de la información de la organización.

Está diseñado para ser utilizado por organizaciones que tienen la intención de: seleccionar controles dentro del proceso de implementación de un Sistema de gestión de seguridad de la información basado en ISO / IEC 27001; implementar controles de seguridad de la información comúnmente aceptados; desarrollar sus propias pautas de gestión de seguridad de la información. (ISO27000.es, 2013)

Es una guía de buenas prácticas para la Seguridad de la Información, fue publicado el 15 de junio del 2005 y detalla los 133 controles reunidos en 11 grupos, más 39 “Objetivos de control”. Los dominios son:

- ✓ Política de Seguridad
- ✓ Organización
- ✓ Gestión de Activos
- ✓ Recursos Humanos
- ✓ Seguridad Física y ambiental
- ✓ Gestión de Comunicaciones y Operaciones
- ✓ Gestión de Accesos
- ✓ Adquisición, Desarrollo y Mantenimiento de Sistemas
- ✓ Gestión de Incidentes de Seguridad
- ✓ Gestión de la Continuidad
- ✓ Cumplimiento

2.5 METODOLOGÍAS

CUADRO COMPARATIVO DE METODOLOGÍAS

Puntos C.	MAGERIT	CRAMM	OCTAVE
País que la creo	España	Reino Unido	Estados Unidos
Responsable del Producto	Secretaria de Estado para la Administración Pública	Cramm	Software Engineering Institute (SEI) Y Camegle Mellon University(CMU)
Website	Versión 3 https://administracionelectronica.gob.es	https://administracionelectronica.gob.es	https://www.cert.org/octave
Versiones	Versión 2 Versión 3	Última versión 5.3	OCTAVESM Method Versión 2.0
Herraienta para aplicar Metodología	PILAR CHINCHON	CRAMM express	Según lo investigado, la norma no especifica un producto, habla de Vulnerability Evaluatión Tools
Principales conceptos	Activos, amenazas, vulnerabilidades, impacto, riesgo y salvaguardas	Activos, amenazas,vulnerabilidades, riesgos, salvaguardas	Activos, amenazas, vulnerabilidades, riesgos

Imagen 1. Cuadro Comparativo
Fuente:**(Mogollon, 2018)**

MAGERIT

Es una metodología de análisis y gestión de riesgos informáticos que fue elaborada por el Consejo Superior de Administración Electrónica de España (CSAE). Es de carácter público el uso de ésta metodología, pertenece al Ministerio de Administraciones públicas (MAP) y está dirigido a los medios electrónicos, informáticos y telemáticos porque su uso es muy frecuente debido a la existencia de riesgos que sin duda se deben evitar con medidas preventivas. (Libro I, 2017)

2.6.1 HISTORIA Y EVOLUCIÓN

En la actualidad se encuentra la versión 3.0, pero el tiempo ha pasado desde la primera publicación de Magerit en 1997, y su segunda publicación en 2005, donde el análisis de riesgos se ha venido consolidado como eje central para la gestión de la seguridad. Los 7 libros segregado en Magerit versión 1, han evolucionado de la siguiente manera:

Tabla 3
Historia y Evolución

MAGERIT Versión 1.	MAGERIT Versión 3.
Libro I. Guía de aproximación a la seguridad de los sistemas de información.	Libro I – Método
Libro II. Guía de procedimientos	Libro I – Método
Libro III. Guía de técnicas	Guía de Técnicas
Libro IV. Guía para desarrolladores de aplicaciones	Libro I – Método / Capítulo 7 Desarrollo de sistemas de información
Libro V. Guía para responsables del dominio protegible	Libro I – Método Libro II – Catálogo de Elementos
Libro VI. Arquitectura de la información y especificaciones de la interfaz para el intercambio de datos	Libro II. – Catálogos de Elementos / formatos XML
Libro VII. Referencia de normas legales y técnicas	Libro I. – Método / Apéndice 3. Marco Legal

Fuente: (Libro I, 2017)

2.6.2 OBJETIVO DE MAGERIT

- ✓ Hacer que los responsables de los sistemas de la información sean conscientes de la existencia de riesgos y de la necesidad de evitarlos o tratarlos a tiempo.
- ✓ Ofrecer un método sistemático para analizar tales riesgos
- ✓ Ayudar a descubrir y planificar las medidas oportunas para mantener los riesgos bajo control.
- ✓ Preparar a la organización para procesos de evaluación y auditoria, certificación o acreditación según corresponda el caso.

La Metodología Magerit puede resumirse en el siguiente Figura 3.

Figura 3. Modelo MAGERIT
Fuente: (TecnoBlog, 2014)

2.6.3 MAGERIT VERSIÓN 3.0

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 Riesgo"; 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.

2.6.3.1 ORGANIZACIÓN DE LAS GUÍAS

La metodología MAGERIT consta de tres volúmenes:

- ✓ Volumen I. Método
- ✓ Volumen II. Catálogo de Elementos
- ✓ Volumen III. Guía de Técnicas

2.6.3.1.1 VOLUMEN I: MÉTODO

Describe los procesos, actividades y las tareas básicas para realizar un proyecto de análisis y gestión de riesgos.

Se encuentra estructurada de la siguiente Tabla 4.

Tabla 4
Volumen I. Método

CAPÍTULO	REFERENTE A	DESCRIPCIÓN
I	Introducción	"Es una fase introductoria de la metodología Magerit", mencionando que organismos la crearon.
II	Visión de Conjunto	"Específicamente se enmarcan las actividades de análisis y análisis de riesgos para tener un proceso integral de gestión de riesgo"
III	Método de Análisis de	"Se enfoca sólo en el Análisis de Riesgos donde y explica detalladamente cada uno de los pasos que se van a realizar en este tipo de

CONTINUA

	Riesgo	proyectos".
IV	Proceso de Gestión de Riesgos	"Describe todas las actividades que se hacen dentro de la Gestión de Riesgo"
V	Proyectos de Análisis de Riesgos	"Se centra en los proyectos de Análisis de Riesgos, proyectos en los que nos veremos inmersos para realizar el primer análisis de riesgos de un sistema y eventualmente cuando hay cambios sustanciales y hay que rehacer el modelo ampliamente".
VI	Plan de Seguridad	"Establece cuáles serán las actividades que servirán para llevar a cabo un plan de seguridad, y una vez realizado el proyecto de Análisis de Gestión de Riesgos, de esta manera se escogen las decisiones apropiadas para el tratamiento de los riesgos".
VII	Desarrollo de sistemas de Información	"Se basa en la seguridad de los sistemas de información considerando varios puntos de vista para mitigar riesgos, además advierte el Análisis de Riesgo que tiene el mismo propósito asegurar la información".
VIII	Consejos Prácticos	"Sugiere recomendaciones prácticas para aplicarlos en las tareas del Análisis de Riesgo, lo que resulta muy conveniente para la persona que realiza este tipo de proyectos".

Fuente:(Libro I, 2017).

Los apéndices recogen material de consulta:

- ✓ Apéndice 1. Un glosario
- ✓ Apéndice 2. Referencias bibliográficas
- ✓ Apéndice 3. Marco Legal
- ✓ Apéndice 4. Marco de Evaluación y certificación

- ✓ Apéndice 5. Herramientas
- ✓ Apéndice 6. Evaluación de Magerit de la versión 1 a la 2.

2.6.3.1.2CATÁLOGO DE ELEMENTOS

Este catálogo complementa el volumen I con los siguientes elementos:

- ✓ Tipos de Activos
- ✓ Dimensiones y criterios de valoración
- ✓ Amenazas
- ✓ Salvaguardas

En este libro se establecen dos objetivos

- ✓ Facilitar la labor de las personas que acometen el proyecto, en el sentido de ofrecerles elementos estándares a los que puedan adscribirse rápidamente, centrándose en lo específico del sistema objeto del análisis.
- ✓ Homogeneizar los resultados de los análisis, promoviendo una terminología y unos criterios uniformes que permitan comprar e incluso integrar análisis realizados por diferentes equipos. (Libro I, 2017)

2.6.3.1.3 GUÍA DE TÉCNICAS

Ésta guía describe algunas técnicas utilizadas en análisis y gestión de riesgos. Se considera técnica a un conjunto de heurístico y procedimientos que ayudan a alcanzar los objetivos propuestos, las cuales se identifican en la siguiente Tabla5.

Tabla 5
Guía de Técnicas

Para cada una de las técnicas referenciadas:	"Se explican brevemente el objetivo que se persigue al utilizarlas"
	"Se describen los elementos básicos asociados"
	"Se exponen los principios fundamentales de elaboración"
	Se presenta una notación textual y/o gráfica
	"Se citan las fuentes bibliográficas que, sin ser exhaustivas, se han estimado de interés para el lector profundice en cada materia".

Fuente: (Libro I, 2017)

Las técnicas que recoge son:

- ✓ Análisis mediante tablas
- ✓ Análisis algorítmico
- ✓ Arboles de ataque
- ✓ Técnicas de ataque
- ✓ Técnicas generales
- ✓ Análisis coste-beneficio
- ✓ Diagramas de flujo de datos (DFD)
- ✓ Diagramas de procesos
- ✓ Técnicas gráficas
- ✓ Planificación de proyectos
- ✓ Sesiones de trabajo: entrevistas, reuniones y presentaciones
- ✓ Valoración Delphi

2.7 METODOLOGÍA MAGERIT

Pasos a seguir:

Paso 1. Llevar a cabo un inventario de equipo de cómputo, software y mobiliario, para determinar cuál es la información crítica que se tiene que resguardar, adicionalmente levantar un inventario de los servicios de cómputo, telecomunicaciones, internet, etc., que son requeridos para que los usuarios estén en posibilidad de llevar a cabo sus actividades normales. (Libro I, 2017)

Paso 2: Determinar Amenazas

Al determinar la amenaza que perjudica a un activo, hay que valorar su influencia en el valor del activo, en dos sentidos: Degradación, es decir conocer cuán perjudicado resultaría el activo y por la probabilidad, es decir cuán probable o improbable es que se materialice la amenaza. La probabilidad de ocurrencia se modela de forma cualitativa y cuantitativa. Ver tabla 6. (Libro I, 2017)

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

Figura 4. Modelación de la probabilidad de ocurrencia

Fuente: (PILAR, 2011)

Paso 3. Determinar Salvaguardas

Son aquellos procedimientos o mecanismos tecnológicos que reducen el riesgo. Revisar la seguridad, controles físicos y ambientales existentes, evaluando si son adecuados respecto a las posibles amenazas. Se debe estar preparado para cualquier percance, verificando que dentro de la organización se cuente con los elementos necesarios para salvaguardar sus activos. (Libro I, 2017)

Existen diversos tipos de protección prestados por las salvaguardas:

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

✓ Administración. - Relacionadas con los componentes de seguridad del sistema. Para medir los aspectos organizativos, se puede emplear una escala de madurez de eficacia. Tal como se indica en la figura 5.

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

Figura 5. Eficacia y Madurez de salvaguardas

Fuente: (PILAR, 2011)

Paso 4: Impacto Residual

El sistema queda en una situación de posible impacto cuando en su proceso de gestión existe un conjunto de salvaguardas desplegadas y una medida de madurez. El impacto residual puede calcularse acumulado sobre los activos inferiores, o repercutido sobre los activos superiores. (Libro I, 2017)

Paso 5. Riesgo Residual

El sistema queda en una situación de posible riesgo cuando en su proceso de gestión existe un conjunto de salvaguardas desplegadas y una medida de madurez. (EAR/PILAR, 2013)

2.7.1PLAN DE ACTIVIDADES

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

Tareas del Método de Análisis de Riesgos

TAREA 1. CARACTERIZACIÓN DE LOS ACTIVOS

Identificación de los activos

Dependencias entre activos

Valoración de los activos

TAREA 2. CARACTERIZACIÓN DE LAS AMENAZAS

Identificación de las amenazas

Valoración de las amenazas

TAREA 3. CARACTERIZACIÓN DE LAS SALVAGUARDAS

Identificación de las salvaguardas pertinentes

Valoración de las salvaguardas

TAREA 4. ESTIMACIÓN DEL ESTADO DEL RIESGO

Estimación del impacto

Estimación del riesgo

TAREA 1: CARACTERIZACIÓN DE LOS ACTIVOS

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

Identificación de los Activos

Esta actividad se basa en recolectar la información necesaria para identificar los activos, mediante entrevistas al personal, solicitando diagramas de proceso y de flujos de datos. De esta manera, se puede medir el alcance del proyecto y obtener las relaciones entre los activos. (Libro I, 2017)

Dependencias entre Activos

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

Valoración de los Activos

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

TAREA 2: CARACTERIZACIÓN DE LAS AMENAZAS

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

Identificación de las amenazas

Se debe identificar las amenazas más relevantes sobre cada activo, se lo consigue analizando los informes y registros de incidentes y vulnerabilidades. Además

realizando árboles de ataque, los cuales permiten estudiar y analizar cómo se puede atacar un objetivo permitiendo identificar qué salvaguardas se necesitan desplegar para impedirlo.

Valoración de las amenazas

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

TAREA 3: CARACTERIZACIÓN DE LAS SALVAGUARDAS

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

Identificación de las salvaguardas pertinentes

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

Valoración de las salvaguardas

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

- ✓ La idoneidad de la salvaguarda para el fin perseguido
- ✓ Calidad de implantación

- ✓ Formación de los responsables de su configuración y operación
- ✓ Existencia de controles de medida de su efectividad.

El resultado de esta actividad se concreta en varios informes: declaración de aplicabilidad, evaluación de salvaguardas, y de insuficiencias o vulnerabilidades del sistema de protección. (TecnoBlog, 2014)

TAREA 4: ESTIMACIÓN DEL ESTADO DEL RIESGO.

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

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

- ✓ Estimación del Impacto

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

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

Impacto residual. - Al que se encuentra expuesto el sistema teniendo en cuenta el valor de los activos y la valoración de las amenazas, así como la eficacia de las salvaguardas actualmente desplegadas.

- ✓ Estimación del Riesgo

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

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

Riesgo Residual. - Al que está sometido el sistema teniendo en cuenta el valor de los activos y la valoración de las amenazas, así como la eficacia de las salvaguardas actualmente desplegadas. (TecnoBlog, 2014)

2.8 HERRAMIENTAPILAR

PILAR es una herramienta EAR (Entorno de Análisis de Riesgos) que soporta el análisis y la gestión de riesgos de un sistema de información siguiendo la metodología MAGERIT (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información) y está desarrollada y financiada parcialmente por el CCN. Las siglas de PILAR provienen de “Procedimiento Informático Lógico para el Análisis de Riesgos” creado por el Centro Nacional de Inteligencia. (EAR/PILAR, 2013)

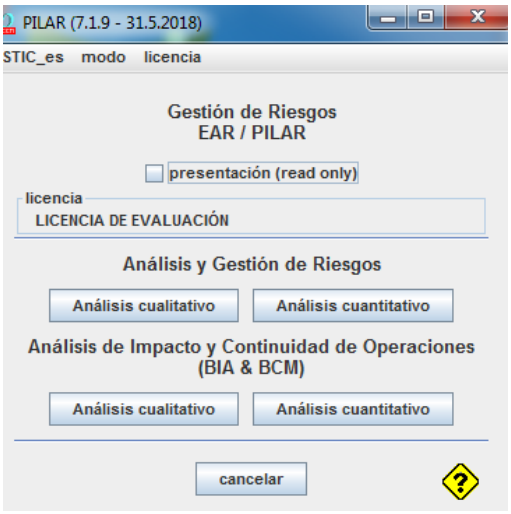


Figura 6. Herramienta Pilar

"PILAR contiene una biblioteca estándar y su función es de realizar valoraciones de seguridad informática de las empresas que manejan esta herramienta y permite realizar el Análisis y Gestión de Riesgos Informáticos en varias dimensiones (confidencialidad, integridad, disponibilidad y autenticidad); también realiza el Análisis de Impacto y Continuidad de Operaciones, donde se realiza el análisis de las interrupciones de servicio teniendo en cuenta la duración de la misma". (EAR/PILAR, 2013)

La versión que se utilizara será la 7.1.9 "Análisis y Gestión de Riesgos" – "Análisis Cualitativo" se escogió este tipo de análisis ya que permite realizar el análisis de los activos asignándoles un valor relativo; se trabajara con la herramienta a modo de prueba ya que no se cuenta con la licencia.

CAPÍTULO 3
SITUACIÓN ACTUAL DEL DEPARTAMENTO INFOMÁTICO DE GADMCLL

3.1 Situación Actual del Departamento Informático del GADMCLL.

El Gobierno Autónomo Descentraliza Municipal de Cantón La Libertad es una Institución pública cuya misión es de promover el desarrollo humano sostenible, entregando a la comunidad servicios de calidad y calidez; con tal propósito desarrolla una gestión eficiente, transparente y participativa; contribuyendo de esta manera, al bienestar material y espiritual de la colectividad. Se identifica en la siguiente Figura 7 el Organigrama estructural.

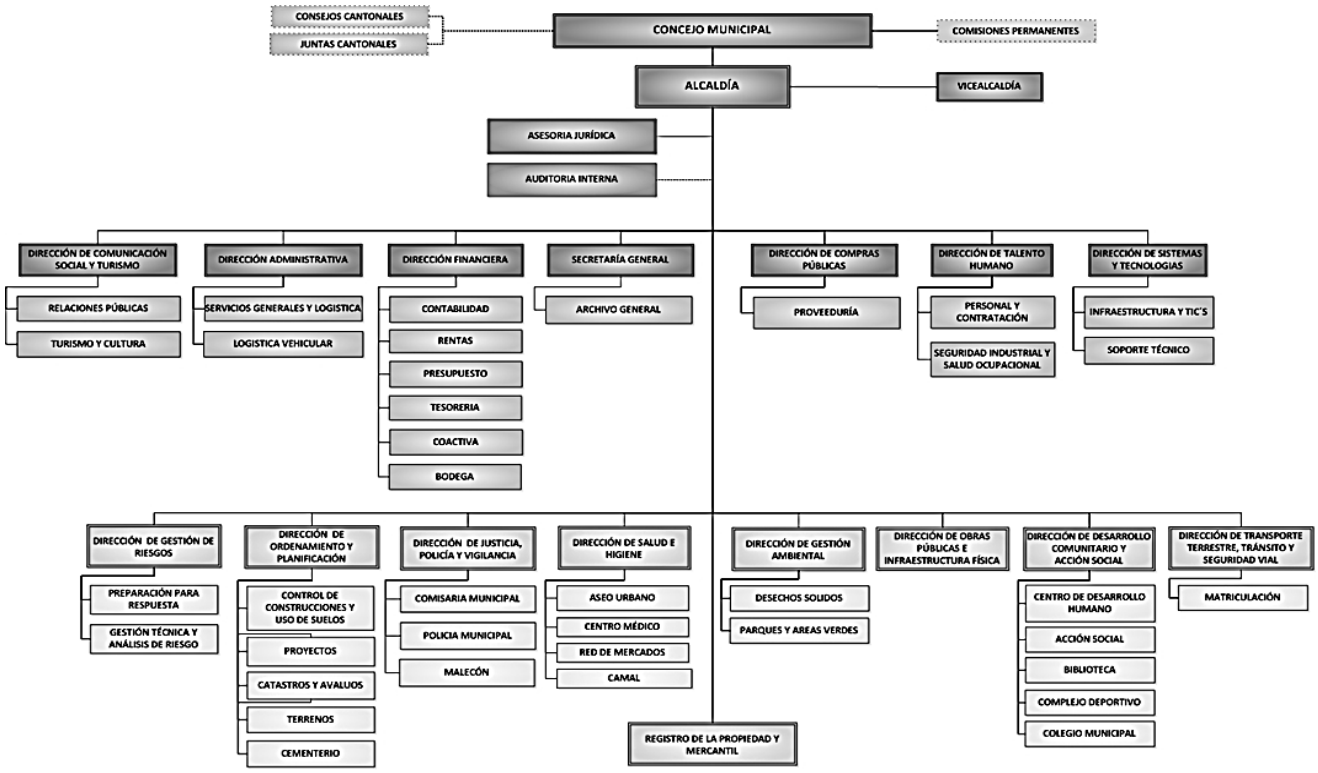


Figura 7. Organigrama del GADMCLL
Fuente: (http://www.lalibertad.gob.ec/portal/)

En la figura 7, se muestra el organigrama estructural, en la cual constan los diferentes departamentos administrativos y entre los que se encuentra el Departamento Informático (DI), el mismo que administra la infraestructura y procesos para brindar los servicios tecnológicos con el fin de cumplir con las tareas administrativas de la institución.

El Departamento Informático tiene una infraestructura variada de equipos y se encuentra en una etapa de innovación de equipos de última tecnología: lo cual ha tolerado dificultades de compatibilidad, configuración y administración.

Se detalla a continuación el entorno físico, la infraestructura, el control de acceso, la entrega de servicios, soporte técnico, operaciones y los incidentes de la institución.

Entorno Físico

El edificio de GADMCLL es de dos plantas y su interior se divide en planta baja que es donde se encuentra la recepción y departamentos financieros y el primer piso las áreas administrativas entre los que se encuentra el departamento informático que se divide en un área de oficinas y el área de la data center que es donde se encuentran los equipos de comunicaciones y servidores. Ambas áreas cuentan con el sistema de climatización y extintores.

El edificio tiene un cuarto de generador eléctrico y su función es mantener a los equipos protegidos por un determinado tiempo, alimentando a los UPS que protegen a los equipos de apagones y sobrecargas.

El control de acceso es controlado por el guardia en la recepción que se encarga de llevar un control del personal que ingresa y sale del edificio. También hay cámaras de seguridad instaladas en planta baja, primer piso y en la entrada del edificio municipal.

La data Center se compone por 1 armario con puerta y dos racks abiertos donde se están alojados los equipos de comunicación.

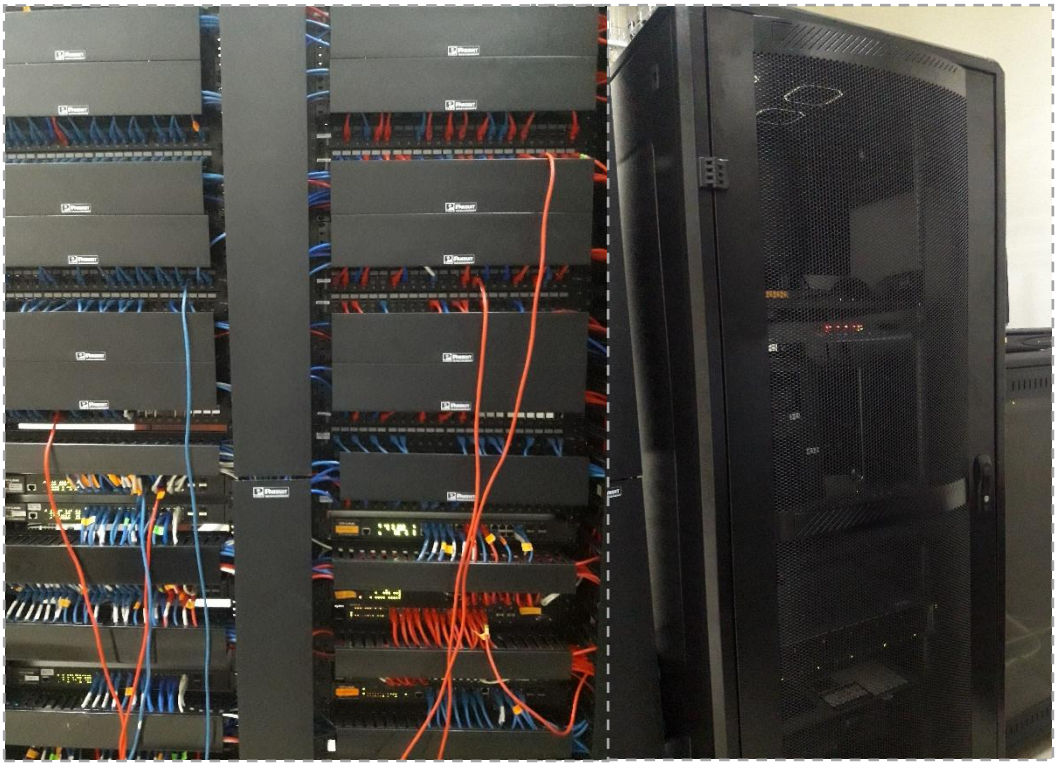


Imagen 2. Data Center del GADMCLL

Fuente: Centro de datos del Departamento Informático del GADMCLL

Infraestructura

El GADMCLL cuenta con una conexión permanente de Internet mediante un enlace de fibra óptica con su proveedor.

Está conformada por dos router, cinco switch y un cortafuego que protege los servidores internos.

Los servidores con sistemas operativos de Windows están protegidos con antivirus y los servidores con Linux mantienen listas de acceso.

Control de acceso

Para tener acceso a los sistemas administrativos se lo realiza por medio de una cuenta usuario y clave, las mismas son asignadas a los usuarios, así como también la cuenta de correo electrónico de acuerdo a la petición de cada Jefe departamental.

Entrega de Servicios

Se encuentran los sistemas financieros de recaudación, administrativos y el sistema de gestión registral en plataforma web.El servicio de correo Zimbra es una herramienta importante para la comunicación interna y externa soportada por la plataforma Office 365 de Microsoft. Aplican la virtualización que permite optimizar recursos de acuerdo a las necesidades de cada servicio. El servicio de almacenamiento es de vital importancia y por ello generan backup diariamente y semanalmente y son alojados en otro departamento. El servicio de internet es distribuido por cable a todas las oficinas y de forma inalámbrica a ciertos usuarios.

Soporte Técnico

Se realizan soporte (mantenimiento, instalación de aplicaciones, antivirus y configuración) a todos los equipos informáticos y de comunicación, se detectan incidentes, pero no se previene.

Operaciones

Las siguientes actividades que realizan de forma periódica son:

- ✓ Mantenimiento lógico y físico de servidores de base de datos, cada mes.
- ✓ Diariamente se realiza actualización de firmas de antivirus en los servidores de Windows.
- ✓ Mantenimiento de UPS, cada mes.

Incidentes

- ✓ En ocasiones se desconecta el enlace principal con el ISP
- ✓ En los últimos meses los equipos de climatización se han averiado con frecuencia.
- ✓ La configuración de las computadoras de escritorio ha sido modifica por personas no autorizadas.

Actualmente el Departamento Informático NO cuenta con:

- ✓ Cronograma de mantenimientos de equipos informáticos y de comunicación
- ✓ Mapa de infraestructura de puntos de red
- ✓ Políticas de seguridad
- ✓ Procesos definidos para la administración de cuentas
- ✓ Procedimiento de respuesta ante incidentes

- ✓ Cableado estructurado eléctrico en todas las áreas
- ✓ Administración de copias de seguridad
- ✓ Sistema de detección de intrusos
- ✓ Encriptación y autenticación remota
- ✓ La seguridad de GRUB, archivo de configuración del SO.
- ✓ Restricciones de puertos USB

Se detalla a continuación la situación actual del departamento informático del GADMCLL, tal como se indica en la Tabla 6.

Tabla 6
Situación Actual del DI del GADMCLL

Resultados de la situación actual del DI del GADMCLL

Criterios	Porcentaje de cumplimiento	Recomendaciones
Política de Seguridad	0%	Porcentaje de cumplimiento 0,00%, se debe a que la institución y el DI del GADMCLL no cuenta con políticas de seguridad necesarias para un trabajo organizado y preventivo, por lo que se recomienda urgente crear Políticas de Seguridad y aplicarlas.
Organización de la Información	30%	Porcentaje de cumplimiento 30,00%, se debe a que el DI del GADMCLL tiene definido de manera informal la responsabilidad mediante perfiles de usuarios, por lo que se recomienda la asignación del responsable de Seguridad y la creación de un comité de seguridad, que se encargaran de mantener la política de seguridad y de revisar y aprobar la valoración y los riesgos de la empresa.

CONTINUA

Gestión de Activos	50%	Porcentaje de cumplimiento 50%, se debe a que las actividades de control de riesgo del DI no las tienen totalmente definidas, se recomienda utilizar un código de barra para facilitar las tareas de realización de inventario y vincular los equipos TI que entran y salen de la institución con los empleados. También se recomienda asignación de responsable de la gestión de activos.
Seguridad Lógica a los Recursos Humanos	80%	Porcentaje de cumplimiento 80,00%, se debe a que DI del GADMCLL si cuenta con la selección y contratación, la formación de empleados y salida de la empresa, pero de manera desorganizada, por lo que se recomienda se incluya los criterios de seguridad de la información en la gestión de los Recursos Humanos.
Seguridad Física y del Entorno	70%	Porcentaje de cumplimiento 70,00%, se debe a que el DI del GADMCLL no cuenta con la seguridad física ni mantienen la seguridad de la data center con puerta de control de acceso necesaria para resguardar la información, por lo que se recomienda realizar lineamientos de seguridad para el área física del DI del GADMCLL.
Gestión de Comunicaciones y Operaciones	65%	Porcentaje de cumplimiento 65,00%, se debe a que la institución y el DI del GADMCLL no cuenta con registro de incidencias y fallos y protección contra software malicioso, por lo que se recomienda urgente crear Políticas de Seguridad y aplicarlas.
Control de Accesos	60%	Porcentaje de cumplimiento 60,00%, se debe a que la institución y el DI del GADMCLL cuenta de manera informal el control de acceso a la información, por lo que se recomienda implementar procedimientos formales para controlar la asignación de los permisosy evitar accesos no autorizados.

CONTINUA

Adquisición, desarrollo y Mantenimientos de Sistemas de Información	30%	Porcentaje de cumplimiento 30,00%, se debe a que el DI del GADMCLL cuenta con poco presupuesto para la adquisición, desarrollo y mantenimiento de sistemas de información, por lo que se recomienda desarrollar presupuesto de necesidades de adquisición para el departamento informático.
Gestión de incidencia de la Seguridad de la Información	0,00%	Porcentaje de cumplimiento 0,00%, se debe a que la institución y el DI del GADMCLL no cuenta con procesos de incidencia de la Seguridad de la información, por lo que se recomienda urgente crear lineamientos de Seguridad y aplicarlas.

3.2 Organigrama del Departamento Informático

Figura 8. Organigrama del Departamento Informático DI

3.3 Descripción de las Principales Funciones

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

- ✓ Dirección Informática

Encargado y responsable de administrar y representar a Departamento Tecnológico, proponer proyectos y liderar los procesos de implementación y mejoramiento continuo de todos los procesos del área de sistemas.

- ✓ Analista de Infraestructura y Redes

Encargado de todos los procesos de las áreas técnicas, redes y seguridad de TI, de la instalación y administración de los servidores físicos y virtuales y servicios de red, equipos de red como switches, routers, Access points, puntos de acceso, entre otros. Además, se asegura de la conexión continua e ininterrumpible de la red interna y de internet.

- ✓ Analista de Base de datos

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

- ✓ Analista Técnico

Encargado del mantenimiento y configuración de los computadores de escritorio, portátiles y periféricos; instalación de los programas utilitarios, apoyo en las demás áreas, helpdesk y de dar seguimiento del cumplimiento de las garantías de los equipos informáticos y de comunicación.

3.4 Inventario de Equipos

Tabla 7
Inventario de Hardware

INVENTARIO DE HARDWARE		
No.	Descripción	Dirección Informática
1	Servidores	Servidor de Base de Datos - IBM System X3250 M5 Intel Xeon E3-1230 v3 3.30GHz
		Servidor de Aplicaciones - IBM System X3250 M5 Intel Xeon E3-1230 v3 3.30GHz
		Servidor de Correo electrónico
		Servidor de Antivirus– Virtual
		Servidor de Archivos– Virtual
2	Computadores personales	Computadores personales - Windows 7 y Linux
		Computadores servidores - Windows Server 2003
3	Almacenamiento de datos	Discos duros locales
		Discos duros externos
4	Periféricos de impresión y escáner	Impresoras
		Escáner
5	Soporte de red	Switch, Router y Firewall
6	Central telefónica	Central telefónica

Tabla 8
Inventario de Comunicaciones/Redes

INVENTARIO DE COMUNICACIONES/REDES		
No.	Descripción	Dirección Informática
1	Red telefónica	Red telefónica
2	Red Local	Red LAN
3	Internet	Internet

Tabla 9
Inventario de Soporte de Información

INVENTARIO DE SOPORTE DE INFORMACIÓN		
No.	Descripción	Dirección Informática
1	Electrónicos	Discos duros
	Discos	Discos compactos
	CD-ROM	Disco versátil digital
	Dispositivos USB	Dispositivos USB
	DVD	
	Tarjetas de Memoria	
2	No electrónicos	Impresiones
	material impreso	

Tabla 10
Inventarios de Servicios

INVENTARIO DE SERVICIOS		
No.	Descripción	Dirección Informática
1	Servicios/ usuarios internos	Mantenimiento de hardware, equipos y software Control en la web
2	Contratos	Internet
		Desarrollo software registro
3	Aplicaciones y servicios	Correo electrónico
		Video conferencia
4	Almacenamiento de archivos	Almacenamiento de archivo
5	Gestión de usuarios	Gestión de usuarios
6	Gestión de privilegios	Gestión de perfiles de usuarios

Tabla 11
Inventario de datos/información

INVENTARIO DE DATOS/INFORMACIÓN		
No.	Descripción	Dirección Informática
1	Datos vitales (importantes)	Base de datos Administrador de los servidores
2	Datos de configuración	Administración y configuración de la red local Administración de firewall Claves de acceso y creación de perfiles de usuarios
3	Datos clasificados	Claves de administrador de diferentes sistemas - Nivel Reservado Claves de administración de servidores - Nivel Reservado

Tabla 12
Inventario de Software/Aplicaciones

INVENTARIO DE SOFTWARE/APLICACIONES		
No.	Descripción	Dirección Informática
1	Desarrollo local (propio)	Sistema financiero y administrativo - Oracle versión 11g
2	Desarrollo contratado	Sistema de Gestión Registral – Plataforma web Sistema Qdoc – Licencia
3	**Estándar**	
	Navegador web	Browser - Navegador Web - Mozilla Firefox
	Servidor de aplicaciones	Centos 6 – Máquinas virtuales con PROXMOX
	cliente de correo electrónico	Sistema Operativo Windows 7 y Linux Ubuntu 12
	sistema de gestión de base de datos	Oracle 11g de 64 bit bajo Linux – Centos 6.8
	anti virus	Servidor proxy squid – Licencia libre
	sistema operativo	Sistema Operativo Windows server 2003

Tabla 13
Inventario de Equipo/Auxiliar

INVENTARIO DE EQUIPO/AUXILIAR		
No.	Descripción	Dirección Informática
1	Cableado	Cableado UTP categoría 6ª
		Fibra óptica
2	Regulador de Voltaje	Regulador de Voltaje
3	Sistema de alimentación ininterrumpida	Sistema de alimentación ininterrumpida

Tabla 14
Inventario de Instalaciones/Infraestructura

INVENTARIO DE INSTALACIONES/INFRAESTRUCTURA		
No.	Descripción	Dirección Informática
1	Ubicación	DI – GADMCLL
2	Edificio	Edificio Municipal del GADMCLL
3	Departamento	DI - Centro de datos

Tabla 15
Inventario de Personal del DI

INVENTARIO DE PERSONAL		
No.	Descripción	Dirección Informática
1	Administrador – Director	Administrador – Director
2	Analista de Bases de datos	Analista de Bases de datos
3	Analista de comunicaciones	Analista de comunicaciones
4	Analista Soporte	Soporte

CAPÍTULO 4
DESARROLLO DEL ANÁLISIS DE RIESGO INFORMÁTICODEPARTAMENTO INFORMÁTICO DEL GADMCLL

4.1 Análisis de Riesgo

Actividades de una gestión de riesgo:

1.- Levantar un modelo del valor del sistema, identificando y valorando los activos relevantes.

2.- Identificar y valorar las amenazas sobre aquellos activos.

3.- Levantar un conocimiento de la situación actual de salvaguardas.

4.- Evaluar el impacto posible sobre el sistema en estudio, tanto el impacto potencial como el residual.

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

6. Informar a las áreas del sistema con mayor impacto o riesgo a fin de que se puedan tomar las decisiones de tratamiento con motivo justificado. El análisis mediante la herramienta PILAR se ha realizado para tener una guía referencial respecto al estudio realizado de forma manual, PILAR identifica las amenazas que afectan a los activos de forma directa e indirecta para finalmente obtener gráficas con los resultados.

Para realizar el Análisis de Riesgo Informático del departamento informático del GADMCLL se mostrará la situación actual de la misma se utilizará información que se consiguió de entrevistas y visita técnica.

Es importante mencionar que es la primera vez que se realiza un análisis de riesgo informático a los diferentes activos informáticos del departamento informático del GADMCLL.

4.1.1 Datos del Proyecto en PILAR

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

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

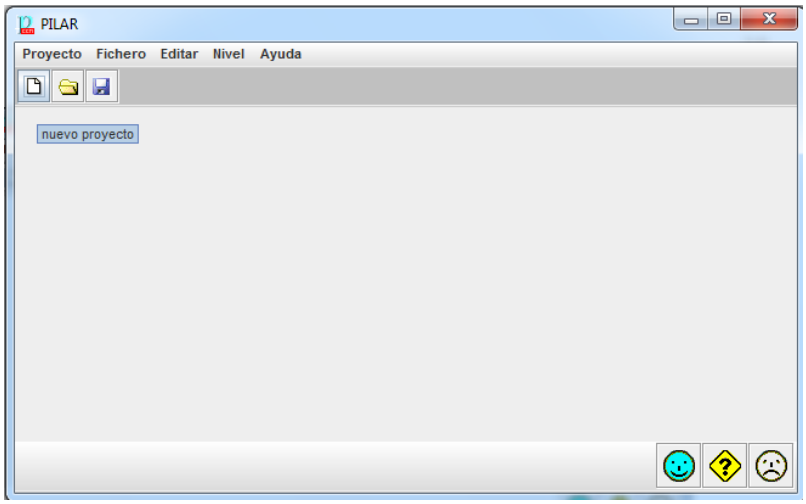


Figura 9. Creación de nuevo proyecto

Al momento de escoger nuevo proyecto se presenta una ventana donde deberá ingresar los datos del proyecto tal como se muestra en la Figura 10. , una vez completada la información se guardaran los datos y se cerrara la ventana.

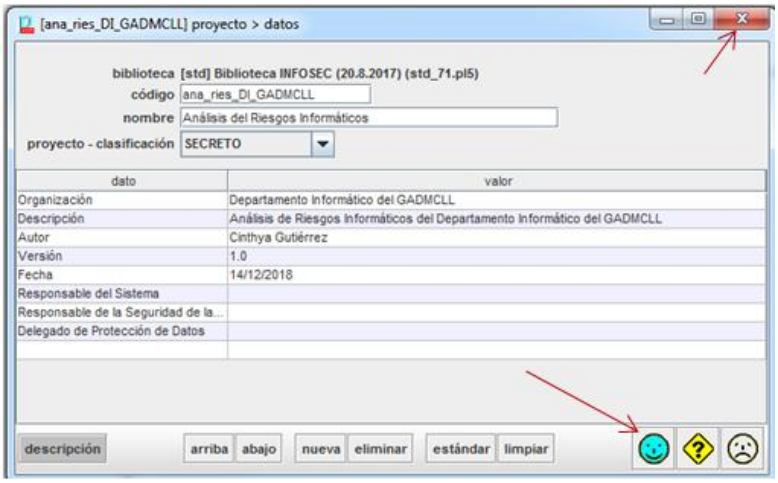


Figura 10. Datos del proyecto

4.1.2 Dominios de Seguridad

Para el análisis de riesgos informáticos del departamento informático del GADMCLL se creó el dominio de seguridad Base_DI que contendrá todos los activos informáticos de este proyecto, tal como se muestra en Figura 11.

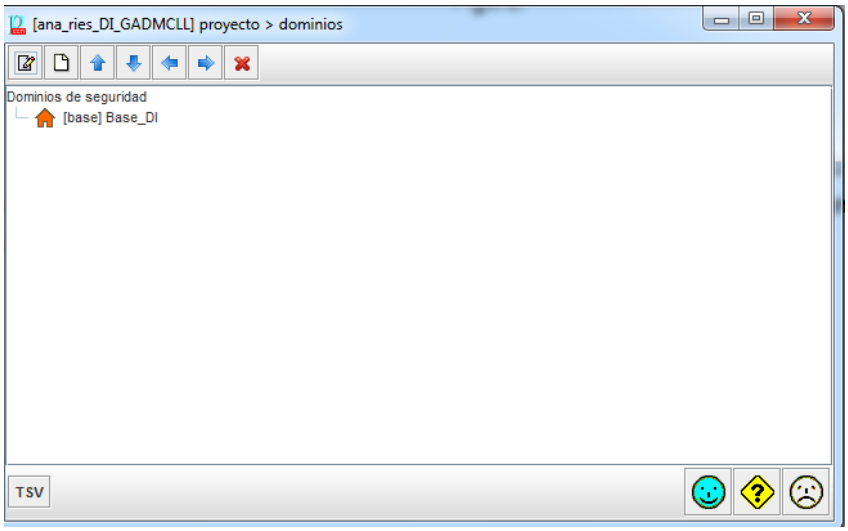


Figura 11. Dominio de seguridad Base_DI

4.1.3 Fases del Proyecto

En esta etapa PILAR permite identificar las fases del proyecto presentando la evolución del riesgo informático, en nuestro caso PILAR posee la identificación [current], situación actual, tal como lo indica la Figura 12.

Figura 12. Situación actual

4.2 Modelo de Valor

"Está conformado por la identificación de los activos considerados prioritarios en las actividades fundamentales de la organización, relación entre los activos, la valoración; y finalmente los resultados obtenidos reflejan la importancia que incurren cada uno, dentro de la organización". Se detalla a continuación los activos prioritarios del departamento informático del GADMCLL.

4.2.1 Identificación de Activos

Equipamiento - Hardware

- ✓ Servidores.- Se encuentran dentro del centro de datos y son administrados por el personal de infraestructura y sistemas, cuenta con dos servidores Servidor IBM System X3250 M5 Intel Xeon E3-1230 v3 3.30GHz
- ✓ Equipos de comunicaciones.- Los equipos que conforman la red de voz y datos ubicados en el centro de datos que son administrados por personal de infraestructura, cuentan con 5 Switches de 24 puertos.
- ✓ Computadores personales.- PCs con sistemas operativos Linux y Windows de 64 bits.

Equipamiento - Software

- ✓ Sistema administrativo y financiero Municipal en Oracle.
- ✓ Almacenamiento – bases de datos.- Oracle 11G R2 de 64 bits bajo Linux Centos 6.8, esto es administrado por administrador de bases de datos.

- ✓ Correo electrónico.- Zimbra.
- ✓ Virtualización.- Máquinas virtuales con Proxmox.

Comunicaciones

- ✓ Internet.- ISP CNT mediante fibra óptica.
- ✓ Red alámbrica.- Conexiones alámbricas de fibra óptica y cable UTP categoría 6a.
- ✓ Red inalámbrica.- Access points
- ✓ Enlace con proveedor.- Router de ISP mediante fibra.

Equipamiento Auxiliar

- ✓ UPS.- se consideran a las baterías que protegen a los servidores y equipos de comunicación de fallos eléctricos, cuentan con 1 UPS de 10 kv.
- ✓ Generador eléctrico.-Engine Make & Model Perkins 1506D-E88TAG4
- ✓ Equipos de climatización.
- ✓ Cableado eléctrico.- Puntos regulados de 110 volteos que conectan al centro de datos, cuarto del generador eléctrico abasteciendo al resto de departamentos de energía eléctrica a los diferentes equipos informáticos.

Instalaciones

- ✓ Centro de datos.- Sealojan todos los servidores y equipos de comunicación del departamento informático del GADMCLL,dos servidores Servidor IBM System X3250 M5 Intel Xeon E3-1230 v3 3.30GHz, también se encuentran 2 rack de comunicación.

Personal

- ✓ Analista de Base de datos

- ✓ Analista técnico.
- ✓ Analista de Infraestructura
- ✓ Administrador- Director

4.2.2 Identificación de Activos en PILAR

PILAR permite definir diferentes capas, grupos y activos informáticos, se inicia haciendo clic en la opción Activos y se puede visualizar que se despliega un listado en el cual escogemos la opción Identificación, tal como se muestra en Figura 13.

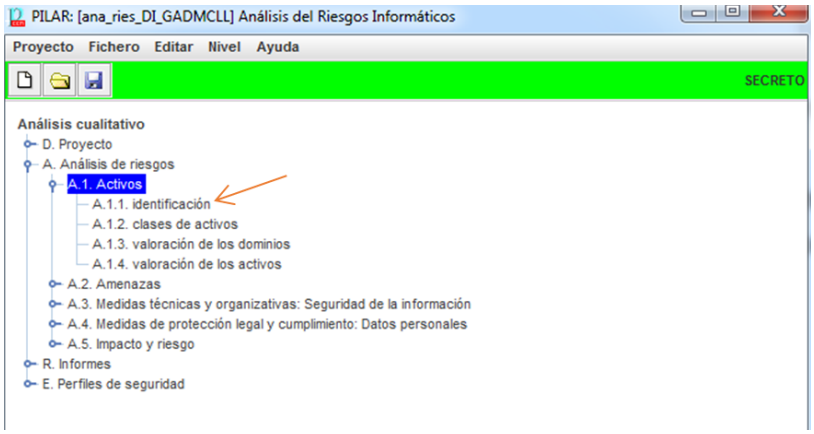


Figura 13. Selección de activos

Si se quiere crear una nueva capa, PILAR dispone de una capa estándar para una mejor agrupación de activos la cuál puede ser modificada de acuerdo a las necesidades del proyecto que maneja el usuario, dando clic en la opción capas y escogiendo nueva capa, tal como se indica en la Tabla 14.

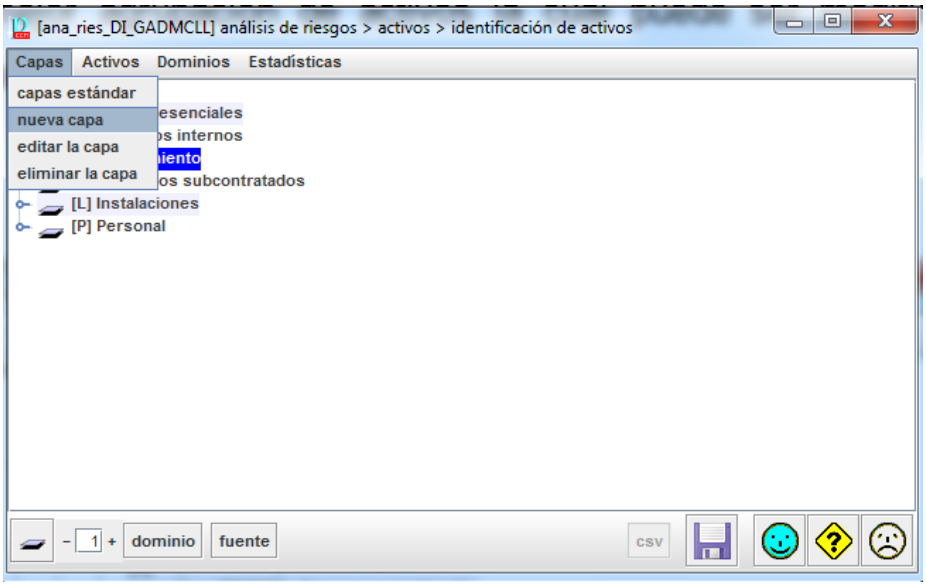


Figura 14. Agregar nueva capa

Cuando se define una nueva capa de activos informáticos, se debe poner un código único a la capa y un nombre de identificación, en nuestro caso no se ha creado una nueva capa se ha trabajado con la estándar.

En cada capa específica podrá agregar varios grupos de activos informáticos y a si mismo tendrá que definir código único y nombre de identificación, tal como se muestra en la siguiente Figura 15.

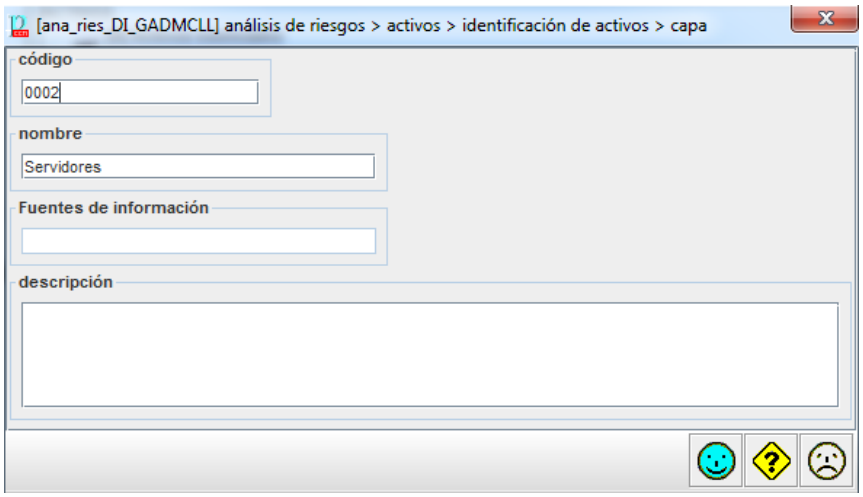


Figura 15. Ejemplo de Identificación y nombre a la capa

Una vez que se crea la capa se debe agregar un grupo de activos informáticos a la misma identificándose con un código único, un nombre y un código de seguridad y estar en una clase activo, como se muestra en la Figura 16.

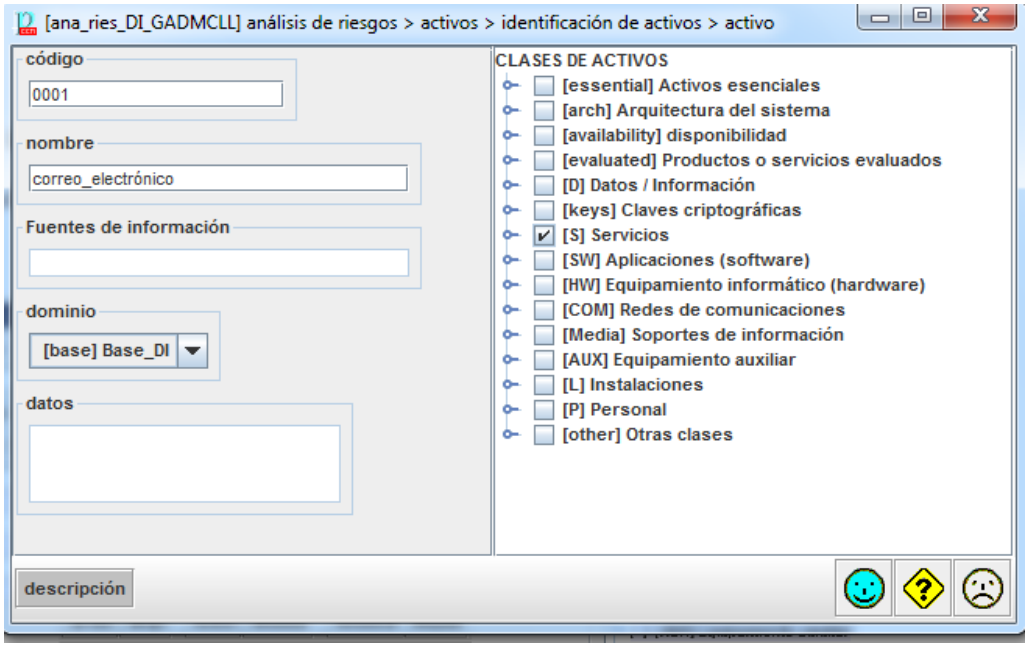


Figura 16. Grupo de activo informático Aplicaciones

A continuación, podrán agregarse los activos informáticos dentro del grupo de activos haciendo clic derecho sobre la carpeta amarilla y seleccionando nuevo activo – nuevo activo, como se muestra en la Figura 17 y 18.

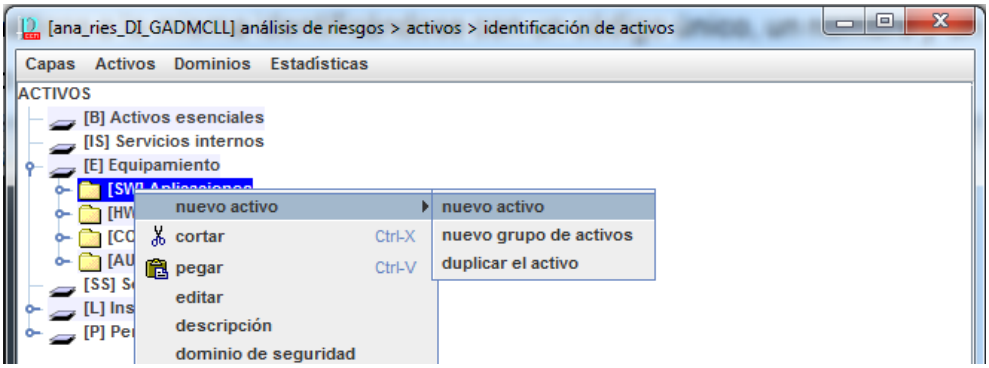


Figura 17. Nuevo activo

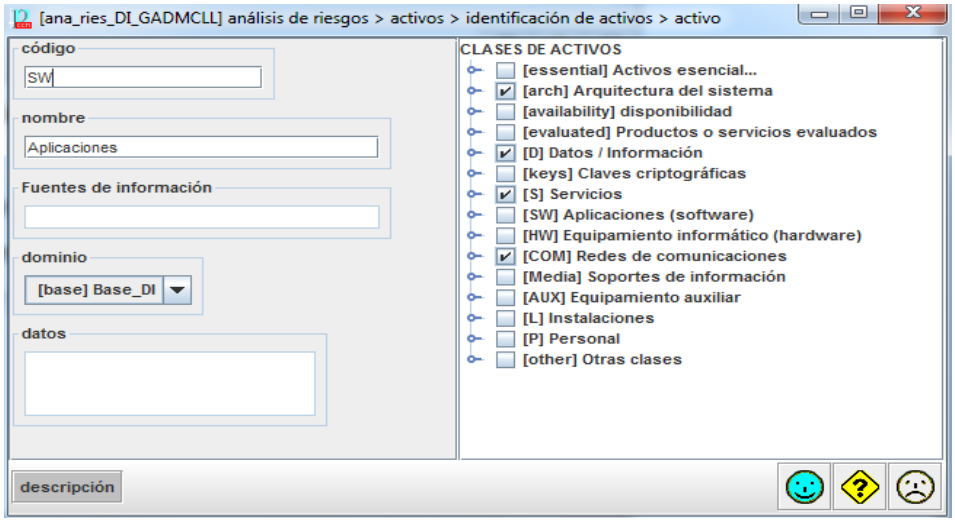


Figura 18. Identificación de activos

A continuación, se muestra en la Tabla 19 todos los activos agregados.

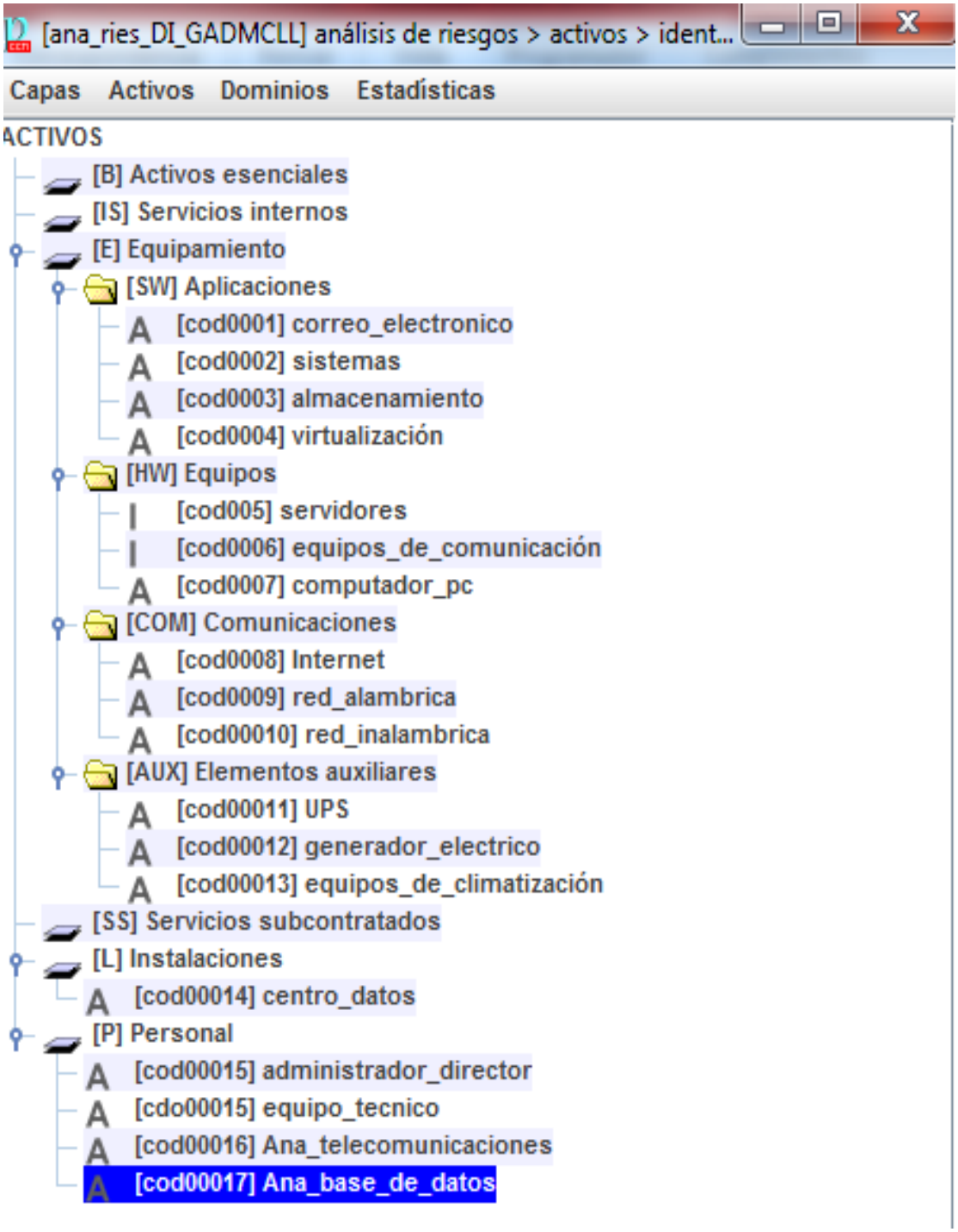


Figura 19. Activos agregados

4.2.3 Árbol de dependencia

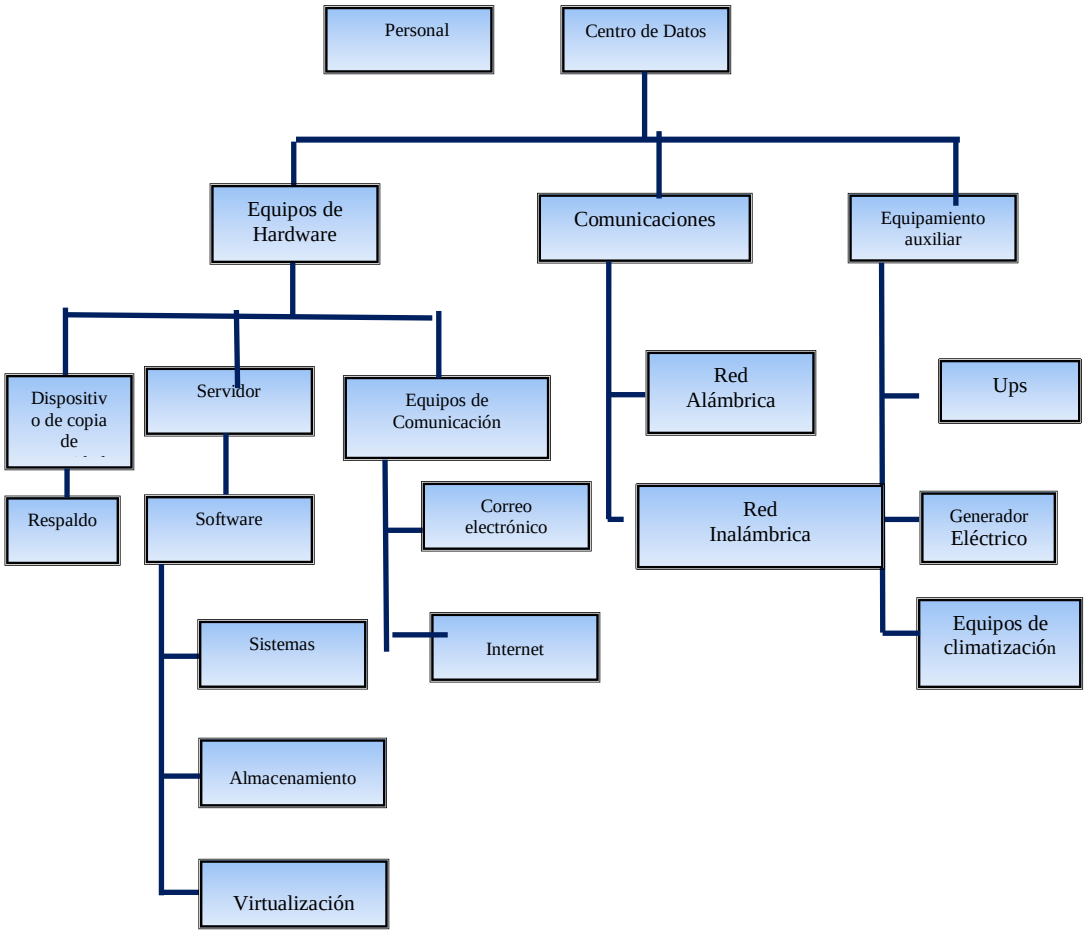


Figura 20. Árbol de dependencia

Como podemos observar en la figura 20., se encuentra el árbol jerárquico de activos de cuerdo al nivel de dependencia. Se ha considerado en el primer nivel al centro de datos, lugar donde se encuentran alojados los servidores y equipos de comunicación, los mismos que se encuentran en el segundo nivel así también como el equipamiento auxiliar.

En el tercer nivel están los servicios y aplicaciones, también se ha considerado los equipos de climatización y generador de electricidad en el centro de datos los cuales son de mayor importancia para el desarrollo y funcionamiento de los equipos.

4.2.4 Clases de Activos

PILAR con esta opción permite asignar la clase de activo a la que pertenece a cada activo informático, tal como se muestra en la Tabla 21.

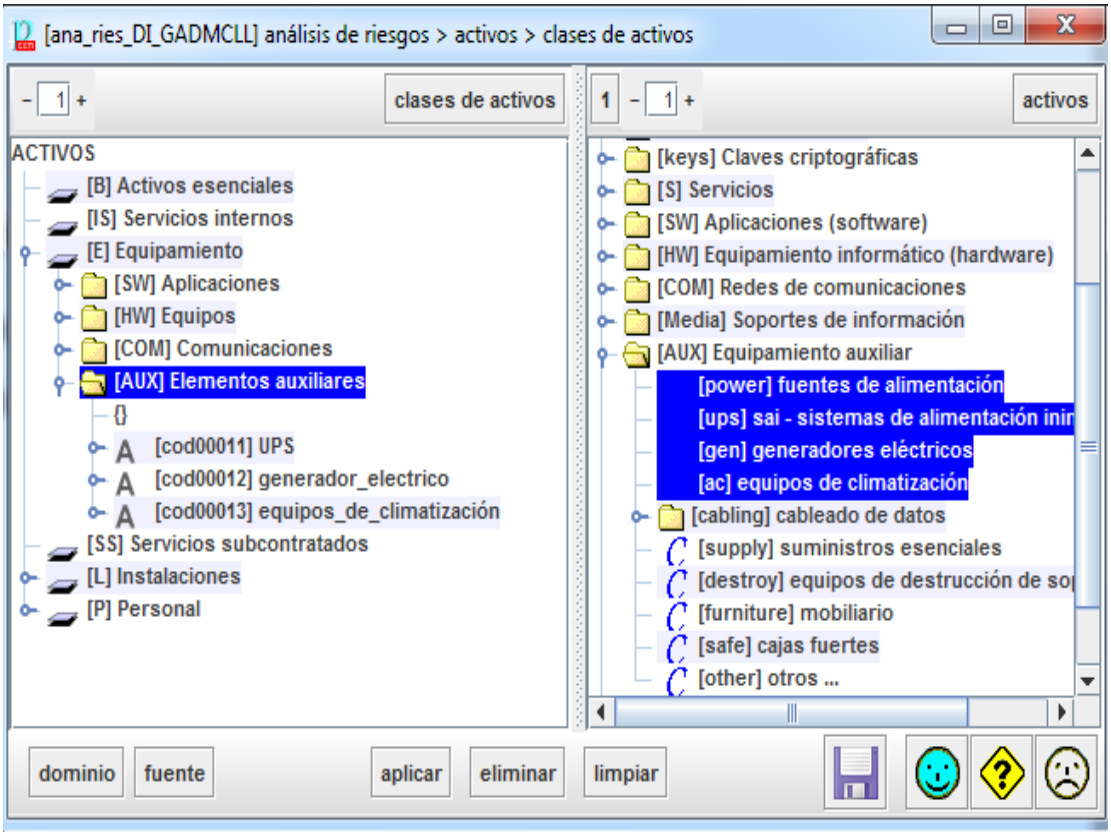


Figura 21. Clase de activo

4.2.5 Dependencias de activos en PILAR

En la figura 22, se ha determinado la dependencia que existe entre los servidores con el equipamiento auxiliar, personal e instalaciones.

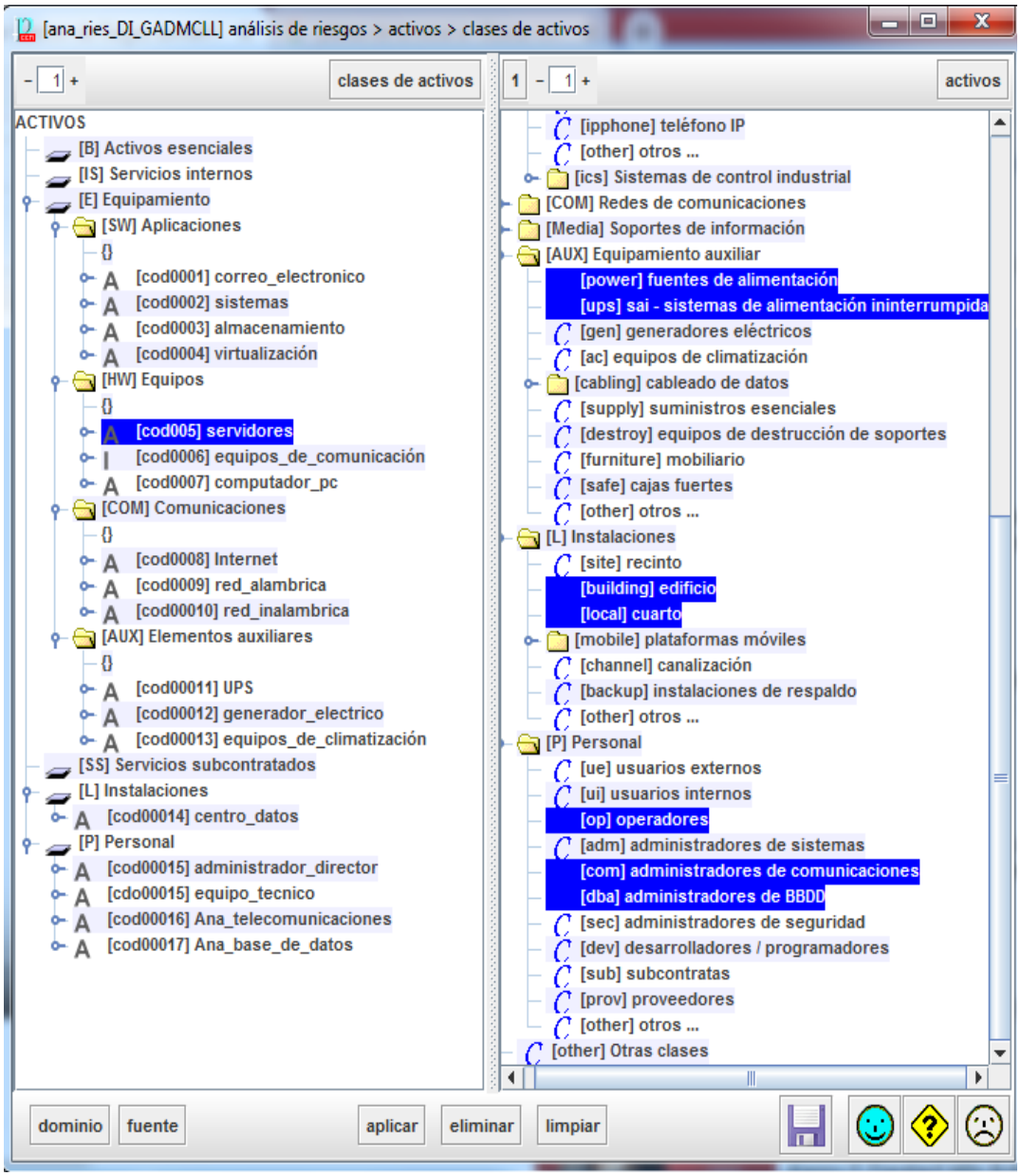


Figura 22. Definición de la dependencia entre activos

4.2.6 VALORIZACIÓN DE ACTIVOS

Una vez realizada la dependencia de activos se realizará la evaluación de los activos en cada uno de los parámetros de seguridad para identificar los diferentes tipos de amenazas a las que se verían afectados al ser expuesto a ellas y lo que causaría si existiera perdida de información o daño físico.

Esta valorización de activos se ha realizado tomando como referencia la escala de criterios definida en la tabla 16.

Escala de Criterios

Tabla 16
Escala de criterios

VALOR		CRITERIO
10	Extremo	Daño extremadamente grave
9	Muy Alto	Daño muy grave
6-8	Alto	Daño grave
3-5	Medio	Daño importante
1-2	Bajo	Daño menor
0	Despreciable	Irrelevante a efectos prácticos

Tabla 17
Valoración de amenazas 1

	Equipamiento - Hardware												Equipamiento - Software														
	Servidores			Equipos de Comunicaciones			Dispositivo de respaldo			Computador de personal			Financiero, Registral y admin.			Almacenimiento Base de datos			Correo electronico			Virtualización			Internet		
AMENAZAS	D	I	C	D	I	C	D	I	C	D	I	C	D	I	C	D	I	C	D	I	C	D	I	C	D	I	C
Incendio	10			10			10			10			8			8			8			10			10		
Terremoto	10			10			10			10			8			8			8			10			10		
Sobrecarga eléctrica																											
Falla de generador eléctrico	8			8			8			8			8			8			8			8			8		
Falla de equipos de climatización	6			6			6			6			6			6			6			6			6		
Errores de Configuración		5			6									6						6			6					
Desconexión física y lógica	8			8						2						9			8			8			10		
Agotamiento de recursos	6															8											
Spyware		8									5																
Malware	8	8								5	5																
Phishing																				6							
Spam																				6							
Flooding				6																							
Acceso no autorizado			9			9						8		8			9			9			8				
Robo	10			10			10			8																	
Fuga de información																											

Tabla 18
Valorización de activos 2

	Instalaciones						Equipamiento auxiliar												Personal								
	Centro de datos			Cuarto de Red			UPS			Generadores eléctricos			Equipos de climatización			Cableado eléctrico			Equipo técnico			Ana. de base de datos			Ana. de telecomunic.		
AMENAZAS	D	I	C	D	I	C	D	I	C	D	I	C	D	I	C	D	I	C	D	I	C	D	I	C	D	I	C
Incendio	10			10			10			10			10			10			10			10			10		
Terremoto	10			10			10			10			10			10			10			10			10		
Sobrecarga eléctrica	9			9			8			8			9			8											
falla de generador eléctrico	8			8						10																	
falla de equipos de climatización	8			8									10														
Errores de Configuración																											
Desconexión física y lógica	10			10												10											
Agotamiento de recursos	5			5																							
Spyware																											
Malware																											
Phishing																											
Spam																											
Flooding																											
Acceso no autorizado	8			8															10			10			10		
Robo							10			10			10			5											
Fuga de información																			10			10			10		

4.2.7 VALORIZACION DE ACTIVOS EN PILAR

Para realizar la valorización de los activos informáticos se debe escoger la opción "Activos" y luego "valorización de los activos", como se muestra en la figura 23.

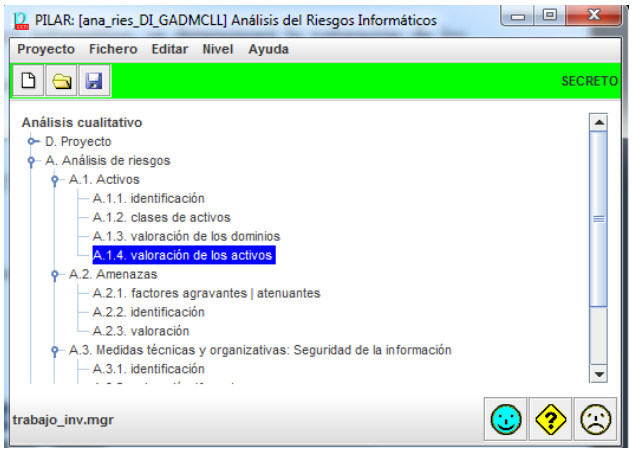


Figura 23. Opción valorización de activos

PILAR nos proporciona una serie de criterios de valoración y cada activo informático debe realizar una valoración por cada dimensión de seguridad, tal como se indica en la figura 24.

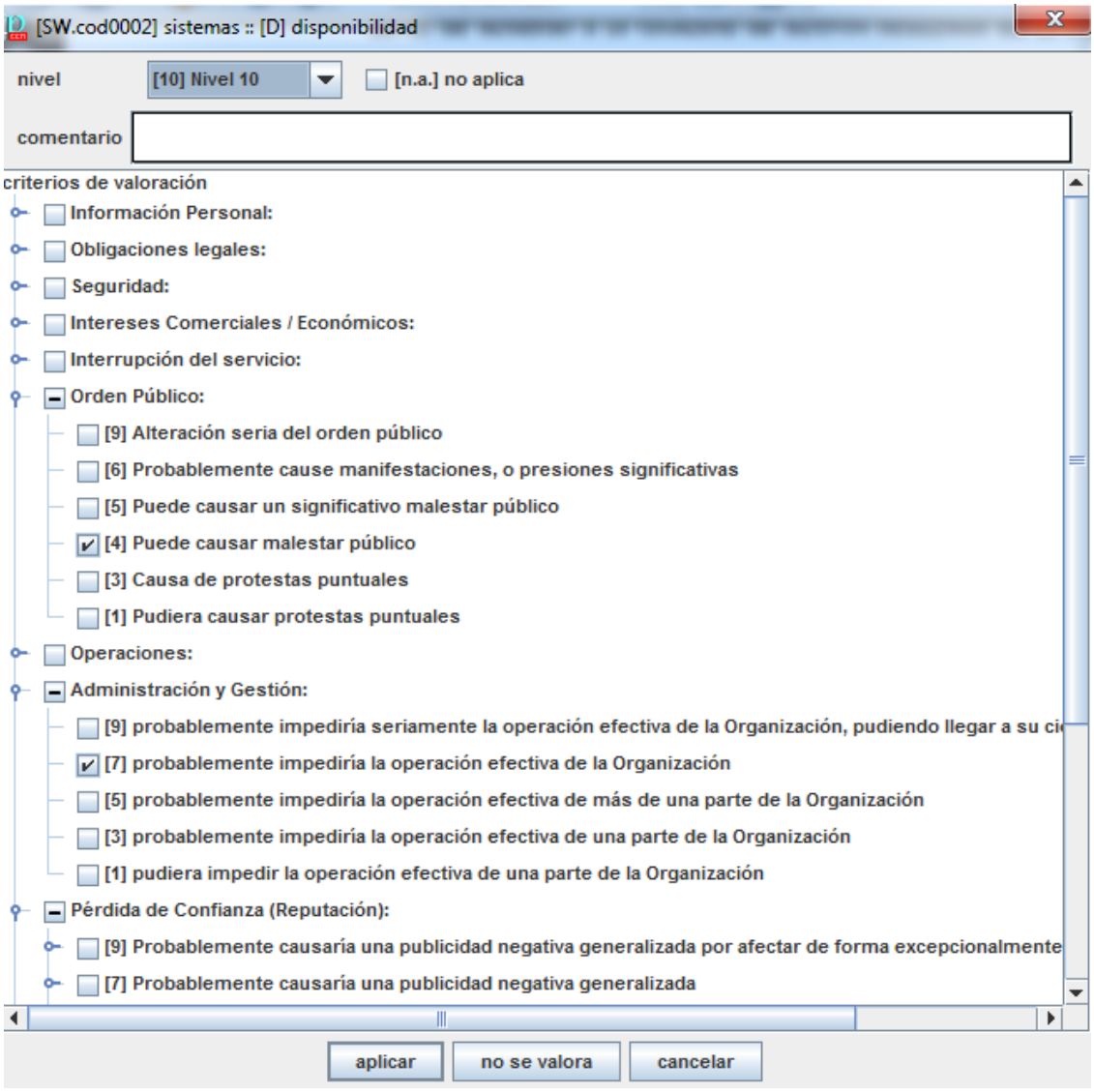
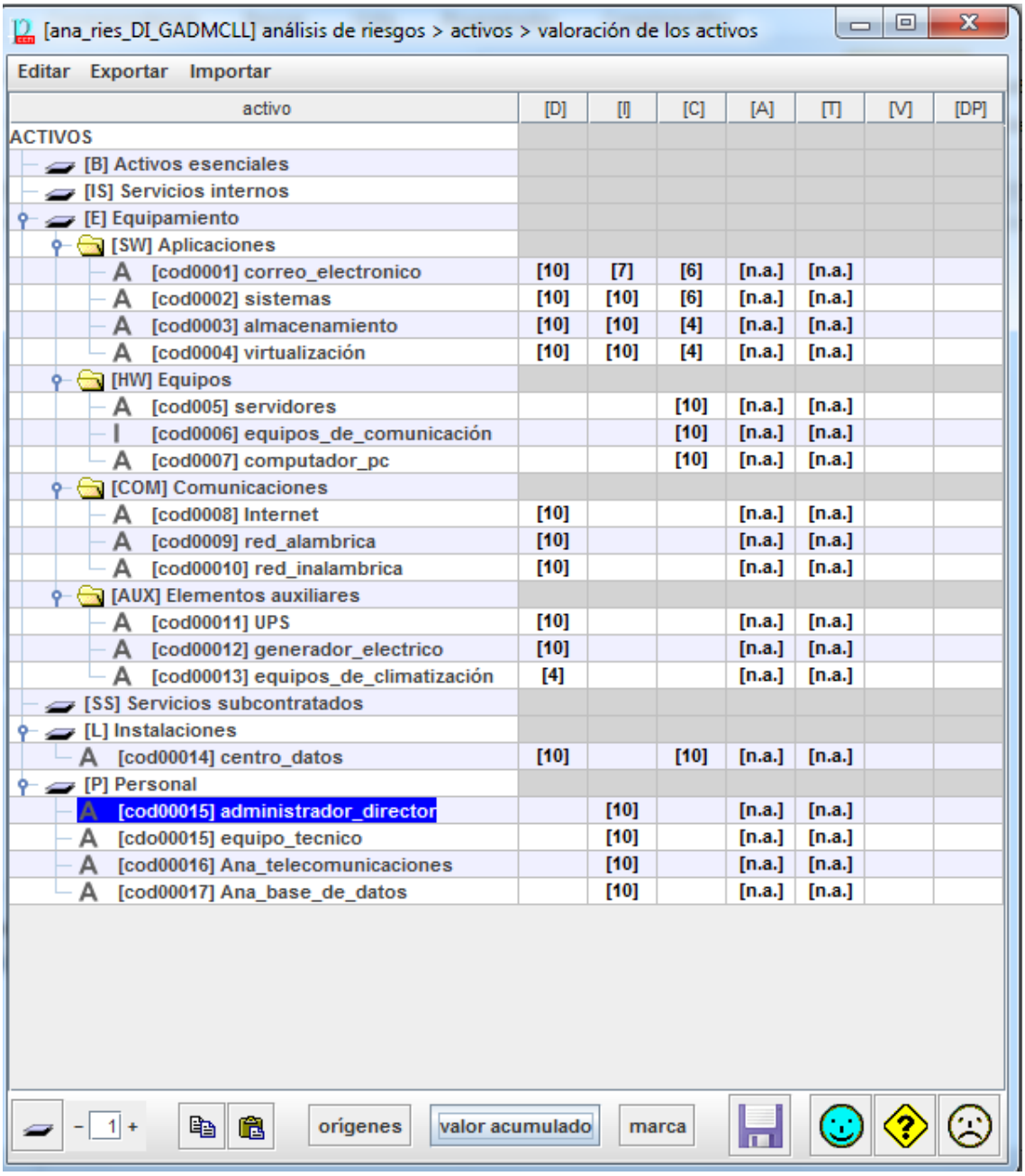


Figura 24. Criterios de valoración

Se presenta la valoración de los activos en PILAR en la Figura 25. , con ésta herramienta se permite realizar la valoración de los activos en tres tipos de niveles, alto, medio y bajo.



activo	[D]	[I]	[C]	[A]	[T]	[V]	[DP]
ACTIVOS							
[B] Activos esenciales							
[IS] Servicios internos							
[E] Equipamiento							
[SW] Aplicaciones							
[cod0001] correo_electronico	[10]	[7]	[6]	[n.a.]	[n.a.]		
[cod0002] sistemas	[10]	[10]	[6]	[n.a.]	[n.a.]		
[cod0003] almacenamiento	[10]	[10]	[4]	[n.a.]	[n.a.]		
[cod0004] virtualización	[10]	[10]	[4]	[n.a.]	[n.a.]		
[HW] Equipos							
[cod005] servidores			[10]	[n.a.]	[n.a.]		
[cod0006] equipos_de_comunicación			[10]	[n.a.]	[n.a.]		
[cod0007] computador_pc			[10]	[n.a.]	[n.a.]		
[COM] Comunicaciones							
[cod0008] Internet	[10]			[n.a.]	[n.a.]		
[cod0009] red_alambrica	[10]			[n.a.]	[n.a.]		
[cod00010] red_inalambrica	[10]			[n.a.]	[n.a.]		
[AUX] Elementos auxiliares							
[cod00011] UPS	[10]			[n.a.]	[n.a.]		
[cod00012] generador_electrico	[10]			[n.a.]	[n.a.]		
[cod00013] equipos_de_climatización	[4]			[n.a.]	[n.a.]		
[SS] Servicios subcontratados							
[L] Instalaciones							
[cod00014] centro_datos	[10]		[10]	[n.a.]	[n.a.]		
[P] Personal							
[cod00015] administrador_director		[10]		[n.a.]	[n.a.]		
[cdo00015] equipo_tecnico		[10]		[n.a.]	[n.a.]		
[cod00016] Ana_telecomunicaciones		[10]		[n.a.]	[n.a.]		
[cod00017] Ana_base_de_datos		[10]		[n.a.]	[n.a.]		

Figura 25. Valoración de los activos en PILAR

En PILAR se puede calcular el valor propio y acumulado de cada activo informático tal como se muestra en la figura 26.

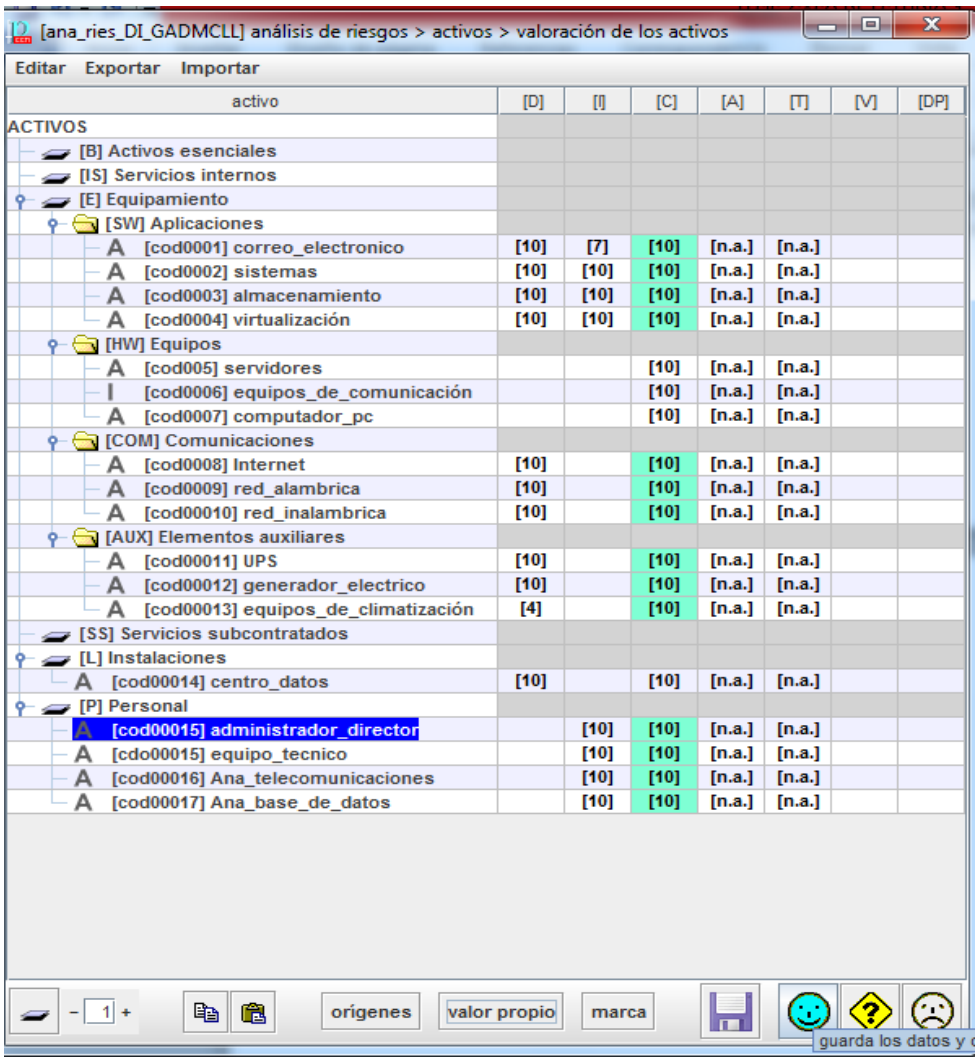


Figura 26.Valor propio y acumulado de activos en PILAR

4.3AMENAZAS

Se han considerado las amenazas que causan más daño a los activos de la institución con el fin de evaluar el nivel del riesgo.

4.3.1 VALORIZACIÓN DE AMENAZAS POR ACTIVOS

Tabla 19

Valorización de Amenazas por Activos

TIPOS DE ACTIVOS	ACTIVOS	AMENAZAS RELEV.	DEGRADACIÓN	FRECUENCIA	RIESGO
EQUIPAMIENTO - HARDWARE	SERVIDORES	Incendio	MA	MB	MEDIO
		Terremoto	MA	MB	MEDIO
		Robo	A	B	MEDIO
		Acceso no autorizado	A	M	ALTO
	EQUIPO DE COMUNICACIÓN	Incendio	MA	MB	MEDIO
		Terremoto	MA	MB	MEDIO
		Robo	A	B	MEDIO
		Acceso no autorizado	M	B	ALTO
		Desconexión física o lógica	MA	A	ALTO
		Falla de generador eléctrico	A	MB	MEDIO
	DISPOSITIVO DE ALMACENAM.	Incendio	MA	MB	MEDIO
		Terremoto	MA	MB	MEDIO
		Robo	A	B	MEDIO
	COMPUTADOR DE PERSONAL	Incendio	MA	MB	MEDIO
		Terremoto	MA	MB	MEDIO
		Robo	MA	B	MEDIO
		Malware	M	A	ALTO
EQUIPAMIENTO - SOFTWARE	SISTEMAS FINANCIEROS, ADMINISTRATIVOS Y REGISTRAL	Incendio	MA	MB	MEDIO
		Terremoto	MA	MB	MEDIO
		Acceso no autorizado	M	A	ALTO
	BASE DE DATOS - ALMACENAMIENTO	Acceso no autorizado	M	M	MEDIO
		Desconexión física o lógica	MA	B	MEDIO
		Agotamiento de recursos	MA	M	ALTO
	CORREO ELECTRÓNICO	Incendio	MA	MB	MEDIO
		Terremoto	MA	MB	MEDIO
		Acceso no autorizado	A	A	ALTO
		Desconexión física o lógica	MA	M	ALTO
	VIRTUALIZACIÓN	Incendio	MA	MB	MEDIO
		Terremoto	MA	MB	MEDIO
		Acceso no autorizado	MA	A	ALTO
		Desconexión física o lógica	MA	M	ALTO
	INTERNET	Incendio	MA	MB	MEDIO
		Terremoto	MA	MB	MEDIO
		Desconexión física o lógica	MA	MA	ALTO
COMUNICACIONES	RED ALÁMBRICA	Incendio	MA	MB	MEDIO
		Terremoto	MA	MA	MEDIO
	RED INALÁMBRICA	Incendio	MA	MB	MEDIO
		Terremoto	MA	MA	MEDIO
	ENLACE CON PROVE.	Incendio	MA	MB	MEDIO
		Terremoto	MA	MB	MEDIO
		Desconexión física o lógica	MA	A	ALTO
EQUIPAMIENTO AUXILIAR	UPS	Incendio	MA	MB	MEDIO
		Terremoto	MA	MB	MEDIO
		Falla de equipo de climatiza	A	MA	ALTO
	GENERADOR ELÉCTRICO	Incendio	MA	MB	MEDIO
		Terremoto	MA	MB	MEDIO
	EQUIPOS DE CLIMATIZACIÓN	Incendio	MA	MB	MEDIO
		Terremoto	MA	MB	MEDIO
		Falla de equipo de climatiza	MA	MA	ALTO
	CABLEADO ELÉCTRICO	Incendio	MA	MB	MEDIO
		Terremoto	MA	MB	MEDIO
		Desconexión física o lógica	MA	B	MEDIO
INSTALACIONES	CENTRO DE DATOS	Incendio	MA	MB	MEDIO
		Terremoto	MA	MB	MEDIO
		Acceso no autorizado	MA	B	MEDIO
PERSONAL	ADMINISTRADOR	Incendio	MA	MB	MEDIO
		Terremoto	MA	MB	MEDIO
		Fuga de información	A	A	ALTO
	EQ. TÉCNICO	Incendio	MA	MB	MEDIO
		Terremoto	MA	MB	MEDIO
		Fuga de información	A	A	ALTO
	ANAL. TELECOM.	Incendio	MA	MB	MEDIO
		Terremoto	MA	MB	MEDIO
		Fuga de información	A	A	ALTO
	ANAL. BASE DE DATOS	Incendio	MA	MB	MEDIO
		Terremoto	MA	MB	MEDIO
		Fuga de información	A	A	ALTO

4.3.2 VALORIZACIÓN DE ACTIVOS POR AMENAZAS

Tabla 20

Valorización de Activos por Amenazas

NATURALES Y DE ENTORNO	INCENDIO Y TERREMOTO	SERVIDORES	MA	MB	MEDIO
		EQUIPO DE COMUNICACIÓN	MA	MB	MEDIO
		DISPOSITIVO DE ALMACENAM.	MA	MB	MEDIO
		COMPUTADOR DE PERSONAL	MA	MB	MEDIO
		SISTEMAS FINANCIEROS, ADMINISTRATIVOS Y REGISTRAL	MA	MB	MEDIO
		BASE DE DATOS - ALMACENAMIENTO	MA	MB	MEDIO
		CORREO	MA	MB	MEDIO
		VIRTUALIZACIÓN	MA	MB	MEDIO
		INTERNET	MA	MB	MEDIO
		RED ALÁMBRICA	MA	MB	MEDIO
		RED INALÁMBRICA	MA	MB	MEDIO
		ENLACE CON PROVE.	MA	MB	MEDIO
		UPS	MA	MB	MEDIO
		GENERADOR ELÉCTRICO	MA	MB	MEDIO
		EQUIPOS DE CLIMATIZACIÓN	MA	MB	MEDIO
		CABLEADO ELÉCTRICO	MA	MB	MEDIO
		CENTRO DE DATOS	MA	MB	MEDIO
		ADMINISTRADOR	MA	MB	MEDIO
		EQ. TÉCNICO	MA	MB	MEDIO
		ANAL. TELECOM.	MA	MB	MEDIO
		ANAL. BASE DE DATOS	MA	MB	MEDIO
ATAQUE NO DELIBERADO	FALLA DE GENERADOR ELECTRICO	SERVIDORES	A	B	MEDIO
		EQUIPO DE COMUNICACIÓN	A	B	MEDIO
	AGOTAMIENTO DE RECURSOS	BASE DE DATOS – ALMACENA-MIENTO	MA	MB	MEDIO
	FALLA DE EQUIPO DE CLIMATIZACIÓN	UPS	A	M	ALTO
		EQUIPOS DE CLIMATIZACIÓN	MA	MA	ALTO
	ACCESO NO AUTORIZADO	SERVIDORES	A	M	ALTO
		EQUIPO DE COMUNICACIÓN	M	B	ALTO
		SISTEMAS	M	A	ALTO
		BASE DE DATOS - ALMACENAMIENTO	MA	M	MEDIO
		CORREO ELECTRÓNICO	A	A	ALTO
		VIRTUALIZACIÓN	MA	A	ALTO
		CENTRO DE DATOS	MA	B	MEDIO
	ROBO	SERVIDORES	A	B	MEDIO
		EQUIPO DE COMUNICACIÓN	A	B	MEDIO
		DISPOSITIVO DE ALMACENAM.	MA	B	MEDIO
		EQUIPO DE	MA	B	MEDIO
	DESCONEXIÓN FÍSICA Y LÓGICA	EQUIPO DE	M	A	ALTO
		BASE DE DATOS -	MA	B	MEDIO
		CORREO	MA	M	ALTO
		VIRTUALIZACIÓN	MA	M	ALTO
		INTERNET	MA	MA	ALTO
		ENLACE CON PROVE.	MA	A	ALTO
		CABLEADO ELÉCTRICO	MA	B	MEDIO
	FUGA DE INFORMACIÓN	ANAL. DE BASE DE	A	A	ALTO
		EQU. TECNICO	A	A	ALTO
		ANAL. COMUNICACIONES	A	A	ALTO
		ADMINISTRADOR	A	A	ALTO

Una vez obtenidos los resultados se muestra que los niveles de riesgos presentados son medios y altos por lo que las amenazas lograrían materializarse y causar daño a los activos informáticos. Se detalla a continuación las amenazas con un alto índice de riesgo:

- ✓ Falla de equipo de climatización
- ✓ Malware
- ✓ Fuga de información
- ✓ Desconexión física y lógica
- ✓ Acceso no autorizado

Es importante indicar que las amenazas que pueden influir sobre un activo y se pueda materializar, PILAR las puede identificar, haciendo clic sobre opción amenazas y escogiendo identificación, nos dirigimos a la capa donde están agrupados los activos y sobre la carpeta amarilla dando clic izquierdose muestran las posibles amenazas sobre él grupo de activos Equipos [HW] tal como se presenta en la siguiente figura 27. En la biblioteca estándar que posee PILAR, están las amenazas elegidas por PILAR para los activos informáticos.

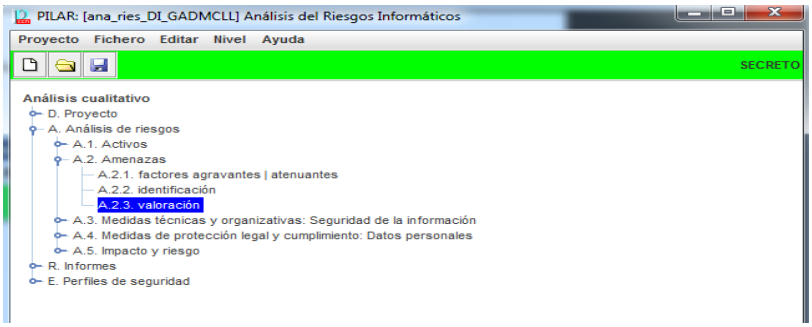


Figura 27. Opción “identificación”

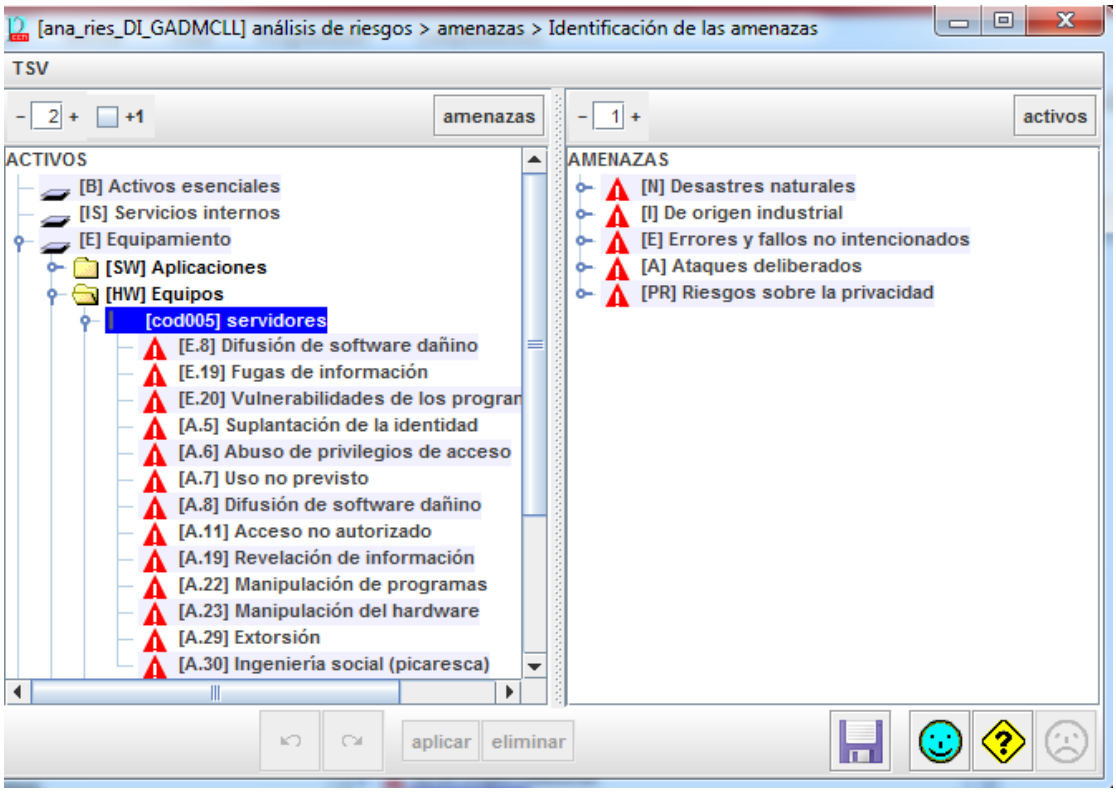
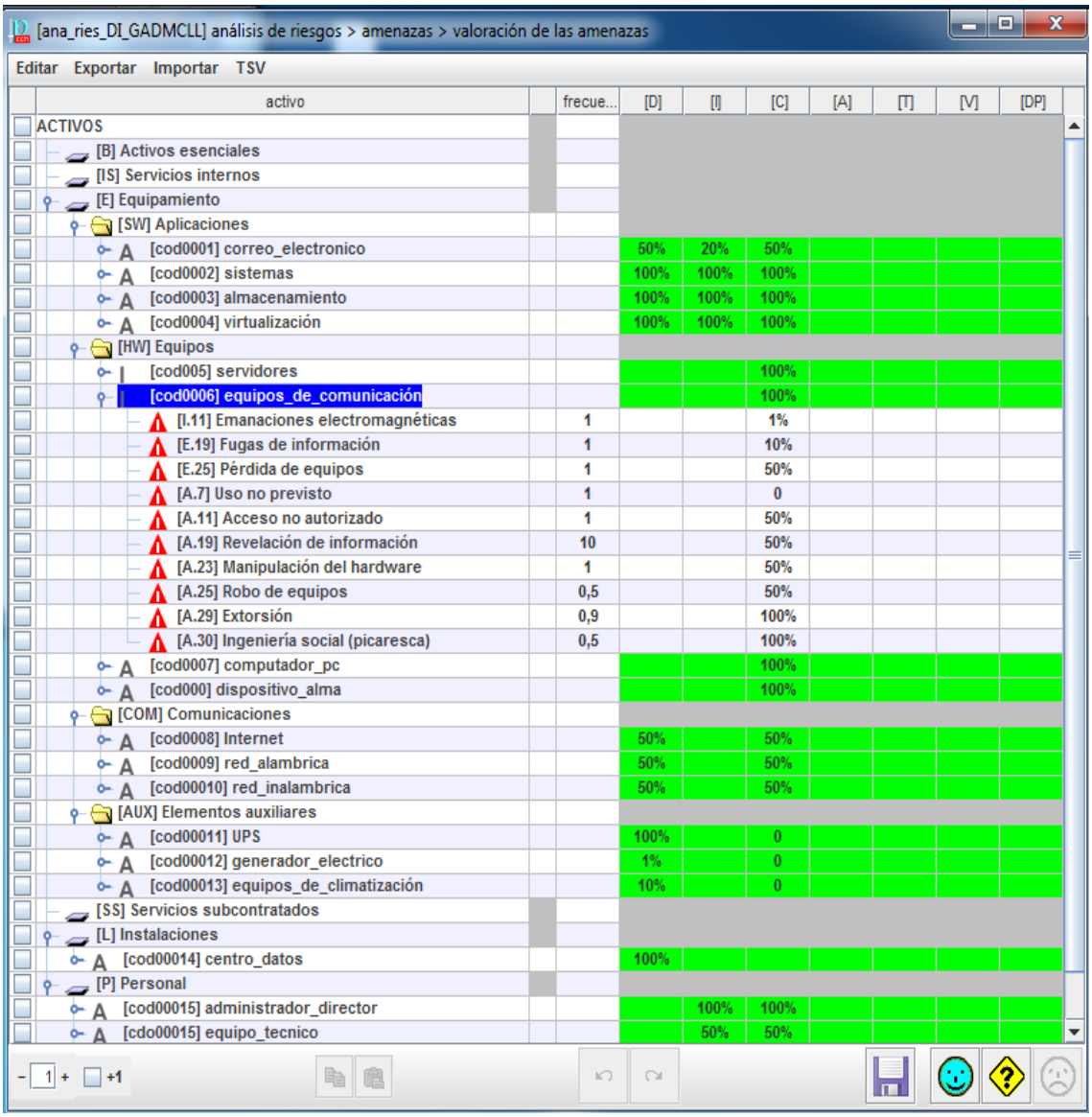


Figura 28. Identificación de amenazas

4.3.3 VALORIZACIÓN DE AMENZAS EN PILAR

La herramienta PILAR nos da la opción de obtener la valoración de las amenazas de forma automática considerando la frecuencia de materialización y el impacto que tendrían en la organización expresada en porcentaje, tal como se muestra en la siguiente Figura 29.



activo	frecue...	[D]	[I]	[C]	[A]	[T]	[V]	[DP]
ACTIVOS								
[B] Activos esenciales								
[IS] Servicios internos								
[E] Equipamiento								
[SW] Aplicaciones								
[cod0001] correo_electronico		50%	20%	50%				
[cod0002] sistemas		100%	100%	100%				
[cod0003] almacenamiento		100%	100%	100%				
[cod0004] virtualización		100%	100%	100%				
[HW] Equipos								
[cod005] servidores				100%				
[cod0006] equipos_de_comunicación				100%				
[I.11] Emanaciones electromagnéticas	1			1%				
[E.19] Fugas de información	1			10%				
[E.25] Pérdida de equipos	1			50%				
[A.7] Uso no previsto	1			0				
[A.11] Acceso no autorizado	1			50%				
[A.19] Revelación de información	10			50%				
[A.23] Manipulación del hardware	1			50%				
[A.25] Robo de equipos	0,5			50%				
[A.29] Extorsión	0,9			100%				
[A.30] Ingeniería social (picaresca)	0,5			100%				
[cod0007] computador_pc				100%				
[cod000] dispositivo_alma				100%				
[COM] Comunicaciones								
[cod0008] Internet		50%		50%				
[cod0009] red_alambrica		50%		50%				
[cod00010] red_inalambrica		50%		50%				
[AUX] Elementos auxiliares								
[cod00011] UPS		100%		0				
[cod00012] generador_electrico		1%		0				
[cod00013] equipos_de_climatización		10%		0				
[SS] Servicios subcontratados								
[L] Instalaciones								
[cod00014] centro_datos		100%						
[P] Personal								
[cod00015] administrador_director			100%	100%				
[cdo00015] equipo_tecnico			50%	50%				

Figura 29. Valoración de amenazas de grupo de activos

4.4 SALVAGUARDAS

"Es una medida de emergencia para mitigar las posibles amenazas a un activo informático". Se inicia escogiendo la opción "identificación" donde se mostrará las salvaguardas que PILAR brinda.

4.4.1 Identificación

Luego de elegir la opción “Identificar” de salvaguardas se mostrarán todas las salvaguardas existentes en la biblioteca estándar de PILAR, ver en Tabla 30.

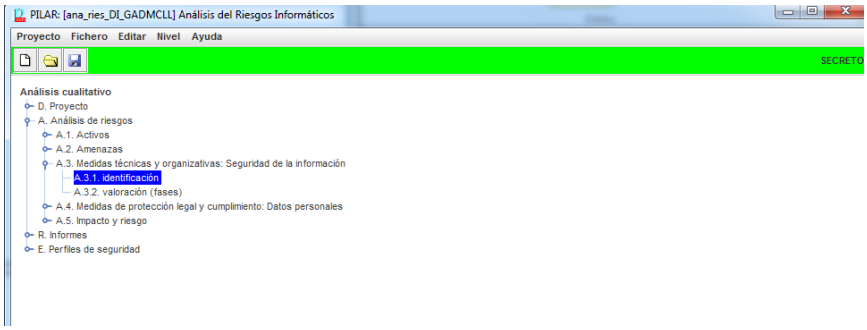


Figura 30. Opción “Valoración” de Salvaguardas

Se podrá mitigar el impacto y mitigar el riesgo mediante la utilización de la opción “salvaguardas”, tomando como referencia la siguiente tabla 21 de Nivel de madurez de las salvaguardas.

Tabla 21
Nivel de madurez de las salvaguardas

EFICACIA	NIVEL	SIGNIFICADO
	n.a.	No es aplicable
0%	L0	Inexistente
10%	L1	Inicial / ad hoc
50%	L2	Reproducible, pero intuitivo
90%	L3	Proceso definido
95%	L4	Gestionado y medible
00%	L5	Optimizado

4.4.2 EVALUACION DE SALVAGUARDASEN PILAR

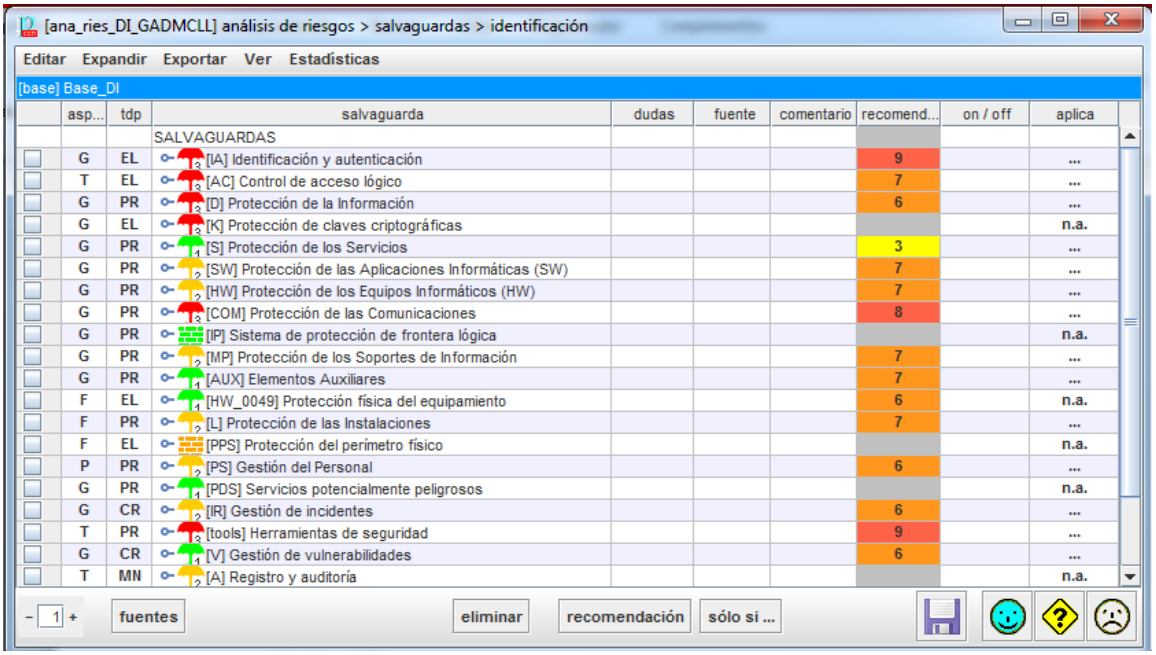


Figura 31. Salvaguarda.

Podemos visualizar en la Figura 31., en la ventana de identificación de salvaguardas que está compuesta por 10 columnas. En la primera columna, trabaja en combinación con el menú Ver >> Riesgos. En la segunda columna, tratan bajo 4 aspectos:

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

En la tercera columna se encuentra el Tipo de protección (tdp) que muestra los diferentes tipos de protección, los cuales son:

- ✓ PR–prevención
- ✓ DR–disuasión
- ✓ EL–eliminación
- ✓ IM–minimización del impacto
- ✓ CR–corrección
- ✓ RC–recuperación
- ✓ AD– administrativa
- ✓ AW–concienciación
- ✓ DC–detección y
- ✓ MN–monitorización

En la cuarta columna Salvaguarda, se muestra el peso de relativo de las salvaguardas. En la quinta columna dudas, la marca se usa, típicamente, para recordar que hay asuntos pendientes de una respuesta.

En la sexta columna fuente, asocia fuentes de información a la salvaguarda (la marcada y sus descendientes).

En la séptima columna comentario, asocia un comentario a la salvaguarda.

En la octava columna recomendación, indica la valoración estimada de la salvaguarda teniendo en cuenta el tipo de activos, el rango va desde el 0 al 10.

En la novena columna On/Off, se usa para descartar de forma temporal algunas salvaguardas. Funciona como [10] pero no es una declaración formal de no-aplicabilidad.

En décima columna Aplicable.- marca la salvaguarda como aplicable, para todas las fases, salvo que se marquen como “n.a.”.

Tabla 22
Barra inferior de herramientas

− 1 +	Controla el despliegue del árbol de salvaguardas.
fuentes	Seleccione una o más fuentes de información. PILAR seleccionará todas las salvaguardas a las que está asociada.
eliminar	Elimina todas las marcas en [9] y [10].
recomendación	Haga clic y PILAR marcará como no aplicables todas las salvaguardas que PILAR no sabe cómo aplicar; es decir, las que tienen una recomendación gris.
sólo si …	PILAR retiene solamente las salvaguardas que se necesitan para cumplir con uno o más perfiles de seguridad.
	Guarda el proyecto en su fichero o en su base de datos.

Fuente: (file:///C:/Program%20Files/PILAR_7.1/help_es/cia/WebHelp/index.html#!1094)

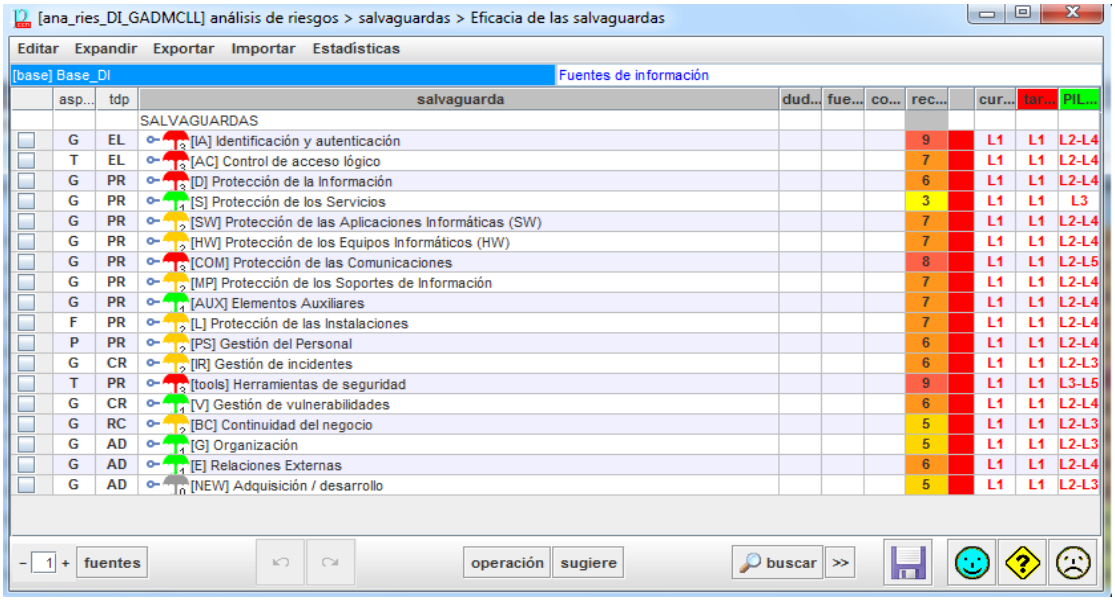


Figura 32. Valoración de Salvaguardas

En la figura 32., se puede mostrar el nivel de madurez que se ingresó en la columna current que es L1 que significa fase inicial ya que es la primera vez que se realiza un análisis de riesgo al departamento informático del GADMCLL, también se muestra la columna PILAR el nivel de madurez al que se quiere llegar como objetivo.

4.5 ESTADO DEL RIESGO

4.5.1 Impacto

El impacto es un indicador del estado de seguridad que mide el daño que causa una amenaza cuando ésta se materializa. PILAR maneja dos criterios que son el impacto acumulado y el impacto repercutido.

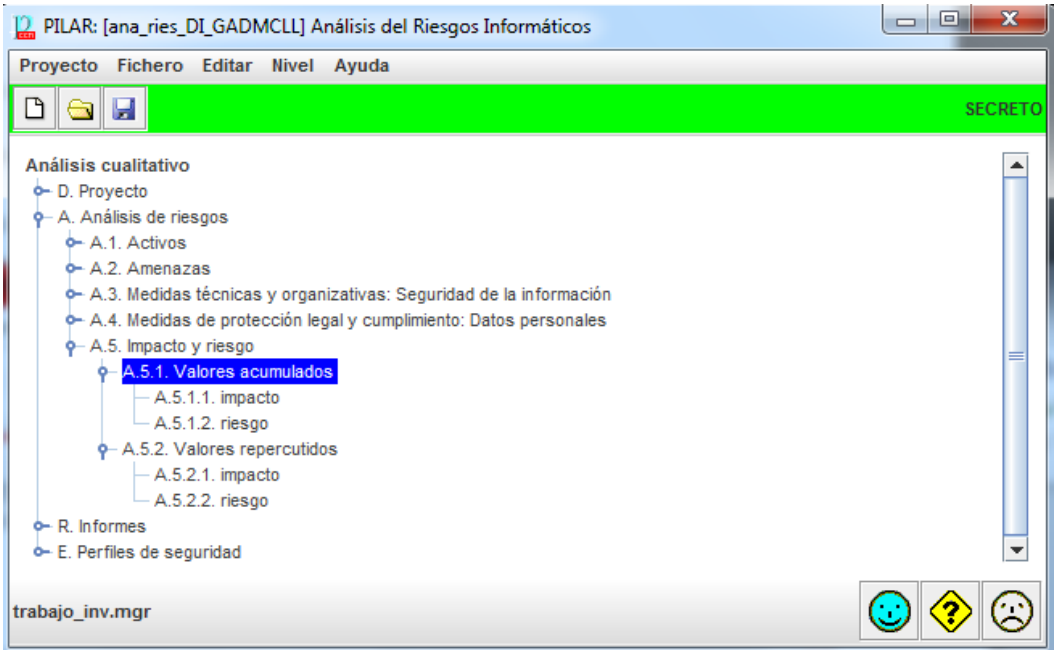


Figura 33. Opción “Impacto acumulado”

4.5.2 Impacto Acumulado

En esta opción se puede visualizar el valor del impacto acumulado, el cual se calcula mediante la siguiente fórmula:

$$IA = VAA * DA$$

Formula 2

“Dónde: IA es el impacto acumulado, VAA es el valor acumulado del activo y DA es la degradación que le provocaría la amenaza; consecuentemente el impacto se mide en la misma unidad que el valor del activo; debido a que el análisis escogido para el presente proyecto es cualitativo el valor e impacto tendrá valores de 0 a 10”.

Luego de escoger la opción impacto acumulado, se muestra una pestaña porfase que presenta los diferentes valores por cada dimensión de seguridad basándose en la siguiente escala de colores.

.

10]: Crítico

· [9]: Muy alto

· [8]: Muy alto

· [7]: Alto

· [6]: Alto

· [5]: Medio

· [4]: Medio

· [3]: Bajo

· [2]: Bajo

· [1]: Despreciable

[0]: Despreciable

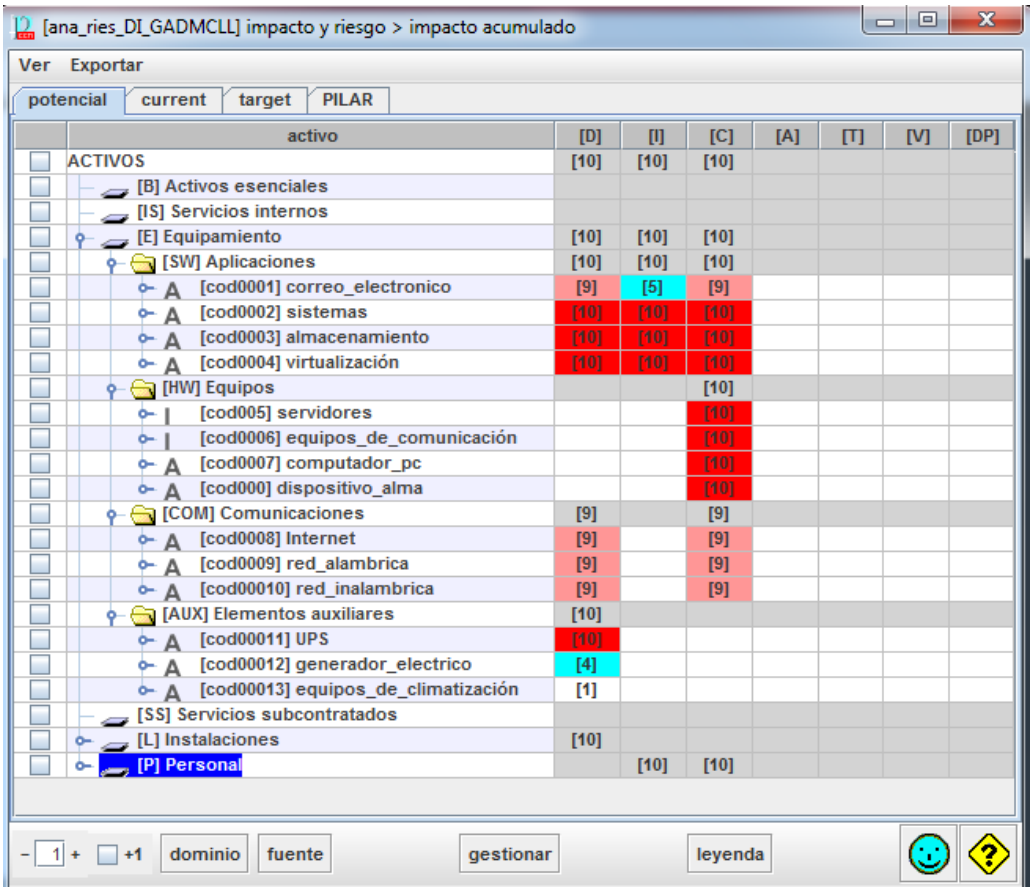


Figura 34. Impacto acumulado potencial

Se muestran en la Figura 34, las diferentes pestañas:

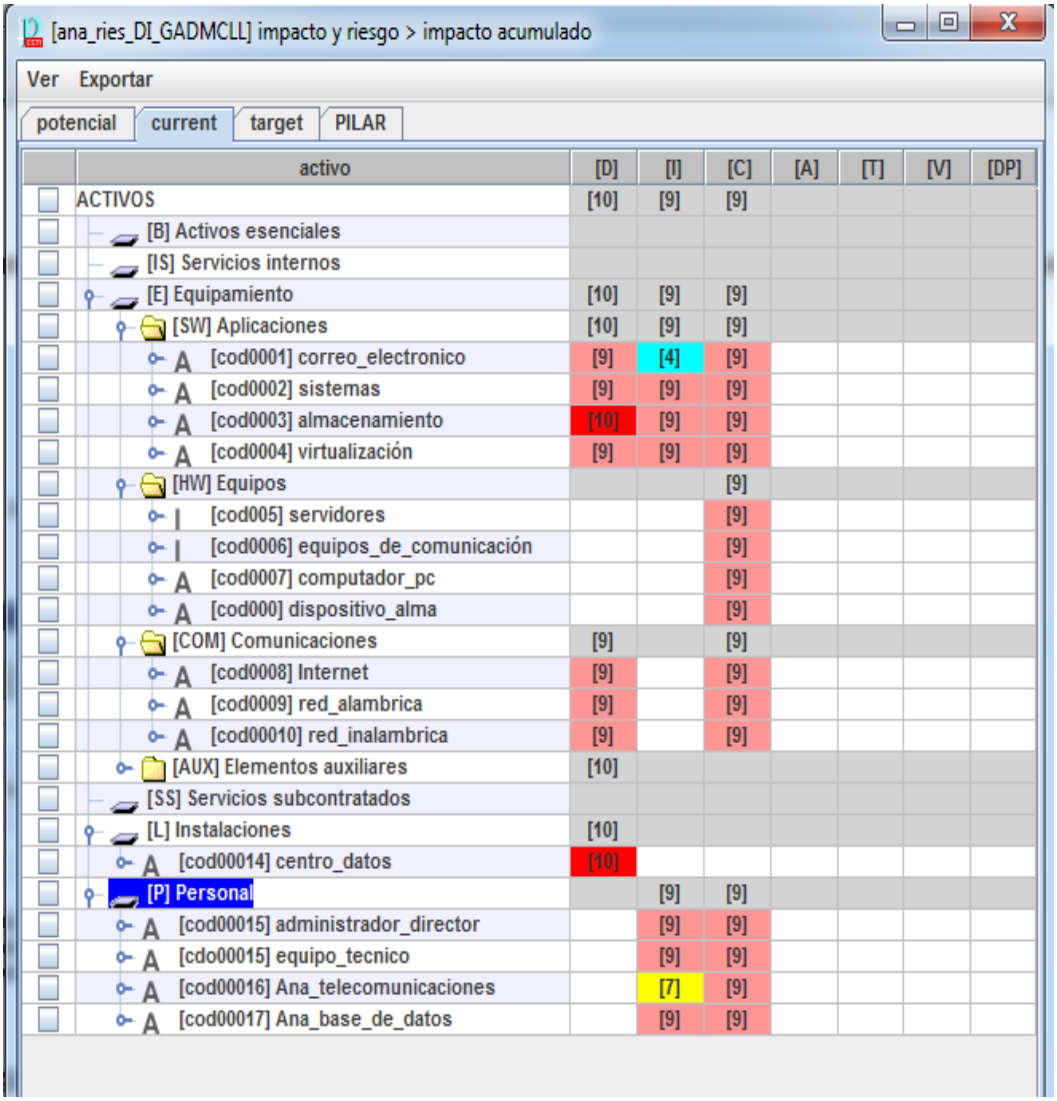
Potencial: indica los valores acumulados sin salvaguarda alguna.

Current: indica los valores acumulados aplicadas las salvaguardas, por lo que los valores del impacto acumulado disminuyen.

PILAR: indica los valores acumulados a la cual debe llegar como objetivo.

Estas diferentes pestañas muestran el valor color del impacto acumulado potencial de los activos informáticos y presenta un resultado estimado de mitigación es decir a lo que

vamos a llegar si se realiza las debidas correcciones. Los resultados de impacto son muy altos.



activo	[D]	[I]	[C]	[A]	[T]	[V]	[DP]
ACTIVOS	[10]	[9]	[9]				
[B] Activos esenciales							
[IS] Servicios internos							
[E] Equipamiento	[10]	[9]	[9]				
[SW] Aplicaciones	[10]	[9]	[9]				
[cod0001] correo_electronico	[9]	[4]	[9]				
[cod0002] sistemas	[9]	[9]	[9]				
[cod0003] almacenamiento	[10]	[9]	[9]				
[cod0004] virtualización	[9]	[9]	[9]				
[HW] Equipos			[9]				
[cod005] servidores			[9]				
[cod0006] equipos_de_comunicación			[9]				
[cod0007] computador_pc			[9]				
[cod000] dispositivo_alma			[9]				
[COM] Comunicaciones	[9]		[9]				
[cod0008] Internet	[9]		[9]				
[cod0009] red_alambrica	[9]		[9]				
[cod00010] red_inalambrica	[9]		[9]				
[AUX] Elementos auxiliares	[10]						
[SS] Servicios subcontratados							
[L] Instalaciones	[10]						
[cod00014] centro_datos	[10]						
[P] Personal		[9]	[9]				
[cod00015] administrador_director		[9]	[9]				
[cdo00015] equipo_tecnico		[9]	[9]				
[cod00016] Ana_telecomunicaciones		[7]	[9]				
[cod00017] Ana_base_de_datos		[9]	[9]				

Figura 35. Impacto acumulado current

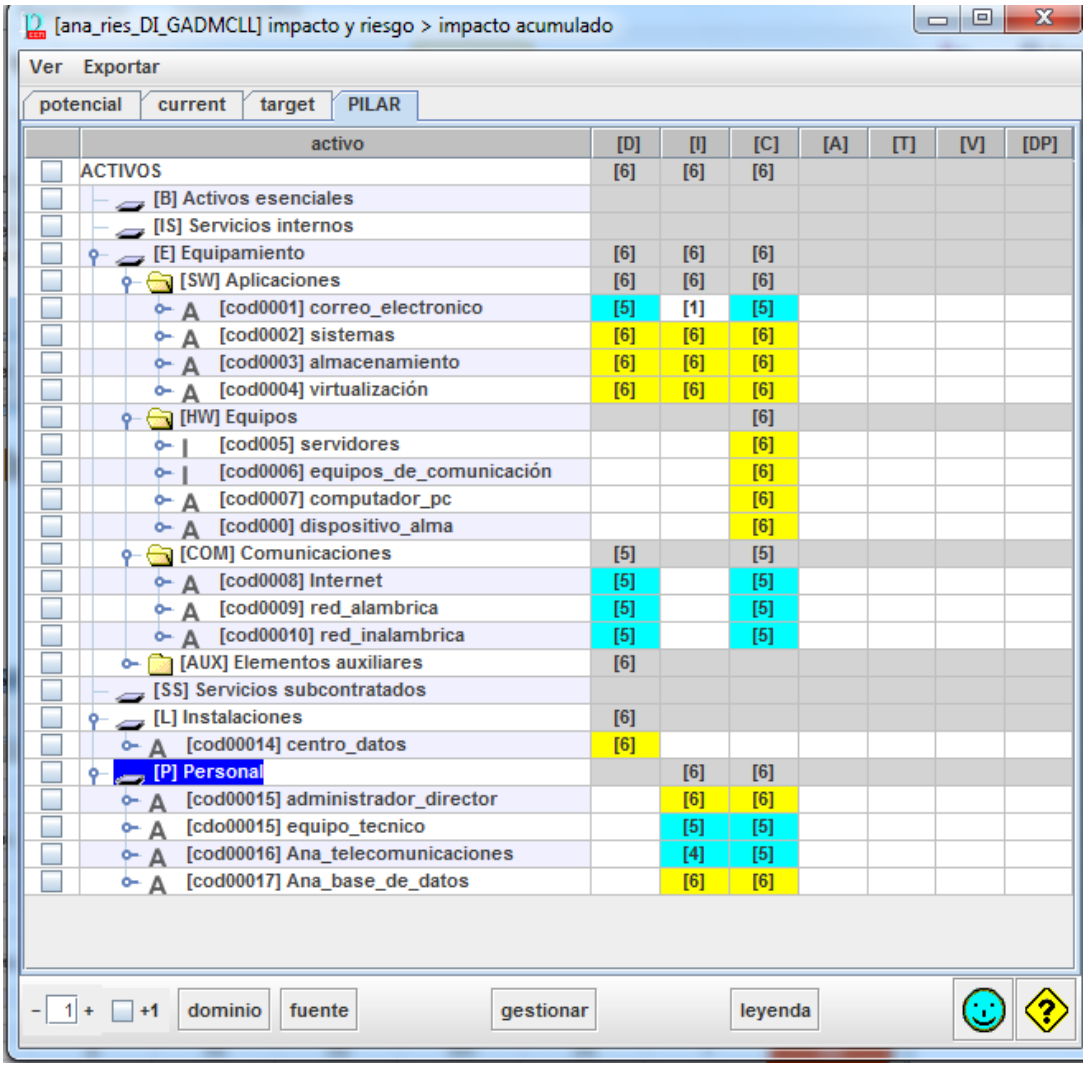


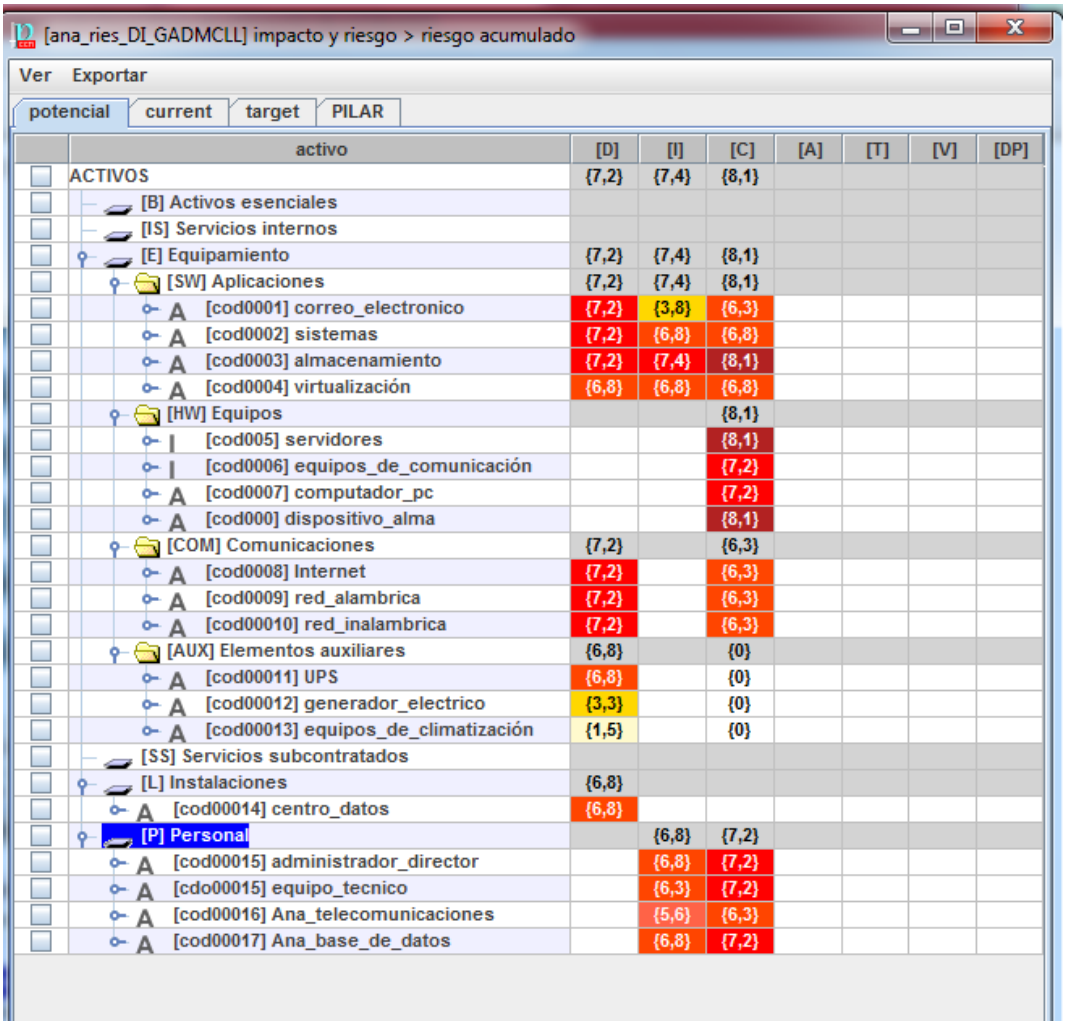
Figura 36. Impacto acumulado PILAR

Se muestran en la Figura 36, los resultados y se puede evidenciar la importancia de aplicar las salvaguardas para disminuir los niveles de impacto, actualmente están en nivel alto y en el nivel PILAR se muestran los resultados a obtener “bajo impacto”.

4.5.3Riesgo Acumulado

PILAR permite medir los niveles de criticidad de los riesgos a los cuales se encuentran expuestos lo activos.

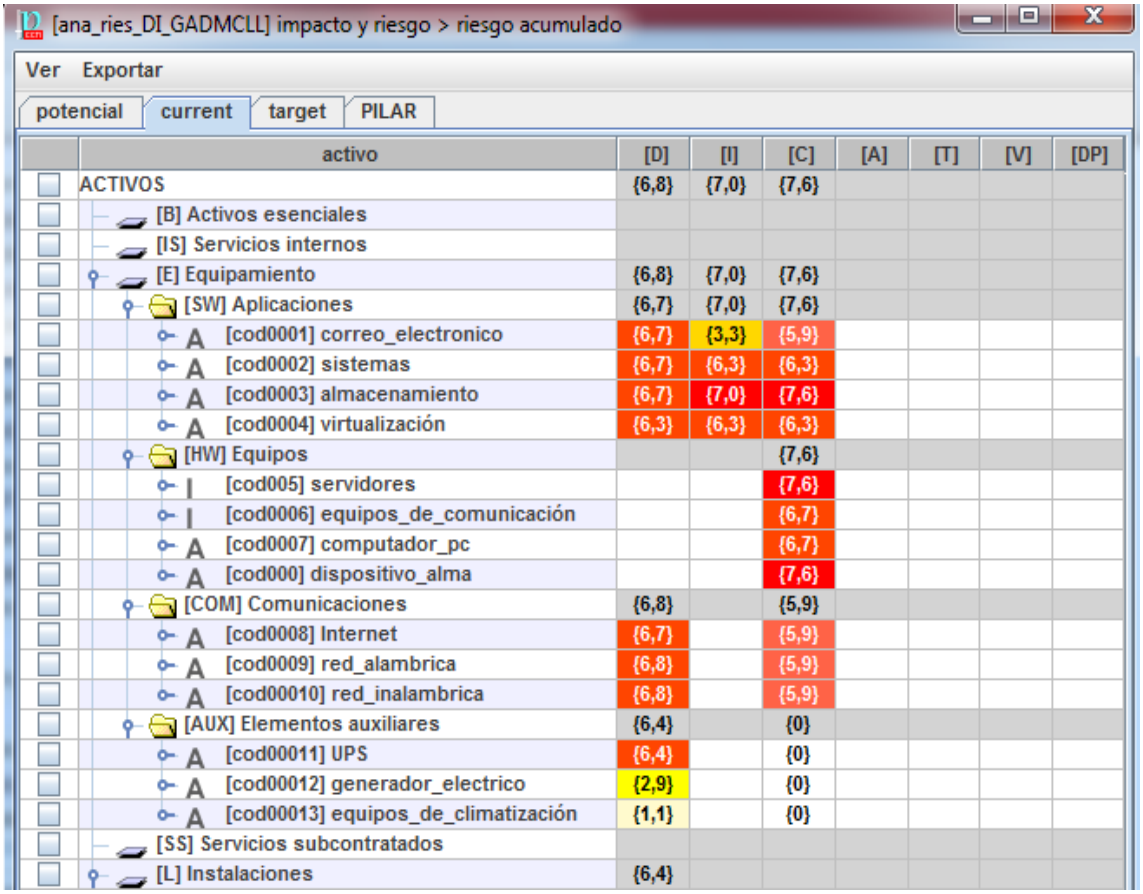
En la figura 37 refleja el nivel del riesgo potencial, el cual es muy alto y requiere de las salvaguardas.



activo	[D]	[I]	[C]	[A]	[T]	[V]	[DP]
ACTIVOS	{7,2}	{7,4}	{8,1}				
[B] Activos esenciales							
[IS] Servicios internos							
[E] Equipamiento	{7,2}	{7,4}	{8,1}				
[SW] Aplicaciones	{7,2}	{7,4}	{8,1}				
[cod0001] correo_electronico	{7,2}	{3,8}	{6,3}				
[cod0002] sistemas	{7,2}	{6,8}	{6,8}				
[cod0003] almacenamiento	{7,2}	{7,4}	{8,1}				
[cod0004] virtualización	{6,8}	{6,8}	{6,8}				
[HW] Equipos			{8,1}				
[cod005] servidores			{8,1}				
[cod0006] equipos_de_comunicación			{7,2}				
[cod0007] computador_pc			{7,2}				
[cod000] dispositivo_alma			{8,1}				
[COM] Comunicaciones	{7,2}		{6,3}				
[cod0008] Internet	{7,2}		{6,3}				
[cod0009] red_alambrica	{7,2}		{6,3}				
[cod00010] red_inalambrica	{7,2}		{6,3}				
[AUX] Elementos auxiliares	{6,8}		{0}				
[cod00011] UPS	{6,8}		{0}				
[cod00012] generador_electrico	{3,3}		{0}				
[cod00013] equipos_de_climatización	{1,5}		{0}				
[SS] Servicios subcontratados							
[L] Instalaciones	{6,8}						
[cod00014] centro_datos	{6,8}						
[P] Personal		{6,8}	{7,2}				
[cod00015] administrador_director		{6,8}	{7,2}				
[cdo00015] equipo_tecnico		{6,3}	{7,2}				
[cod00016] Ana_telecomunicaciones		{5,6}	{6,3}				
[cod00017] Ana_base_de_datos		{6,8}	{7,2}				

Figura 37. Riesgo Acumulado potencial

En la figura 38., refleja el nivel del riesgo actual, el cual es muy alto de tal manera que se debe tomar medidas de seguridad para reducir el riego.



activo	[D]	[I]	[C]	[A]	[T]	[V]	[DP]
ACTIVOS	{6,8}	{7,0}	{7,6}				
[B] Activos esenciales							
[IS] Servicios internos							
[E] Equipamiento	{6,8}	{7,0}	{7,6}				
[SW] Aplicaciones	{6,7}	{7,0}	{7,6}				
[cod0001] correo_electronico	{6,7}	{3,3}	{5,9}				
[cod0002] sistemas	{6,7}	{6,3}	{6,3}				
[cod0003] almacenamiento	{6,7}	{7,0}	{7,6}				
[cod0004] virtualización	{6,3}	{6,3}	{6,3}				
[HW] Equipos			{7,6}				
[cod005] servidores			{7,6}				
[cod0006] equipos_de_comunicación			{6,7}				
[cod0007] computador_pc			{6,7}				
[cod000] dispositivo_alma			{7,6}				
[COM] Comunicaciones	{6,8}		{5,9}				
[cod0008] Internet	{6,7}		{5,9}				
[cod0009] red_alambrica	{6,8}		{5,9}				
[cod00010] red_inalambrica	{6,8}		{5,9}				
[AUX] Elementos auxiliares	{6,4}		{0}				
[cod00011] UPS	{6,4}		{0}				
[cod00012] generador_electrico	{2,9}		{0}				
[cod00013] equipos_de_climatización	{1,1}		{0}				
[SS] Servicios subcontratados							
[L] Instalaciones	{6,4}						

Figura 38. Riesgo Acumulado current

En la figura 39 se obtiene el riesgo acumulado PILAR que debe seguir en evaluación para tratar de disminuirlo o si es posible eliminarlo.

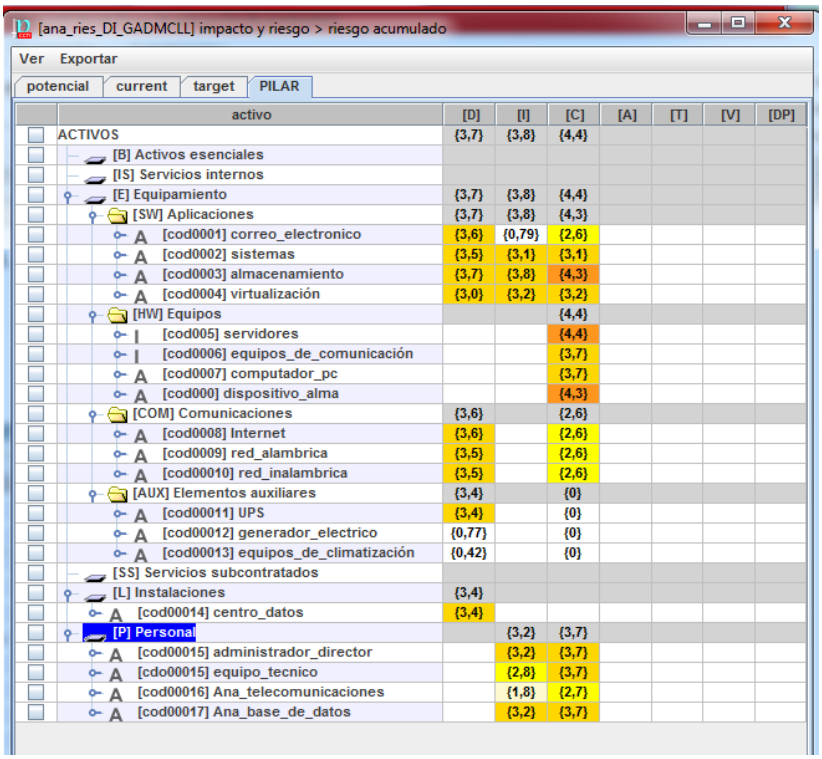


Figura 39. Riesgo Acumulado PILAR

4.5.4 Impacto Repercutido

Se visualiza el valor del impacto repercutido, y se calcula mediante la siguiente fórmula:

$$IR = VA * DA * GD$$

Formula 3

Dónde: IR es el impacto repercutido, VA es el valor propio del activo, DA es la degradación que le provocaría la amenaza y GD es el grado de dependencia Figura 40.

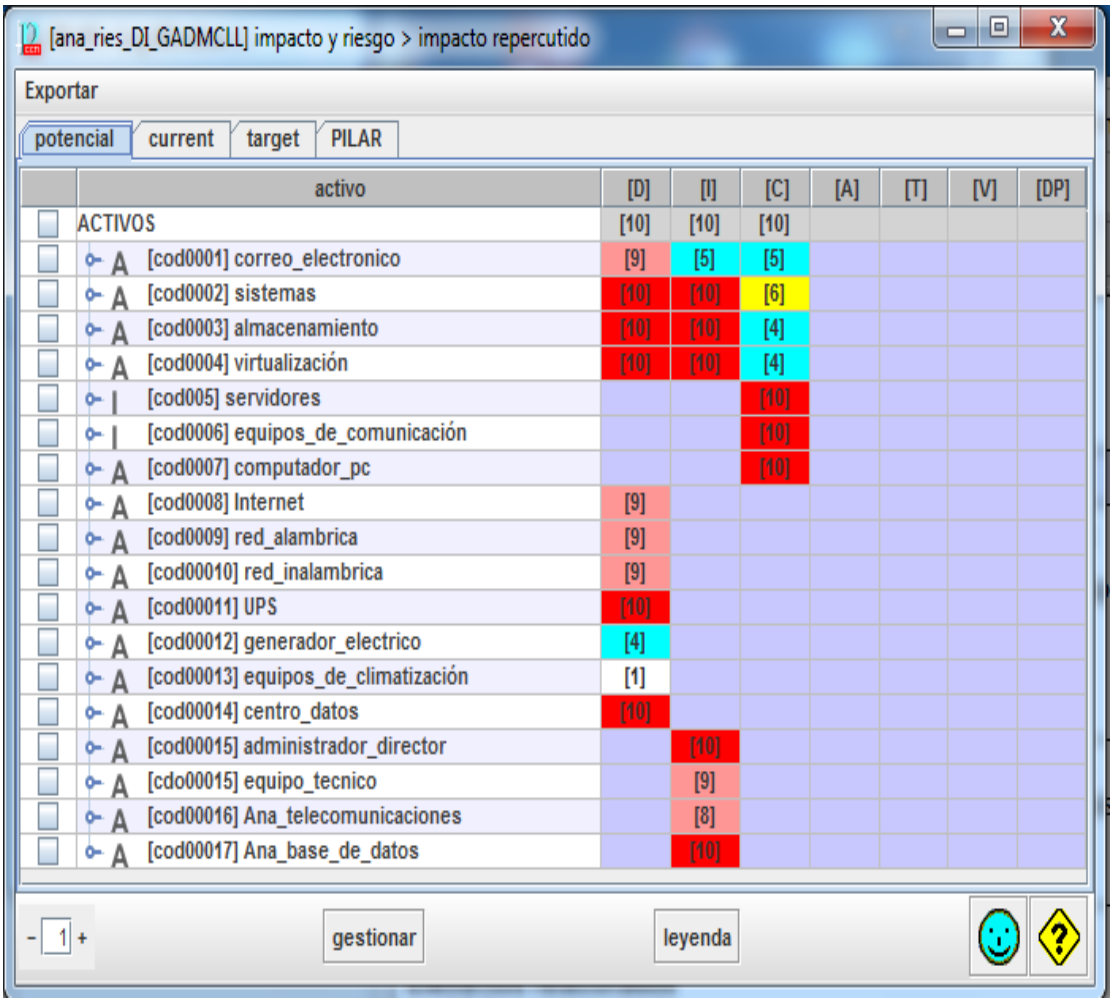
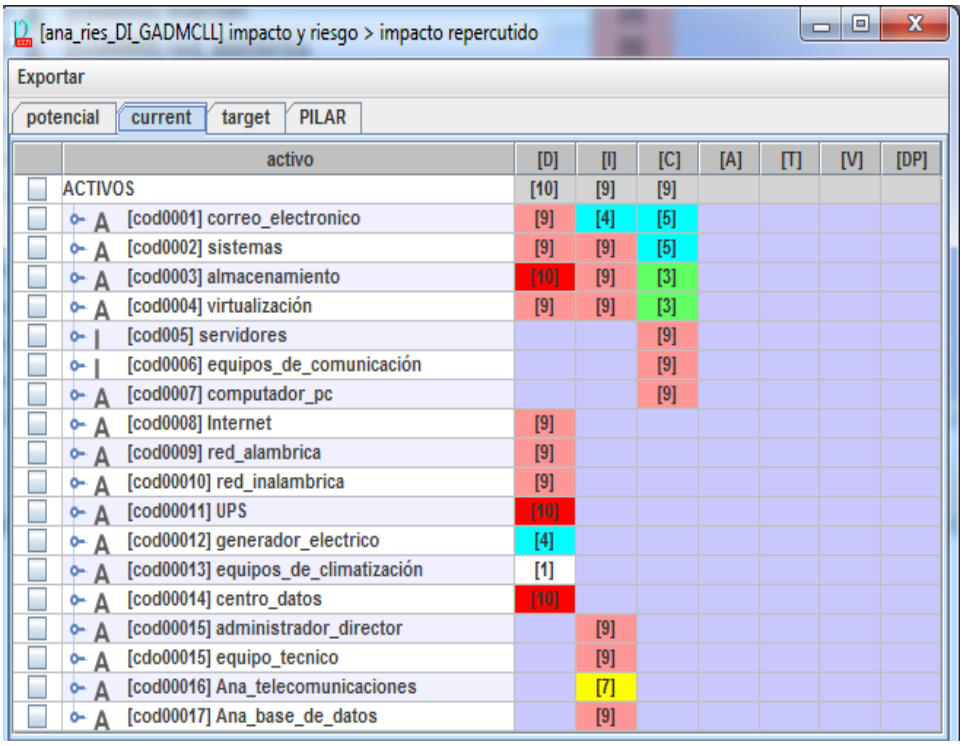


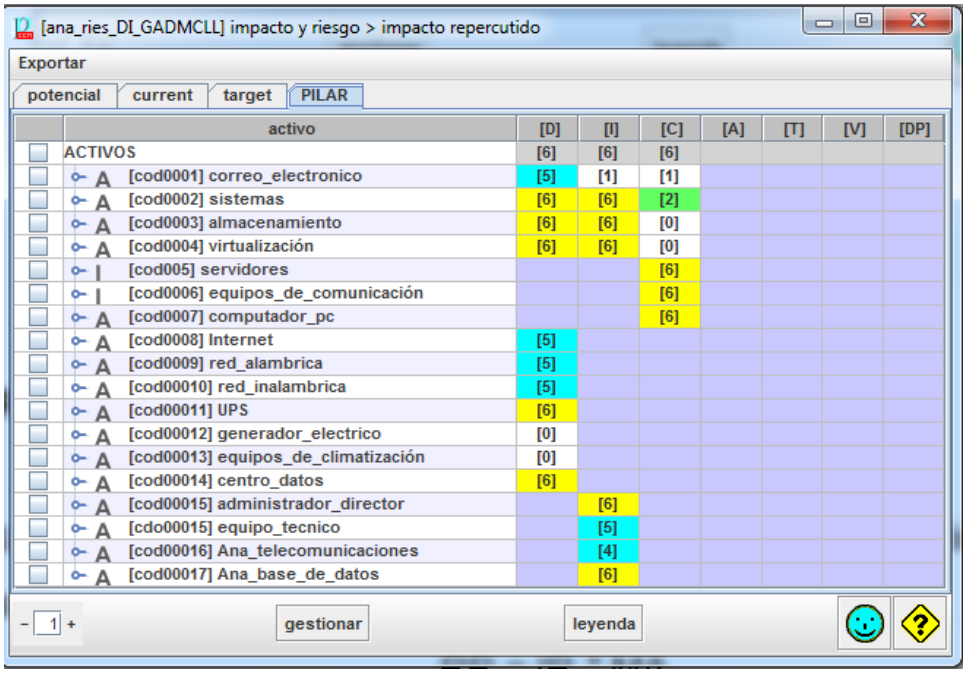
Figura 40. Impacto Repercutido potencial

Se muestra un resultado crítico para los activos en el impacto repercutido potencial, lo cual es muy alto.



activo	[D]	[I]	[C]	[A]	[T]	[V]	[DP]
ACTIVOS	[10]	[9]	[9]				
[cod0001] correo_electronico	[9]	[4]	[5]				
[cod0002] sistemas	[9]	[9]	[5]				
[cod0003] almacenamiento	[10]	[9]	[3]				
[cod0004] virtualización	[9]	[9]	[3]				
[cod005] servidores			[9]				
[cod0006] equipos_de_comunicación			[9]				
[cod0007] computador_pc			[9]				
[cod0008] Internet	[9]						
[cod0009] red_alambrica	[9]						
[cod00010] red_inalambrica	[9]						
[cod00011] UPS	[10]						
[cod00012] generador_electrico	[4]						
[cod00013] equipos_de_climatización	[1]						
[cod00014] centro_datos	[10]						
[cod00015] administrador_director		[9]					
[cdo00015] equipo_tecnico		[9]					
[cod00016] Ana_telecomunicaciones		[7]					
[cod00017] Ana_base_de_datos		[9]					

Figura 41. Impacto Repercutido current



activo	[D]	[I]	[C]	[A]	[T]	[V]	[DP]
ACTIVOS	[6]	[6]	[6]				
[cod0001] correo_electronico	[5]	[1]	[1]				
[cod0002] sistemas	[6]	[6]	[2]				
[cod0003] almacenamiento	[6]	[6]	[0]				
[cod0004] virtualización	[6]	[6]	[0]				
[cod005] servidores			[6]				
[cod0006] equipos_de_comunicación			[6]				
[cod0007] computador_pc			[6]				
[cod0008] Internet	[5]						
[cod0009] red_alambrica	[5]						
[cod00010] red_inalambrica	[5]						
[cod00011] UPS	[6]						
[cod00012] generador_electrico	[0]						
[cod00013] equipos_de_climatización	[0]						
[cod00014] centro_datos	[6]						
[cod00015] administrador_director		[6]					
[cdo00015] equipo_tecnico		[5]					
[cod00016] Ana_telecomunicaciones		[4]					
[cod00017] Ana_base_de_datos		[6]					

Figura 42. Impacto Repercutido PILAR

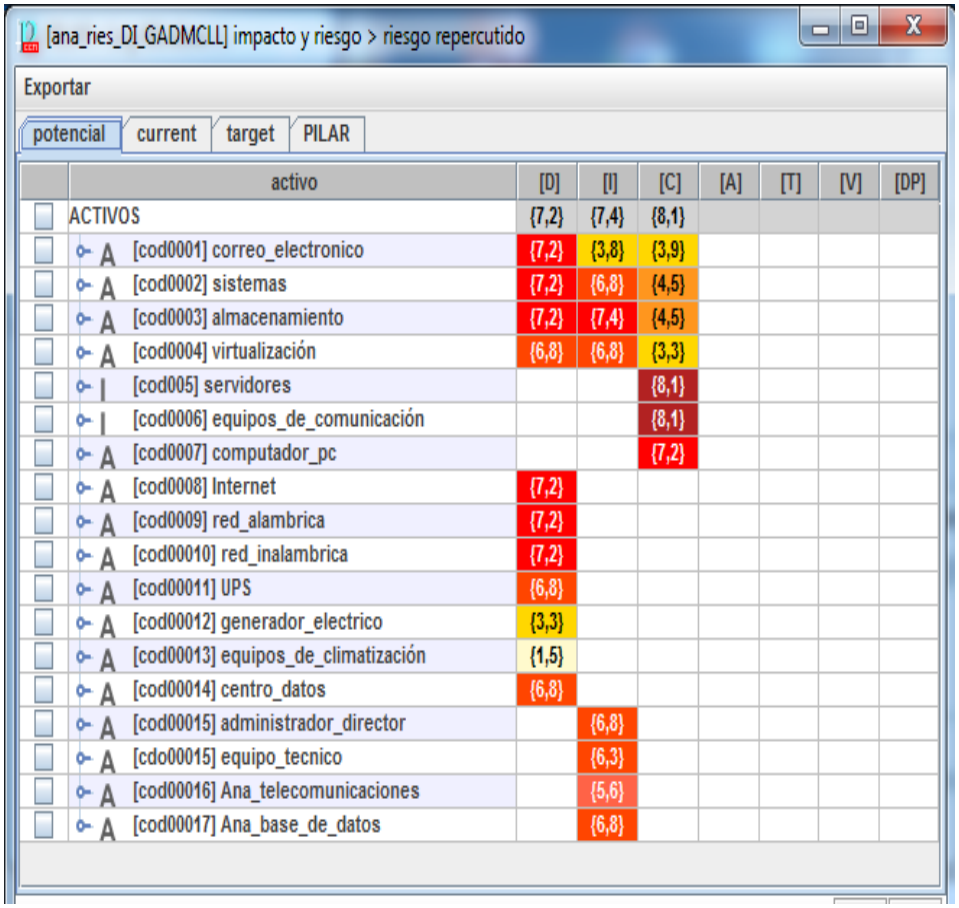
4.5.5 Riesgo Repercutido

Se puede visualizar el valor del riesgo repercutido, y se calcula mediante la siguiente fórmula:

$$RP = IR * MA$$

Formula 5

Dónde: RP es el riesgo repercutido, IR es el impacto repercutido y MA es la materialización de la amenaza.



activo	[D]	[I]	[C]	[A]	[T]	[V]	[DP]
ACTIVOS	{7,2}	{7,4}	{8,1}				
[cod0001] correo_electronico	{7,2}	{3,8}	{3,9}				
[cod0002] sistemas	{7,2}	{6,8}	{4,5}				
[cod0003] almacenamiento	{7,2}	{7,4}	{4,5}				
[cod0004] virtualización	{6,8}	{6,8}	{3,3}				
[cod005] servidores			{8,1}				
[cod0006] equipos_de_comunicación			{8,1}				
[cod0007] computador_pc			{7,2}				
[cod0008] Internet	{7,2}						
[cod0009] red_alambrica	{7,2}						
[cod00010] red_inalambrica	{7,2}						
[cod00011] UPS	{6,8}						
[cod00012] generador_electrico	{3,3}						
[cod00013] equipos_de_climatización	{1,5}						
[cod00014] centro_datos	{6,8}						
[cod00015] administrador_director		{6,8}					
[cdo00015] equipo_tecnico		{6,3}					
[cod00016] Ana_telecomunicaciones		{5,6}					
[cod00017] Ana_base_de_datos		{6,8}					

Figura 43. Riesgo Repercutido potencial

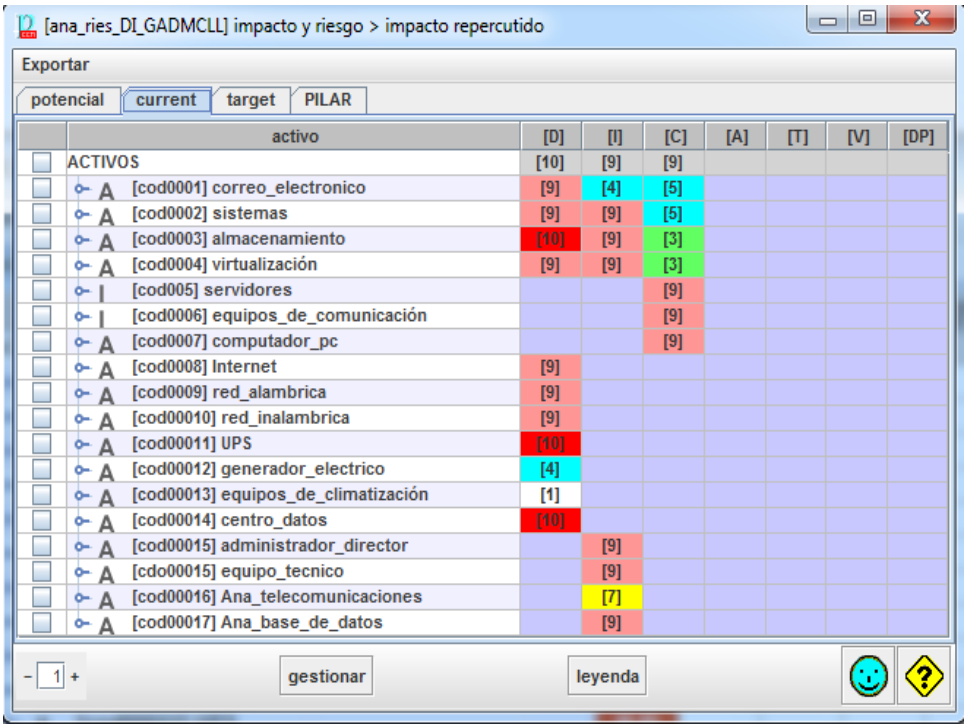


Figura 44. Riesgo Repercutido current

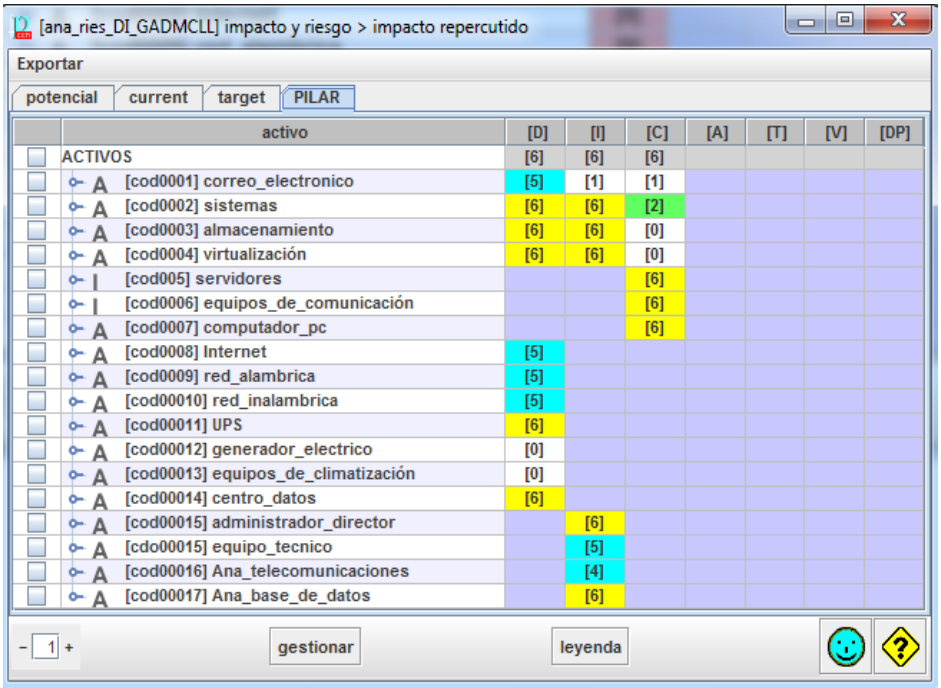


Figura 45. Riesgo Repercutido PILAR

4.6 INFORMES

Se presentan los gráficos resultantes que se han obtenido de las evaluaciones realizadas en PILAR, mostrando los parámetros de seguridad que afectan a los activos informáticos.

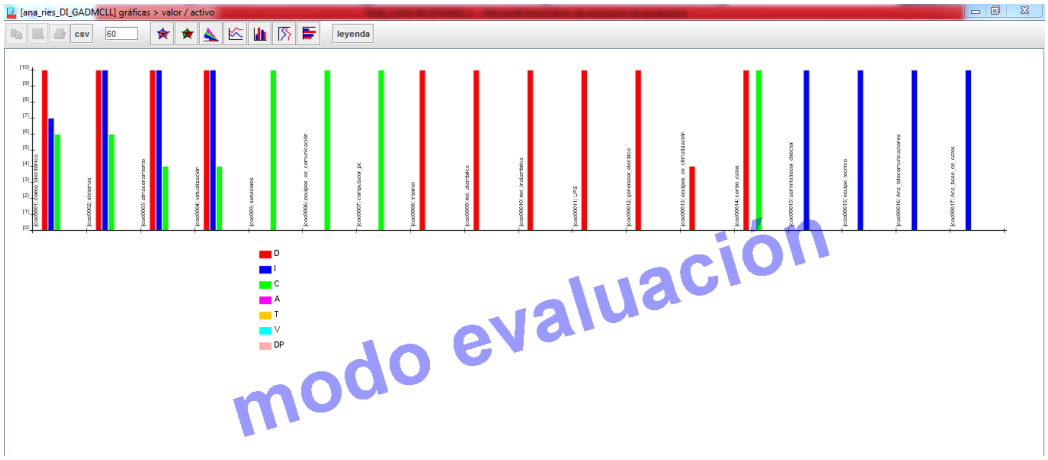


Figura 46. Valor de activo

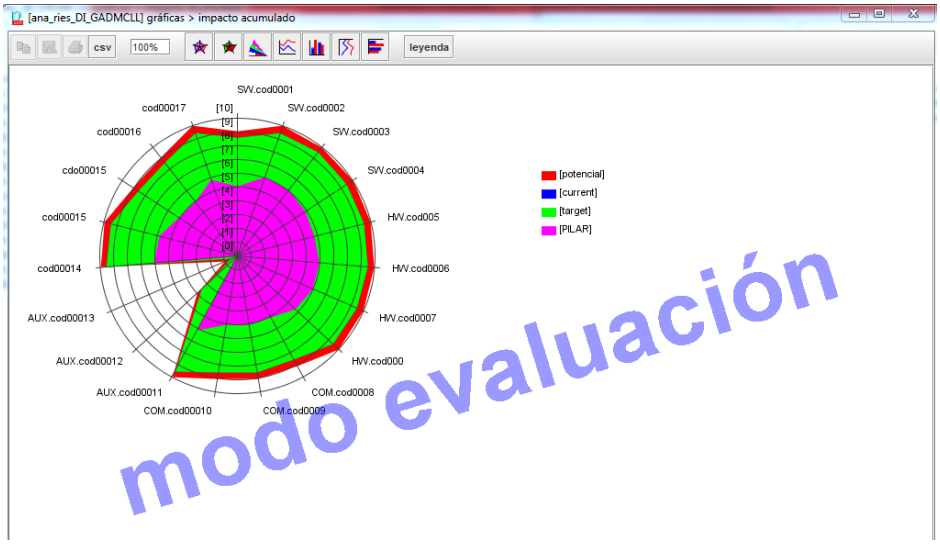


Figura 47. Impacto acumulado

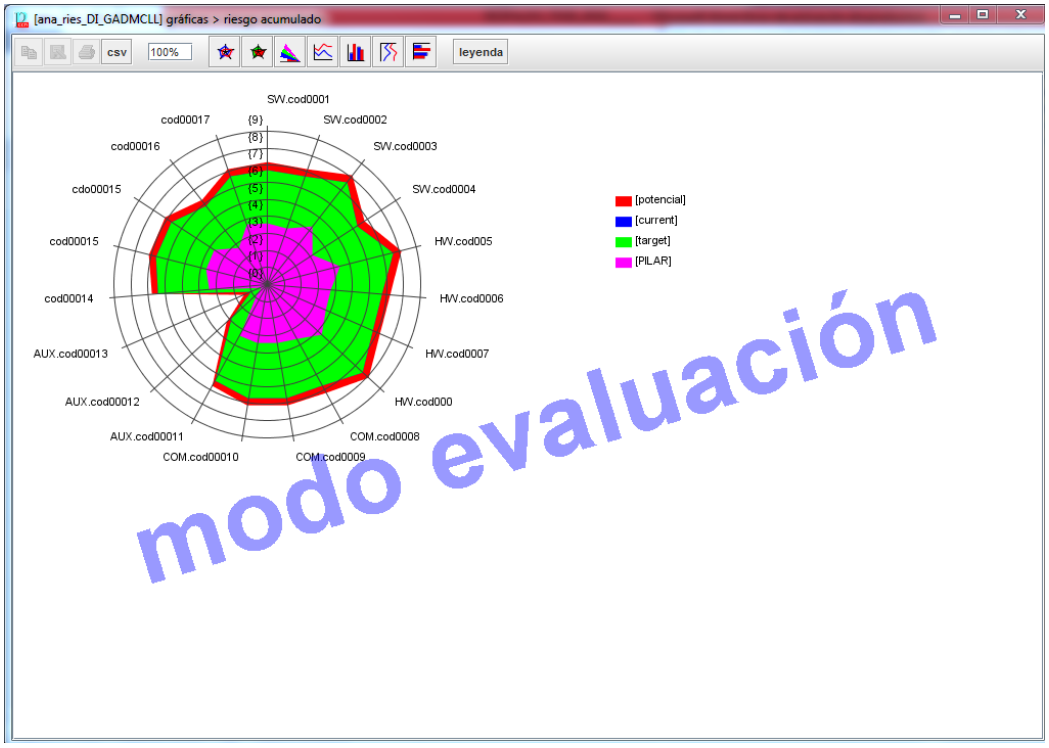


Figura 48. Riesgo acumulado

4.7 LINEAMIENTOS DE SEGURIDAD

Una vez realizada la valoración del riesgo acumulado y repercutido sesugiere lineamientos de seguridad con la finalidad que el departamento informático del GADMCLL conozca las posibles soluciones y las considere una opción para proteger y evitar que ciertas amenazas se materialicen y causen daño a los activosinformáticos críticos, cabe indicar que dependerá de la persona encarda del departamento informático aplicar estas sugerencia o no.

Se muestra el siguiente proceso a seguir para implementar un plan de gestión de los riesgos encontrados según nuestro análisis:

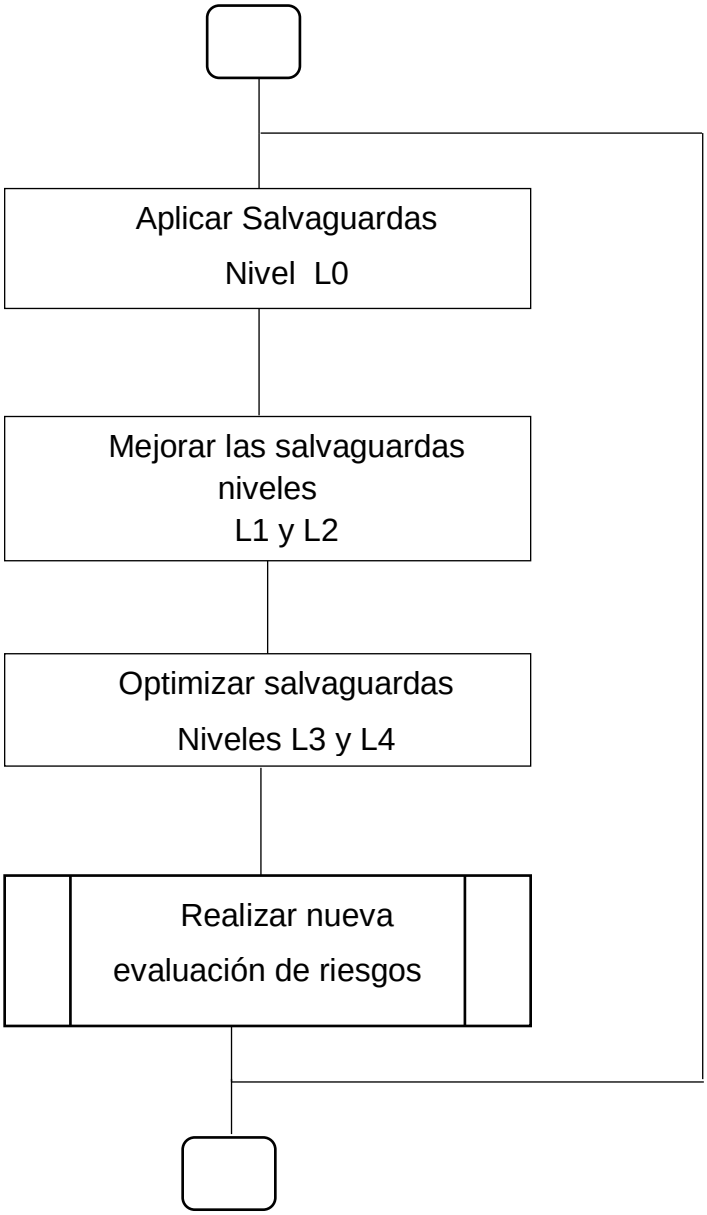


Figura 49 Proceso para implementar un plan de gestión de los riesgos encontrados
Fuente:(DIT, 2016)

Se deberán aplicar primero las salvaguardas de mayor prioridad las de nivel L0 que son medidas preventivas.

Entre las salvaguardas del nivel L0 se encuentran:

- ✓ Prevención contra incendio y terremoto
- ✓ Prevención de fuga de información
- ✓ Prevención de pérdida de almacenamiento
- ✓ Prevención de acceso no autorizado

<u>Salvaguardas nivel L0:</u>

¿Qué hacer?

Para:

Prevenir fuga de información

Reducir riesgo de incendio y terremoto

¿Cómo hacer?

- ✓ Contratar personal responsable de seguridad
- ✓ Realizar simulacros programados periódicamente
- ✓ Desarrollo de plan de emergencia ante incendios
- ✓ Desarrollo de plan de contingencia ante desastres naturales

¿Quién debe hacer?

- ✓ Administrador – Director

¿Qué hacer?

Para:

Prevenir pérdida de almacenamiento

Prevenir errores de configuración

Prevenir acceso no autorizado

¿Cómo hacer?:

- ✓ Coordinar revisión periódica de Copias de seguridad
- ✓ Coordinar revisión periódica de Reglas de cortafuegos
- ✓ Implementar sistema de detección de intrusos
- ✓ Agregar seguridad acceso remoto con autenticación multifactor

¿Quién debe hacer?

- ✓ Analista de Infraestructura y redes

¿Qué hacer?

Para:

Reducir el riesgo de robo de equipos

Disminuir la infección de malware

¿Cómo hacer?

- ✓ Iniciar el uso de cables de seguridad para computadores y laptop
- ✓ Instalar antimalware en servidores y equipos de personal

¿Quién debe hacer?

J. Técnico

En los niveles L1 y L2 se encuentran los procesos que solicitan mejoras.

¿Qué hacer?

Para:

Reducir el riesgo de incendio y terremoto

Mitigar falla de equipos de climatización

Prevenir fuga de información

¿Cómo hacer?

- ✓ Desarrollar plan de emergencia contra incendios
- ✓ Adquirir nuevo equipo de climatización
- ✓ Implementar cifrado de datos
- ✓ Solicitar historial de personal antes de ser contratado
- ✓ Socializar con charlas de seguridad al personal

¿Quién debe hacer?

Administrador - Director

¿Qué hacer?

Para:

Evitar desconexiones físicas

Prevenir acceso no autorizado

¿Cómo hacer?

- ✓ Asegurar equipos de comunicaciones y servidores en armarios cerrados
- ✓ Analizar directivas de cortafuegos con seguridad
- ✓ Asignar cuentas para para la administración de sistemas
- ✓ Implementar controles avanzados de gestión de cuentas
- ✓ Implementar directivas de contraseñas

¿Quién debe hacer?

Analista de infraestructura y redes

¿Qué hacer?

Para:

Evitar errores de configuración

¿Cómo hacer?

- ✓ Realizar pruebas de actualización antes de la instalación

¿Quién debe hacer?

J. Técnico

En los niveles L3 y L4 se encuentran los procesos optimizar las salvaguardas

¿Qué hacer?

Para:

Prevenir riesgo incendio y terremoto

Prevenir falla de generador eléctrico

Prevenir falla de equipo de climatización

¿Cómo hacer?

- ✓ Mantener el uso y mantenimiento de extintores
- ✓ Mantener sistemas y alarmas contra incendios
- ✓ Seguir almacenando los respaldo en otra oficina
- ✓ Mantenimiento semanal al generador
- ✓ Mantenimiento de equipo de climatización
- ✓ Adquirir nuevos equipos de climatización

¿Quién debe hacer?

Administrador – Director

¿Qué hacer?

Para:

Prevenir agotamiento de recurso

Prevenir acceso no autorizado

¿Cómo hacer?

- ✓ Mantenimiento preventivo de servidores y dispositivos de almacenamiento
- ✓ Monitorea de recursos de equipos críticos
- ✓ Mantener los controles de acceso físico

¿Quién debe hacer?

Analista de infraestructura y redes

¿Qué hacer?

Para:

Prevenir infección de virus

¿Cómo hacer?

- ✓ Mantener la instalación de antivirus en servidores y equipos personales

¿Quién debe hacer?

J. Técnico

4.8 PLAN DE SEGURIDAD

El presente plan de seguridad es aplicable en su totalidad en el área del departamento informático del GADMCLL y demás áreas del Gobierno Autónomo Descentralizado Municipal del Cantón La Libertad.

Las políticas expresadas en este plan son necesarias y de vital cumplimiento para todo el personal del GADMCLL, incluyendo sus dependencias adscritas.

Es una propuesta que incluye un porcentaje monetario accesible para la institución; que busca mejorar la seguridad informática.

Tabla 23
Presupuesto Plan de Seguridad

PRESUPUESTO ESTIMADO DE PLAN SEGURIDAD

Criterios de vulnerabilidad	Porcentaje %	Valor
EQUIPOS DE COMUNICACIÓN	40%	3000
SERVIDORES	50%	2500
CORREO ELECTRÓNICO	35%	1500
BASE DE DATOS	50%	2000
COMPUTADORAS PERSONALES	20%	5000
SISTEMAS ADMINISTRATIVOS	30%	2000
INFORMACIÓN	45%	3500

De acuerdo a las siguientes valoraciones realizas mediante encuestas al personal de la dirección informática del GADMCLL para la adquisición de aplicaciones y licencias que permitan detectar e identificar nuevas amenazas para mitigar el riesgo con la prevención y que formen parte del Plan de Seguridad; podemos visualizar que realmente es necesario la aplicación de políticas de seguridad; por lo que se presenta la siguiente propuesta de un Plan de Seguridad que dependerá de la Autoridad Competente implementarla.

RESULTADOS DEL ANÁLISIS DE RIESGO

Los bienes informáticos más importantes a proteger son:

- ✓ La red de trabajo interno
- ✓ El servidor de aplicaciones.
- ✓ Las bases de datos del sistema ORACLE
- ✓ El servicio de correo electrónico

- ✓ El sistema Administrativo

Las amenazas más importantes a considerar de acuerdo al impacto que pudieran tener sobre la empresa son:

- ✓ El acceso no autorizado a la red, tanto producto de un ataque externo como interno.
- ✓ Pérdida de disponibilidad.
- ✓ La sustracción, alteración o pérdida de datos.
- ✓ Fuga de información clasificada
- ✓ La introducción de programas malignos.
- ✓ El empleo inadecuado de las tecnologías y sus servicios.

Las áreas sometidas a un mayor peso riesgo y las amenazas que lo motivan son:

- ✓ El local de los servidores de la red (acceso no autorizado y pérdida de disponibilidad).
- ✓ Servidores (alteración o pérdida de datos, pérdida de disponibilidad y la introducción de programas malignos)

POLÍTICAS DE SEGURIDAD INFORMÁTICA

- ✓ Las propuestas de iniciativas encaminadas a mejorar el sistema de seguridad informática se aprobarán por la Dirección y Autoridad Competente del GADMCLL.
- ✓ El acceso a las tecnologías de la entidad será expresamente aprobado en cada caso y el personal tiene que estar previamente preparado en los aspectos relativos a la seguridad informática.

- ✓ Los usuarios de las tecnologías informáticas y de comunicaciones responden por su protección y están en la obligación de informar cualquier incidente o violación que se produzca a su Jefe inmediato superior.
- ✓ Todos los bienes informáticos serán identificados y controlados físicamente hasta nivel de componentes.
- ✓ Se establecerán procedimientos que especifiquen quién y cómo se asignan y suspenden los derechos y privilegios de acceso a los sistemas de información.
- ✓ Se prohíbe vincular cuentas de correo electrónico de la entidad a un servidor en el exterior del país con el fin de re-direccionar y acceder a los mensajes a través del mismo.
- ✓ En caso de violación de la seguridad informática, se comunicará al Jefe inmediato superior y a la Oficina de Seguridad para las Redes Informáticas y se creará una comisión encargada de analizar lo ocurrido y proponer la medida correspondiente.

RESPONSABILIDADES

- ✓ El analista de redes tiene entre sus funciones, responsabilidades y obligaciones:
- ✓ Garantizar la aplicación de mecanismos que implementen las políticas de seguridad definidas en la red.
- ✓ Proteger la integridad del funcionamiento de la Red supervisando el trabajo de los servidores y velando por el correcto funcionamiento de las comunicaciones informáticas tanto internas como externas.
- ✓ Realizar el análisis sistemático de los registros de auditoría que proporciona el

sistema operativo de la red.

- ✓ Garantizar que los servicios implementados sean utilizados para los fines que fueron creados.
- ✓ Comunicar al Analista de Seguridad Informática los nuevos controles técnicos que estén disponibles y cualquier violación o anomalía detectada en los existentes.
- ✓ Activar los mecanismos técnicos y organizativos de respuesta ante los distintos tipos de incidentes y acciones nocivas que se identifiquen, preservando toda la información requerida para su esclarecimiento.
- ✓ Participar en la elaboración de los procedimientos de recuperación ante incidentes y en sus pruebas periódicas.
- ✓ Informar a los usuarios de las regulaciones de seguridad establecidas y controlar su cumplimiento.
- ✓ Participar en la confección y actualización del Plan de Seguridad Informática informando a la Especialista de Seguridad Informática acerca de cualquier modificación que sea necesaria.
- ✓ Ante indicios de contaminación por virus informáticos u otros programas malignos, descontaminar e informar al Especialista de Seguridad Informática de la entidad.
- ✓ Cumplimentar lo establecido entre las políticas y medidas de seguridad respecto a las salvas del sistema operativo y de las aplicaciones, así como de los datos, con la periodicidad requerida por la frecuencia de actualización de los mismos.
- ✓ Activar los mecanismos técnicos y organizativos de respuesta ante los distintos tipos de acciones nocivas que se identifiquen.
- ✓ Controlar de forma sistemática la integridad del software que se encuentra

instalado en los servidores.

- ✓ Controlar el acceso a los sistemas, aplicaciones y bases de datos en correspondencia con la política establecida para los mismos.
- ✓ Detectar posibles vulnerabilidades en los sistemas y aplicaciones bajo su responsabilidad y proponer acciones para su solución.

MEDIDAS Y PROCEDIMIENTOS

CLASIFICACIÓN Y CONTROL DE LOS BIENES INFORMÁTICOS.

Medidas:

- ✓ Los bienes informáticos deberán estar identificados y controlados, hasta nivel de componentes.
- ✓ Cada uno de los bienes informáticos debe estar puesto bajo la custodia documentada legalmente de una persona, que actuando por delegación de la dirección, es responsable de su protección.
- ✓ Cada ordenador contara con un expediente técnico donde se registraran todos los cambios que ocurran con el equipo.
- ✓ El Dpto. de Informática es responsable del control de los medios informáticos.

Procedimiento No. 1: Alta de Medios Informáticos para su uso.

1. Realizar controles sobre los bienes informáticos que se encuentran en cada departamento
2. Elaborar informe con los resultados de cada control y ponerlo en conocimiento de la dirección del centro.

3. Responsable: Jefe de la Administración Interna.
4. Garantizar que el local donde se ubique el medio informático cuente con las medidas de protección física requeridas.
5. Responsable: Jefe de la Administración Interna.
6. Instalar el software autorizado a utilizar en el área a la que fue asignado el medio informático, dejando constancia en el Registro de software autorizado
7. Responsable: Informático del área.
8. Integrar el equipo al dominio de la red de la Entidad y dejar en funcionamiento el equipo.
9. Actualizar el Sistema Informático de la Entidad.
10. Responsable: Jefe de Informática
11. Confeccionar el Expediente Técnico del medio informático.
12. Responsable: Jefe de Informática
13. Firma del Acta de Responsabilidad Material que incluye el Expediente Técnico del medio informático.
14. Responsable: Funcionario.
15. Capacitar al personal encargado de la operación y protección del medio informático en materia de Seguridad Informática.
16. Responsable: Especialista de Seguridad Informática.

Procedimiento No. 2: Control de Medios Informáticos

1. Aplicar a cada PC las actualizaciones de antivirus
2. Responsable: Informático del área.

3. Elaborar el Expediente Técnico.
4. Responsable: Informático del área.
5. Velar porque los expedientes se encuentren actualizados y se registren en ellos todos los cambios.
6. Responsable: Informático del área.
7. Sellar todas las PC y registrar el número del sello
8. Responsable: Informático del área.
9. Revisar periódicamente que se registren en los expedientes de las PC las revisiones y cambios que se realicen en el equipo.
10. Responsable: Analista de Seguridad Informática.

Procedimiento No. 3: Asignación y control de Medios Informáticos Portátiles.

1. Solicitar por escrito a la Administración Interna la asignación del Medio Informático Portátil
2. Responsable: Jefe del área.
3. Una vez aprobada la solicitud, se notifica al Jefe del Dpto. de Informática para que proceda recoger el medio del almacén.
4. Responsable: Jefe de la Administración Interna.
5. Prepara el medio informático con el software autorizados necesarios para su uso.
6. Responsable: Especialista Informático.
7. Entrega el medio informático al funcionario que hará uso del mismo, dejando constancia en el Acta de Responsabilidad Materia del Expediente Técnico del que se confecciona en el momento de entrega.

8. Responsable: Jefe de Informática.
9. Solicita autorización escrita a la Administración Interna, para la entrada y salida de la Entidad del bien informático.
10. Responsable: Funcionario
11. Evalúa y autoriza el uso del bien informático fuera de las instalaciones de la Entidad.
12. Responsable: Jefe de la Administración Interna.
13. Garantiza en el acceso principal de la Entidad que la salida y entrada de computadoras portátiles se realice por el personal autorizado.
14. Responsable: Jefe de Seguridad y Protección.
15. En caso de que sea necesario la entrada de una computadora portátil ajena a la Entidad por cuestiones de trabajo, solicitar la autorización temporal en el Control de Pases.
16. Responsable: Funcionario.
17. Conservar por un periodo no menor de un año las autorizaciones escritas para la entrada y salida de los equipos portátiles.
18. Responsable: Jefe de Informática.
19. Actualizar el Registro Usuarios autorizados a utilizar las portátiles fuera de la Entidad.
20. Responsable: Jefe de Informática.
21. Revisar periódicamente que el Registro de Usuarios autorizados a utilizar las portátiles fuera de la Entidad se encuentre debidamente actualizado.
22. Responsable: Analista de Seguridad Informática.

PERSONAL

Medidas:

- ✓ En el proceso de selección del personal que se incorpora al GADMCLL, en caso que su trabajo se vincule con las tecnologías informáticas, se incluirá una valoración de su nivel de preparación.
- ✓ La Dirección de Recursos Humanos será la responsable de la valoración de la preparación de cada trabajador, la que requerirá del Jefe de Área correspondiente. Debe quedar documentado el resultado de esta evaluación, así como el plan de capacitación en caso que se requiera.
- ✓ La Dirección de Recursos Humanos garantiza que en el expediente laboral de cada trabajador que se vincula con las tecnologías informáticas se incluya:
- ✓ Obligación de la entidad en cuanto a la preparación del personal

SEGURIDAD FÍSICA Y AMBIENTAL

Medidas:

- ✓ El equipo que cause baja o sea destinado para otras funciones será objeto de revisión por parte del Dpto. Informático, para evitar que la información que contiene pueda realizar comprometida.
- ✓ Para lograr la baja de los bienes informáticos se creara una comisión presidida por el jefe del Dpto. Informático quien decidirá el destino final, cumpliendo con lo legislado al respecto.

Medidas generales para todas las áreas con tecnologías informáticas:

- ✓ Todos los tomacorrientes tendrán señalizado el tipo de voltaje que suministran para evitar accidentes o incendios.
- ✓ Los usuarios antes de conectar o desconectar los equipos de la red eléctrica chequearán que estos estén apagados.
- ✓ Contar con fuentes de respaldo de energía y estabilizadores de voltaje para cada computadora.

Medidas para el Control de Acceso DATA CENTER:

Pueden entrar:

1. Miembros de la Dirección de Seguridad y Protección para verificar el cumplimiento de las medidas de protección física.
2. El Especialista de Seguridad Informática para verificar el cumplimiento de las medidas de seguridad informática y la protección de la información.
3. Miembros del equipo que realiza las auditorías, en cumplimiento de esta tarea.
4. Los máximos niveles de Dirección de la entidad.

Procedimiento No. 5: Mantenimiento a Equipos.

1. Una vez al año se le da mantenimientos a los Equipos.
2. Registra en el Expediente Técnico del equipo la fecha del mantenimiento y el nuevo sello asignado.

3. Una vez finalizado el mantenimiento, se le entrega al Jefe del Dpto. de Informática un Registro de Sellos puestos y la Conformidad de los equipos a los que se les dio mantenimiento.
4. Responsable: Técnico
5. Revisa que se deje constancia en los Expedientes Técnicos del mantenimiento realizado.
6. Responsable: Especialista de Seguridad Informática.

Procedimiento No.6: Autorización y control sobre los movimientos de los bienes informáticos

1. Solicitar autorización por escrito al Director de la Administración Interna para el movimiento de las tecnologías, fundamentando en que consiste el movimiento, los motivos y si es temporal el tiempo requerido.
2. Responsable: Jefe del área a que pertenece el medio a trasladar.
3. Autorizar si es procedente el movimiento de las tecnologías y darlo a conocer al Jefe del área que realizó la solicitud, al Responsable de Medios Básicos y al Departamento de Seguridad y Protección, especificando el tiempo de vigencia de la autorización.
4. Responsable: Jefe de Administración Interna.
5. Actualizar el documento de los medios básicos del Departamento donde se produce el movimiento.
6. Responsable: Responsable de Medios Básicos.
7. Revisar antes de su salida (entrada) de la entidad las tecnologías autorizadas a

trasladar, precisando la existencia y estado de sus partes y componentes, si contienen información y de qué tipo, así como lo relacionado con el control antivirus.

8. Responsable: Jefe del área a que pertenece el medio a trasladar y Jefe de Informática.
9. Consignar el movimiento en el Registro de Movimiento de Equipos, especificando la fecha en que se produce, los datos del equipo objeto del movimiento, de qué lugar se extrae o proviene y a qué lugar se lleva y motivo por el que se realiza el movimiento.
10. Responsable: Jefe del área a que pertenece el medio a trasladar
11. Controlar el cumplimiento de las autorizaciones sobre el movimiento de las tecnologías y su registro adecuado.
12. Responsable: Jefe de Departamento de Seguridad y Protección.
13. Realizar inspecciones sorpresivas para detectar las extracciones no autorizadas.
14. Responsable: Especialista de Seguridad Informática

SEGURIDAD DE OPERACIONES

Medidas:

1. El Especialista de Seguridad Informática designado no realiza tareas vinculadas con la administración de la red, los sistemas y los diferentes servicios.
2. El cambio de contraseñas corresponde al Departamento de Informática.
3. La introducción de nuevas tecnologías de la información en la Entidad será

previamente autorizada por el director, el Jefe de Informática y el Especialista de Seguridad Informática.

4. Las aplicaciones que se utilizan en la entidad son las aprobadas por el Jefe del Departamento Informática.

Procedimiento No. 7: Corrección de errores y brechas de seguridad

1. Preservar las trazas de auditoría de los sistemas en los soportes habilitados al efecto por un tiempo no menor de un año.
2. Ejecutar las herramientas de seguridad autorizadas en la entidad.
3. Analizar los resultados que arrojaron las herramientas y su correspondencia con el nivel de seguridad previsto en la entidad.
4. En caso de detectarse nuevas vulnerabilidades, proponer las acciones necesarias para su evaluación y determinación de las modificaciones requeridas para su eliminación.
5. Informar al Especialista de Seguridad Informática las acciones de emergencias ejecutadas para garantizar la seguridad del sistema.
6. Responsable: Administrador de red.
7. Documentar en el Registro de Incidencias de Seguridad Informática las acciones ejecutadas.
8. Determinar si es necesario realizar cambios en el sistema de seguridad informática diseñado. Diseñar la nueva estrategia a seguir.

Procedimiento No. 8: Introducción de nuevos sistemas informáticos, actualizaciones y

nuevas versiones.

1. Solicitar la aprobación del Jefe de la Administración Interna para la instalación del nuevo sistema informático, actualización o versión.
2. Responsable: Jefe del área
3. Aprobar o denegar solicitud.
4. Responsable: Jefe de la Administración Interna.
5. Notificar al Jefe del Dpto. de Informática sobre la aprobación.
6. Responsable: Jefe del área
7. Comprueba que el del nuevo sistema informático, actualización o versión cumple con el sistema de seguridad establecido en la institución.
8. Responsable: Jefe del Dpto. de Informática y Especialista de Seguridad Informática.
9. Instala y configura el nuevo sistema informático, actualización o versión.
10. Responsable: Proveedor.

IDENTIFICACIÓN, AUTENTICACIÓN Y CONTROL DE ACCESO.

Medidas:

1. Se establecerán identificadores de usuarios en las PCs, sistemas y servicios informáticos en la red.
2. Los identificadores de usuarios se darán por el Administrador de la red al causar alta un usuario al trabajo con las tecnologías de la información, lo cual será notificado por el Jefe de Área correspondiente.
3. Estos identificadores serán eliminados por el Administrador de la red tan pronto el

trabajador cause baja (empleando el mismo procedimiento de notificación).

Procedimiento No. 9: Control de la Identificación de usuario

1. Una vez que los usuarios estén creados, se revisara que los identificadores que se están utilizando correspondan con la situación de los trabajadores autorizados a trabajar con las tecnologías informáticas.
2. Elaborar un informe con los resultados de la inspección y enviárselo al Director de la Administración Interna.
3. Responsable: Especialista de Seguridad Informática.

Procedimiento No. 10: Autentificación de usuario

1. Las Pc contarán con contraseñas que bloqueen el acceso al Setup.
2. La cuenta de administrador estará deshabilitada.
3. El trabajador accederá al ordenador con el usuario que le sea asignado por el dominio. (inicial del nombre + 1er apellido)
4. Responsable: Administrador de la Red.
5. Realizar periódicamente un Control de la Autenticación de usuarios.
6. Responsable: Especialista de Seguridad Informática.

Procedimiento No. 10: Autentificación de usuario en ordenadores desconectados de la red.

1. Las Pc contarán con contraseñas de Inicio del SO, Setup, cuentas de

administrador y usuario estándar.

2. Cada usuario poseerá una contraseña para acceder a la PC en una sesión independiente.
3. Habilitar el uso de protectores de pantalla con contraseña, lo que evitará que la información sea vista en momentos de inactividad y la entrada de intrusos.
4. Responsable: Dpto. de Informática
5. Los usuarios se autenticarán para hacer uso de su cuenta de usuario en la red local y los servicios autorizados.
6. Responsable: Usuarios
7. Realizar periódicamente un Control de la Autenticación de usuarios.
8. Responsable: Especialista de Seguridad Informática.

Procedimiento No. 11: Cambio de contraseña de los servicios de correo e Internet.

Solicitar al Administrador de red el cambio de contraseñas de los servicios de correo e Internet.

1. Responsable: Usuarios
2. Buscar al usuario en el servicio correspondiente.
3. Responsable: Administrador de la Red.
4. Cambiar la contraseña de la cuenta, respetando las políticas definidas para las contraseñas.
5. Responsable: Usuarios.
6. Chequear que en los servicios de correo e Internet estén implementadas las políticas de contraseñas definidas.

7. Responsable: Especialista de Seguridad Informática.

Procedimiento No. 15: Cambio de contraseña de usuario del dominio.

1. Cada 3 meses la contraseña de usuario del dominio expira, por lo que al cumplirse el plazo se notificara al iniciar la sesión que debe realizarse el cambio de la misma.
2. Responsable: Administrador de red.
3. Cambiar la contraseña antes del plazo de 3 meses a través de la combinación de teclas Ctrl+Alt+Supr.
4. Cambiar la contraseña cuando esta expira o solicitar al Administrador de red el cambio de contraseñas antes del tiempo definido.
5. Responsable: Usuarios

SEGURIDAD ANTE PROGRAMAS MALIGNOS.

Medidas:

1. Cada trabajador es responsable de efectuar el chequeo de todos los soportes de propiedad personal o de otra entidad que se autoricen introducir en el ordenador antes de su utilización.
2. La Especialista de Seguridad Informática será la encargada de efectuar la descontaminación de los ordenadores ante la aparición de programas malignos.
3. El Administrador de la Red es el encargado de la correcta actualización del Software Antivirus en el Servidor

4. La actualización del Software Antivirus de las máquinas y Servidores de la Red se realizara diariamente, de forma programada.
5. La actualización del Software Antivirus en los ordenadores donde se procesa Información Oficial Clasificada es responsabilidad del Especialista de Seguridad Informática.
6. Cada trabajador es responsable de comprobar la correcta actualización del Software Antivirus instalado en el ordenador a su cargo.

Procedimiento No. 12: Actualización del Software Antivirus en el Servidor

1. Chequear si la actualización se descargó con efectividad.
2. Responsable: Administrador de la Red.
3. Chequear periódicamente la actualización del Antivirus en el Servidor
4. Responsable: Especialista de Seguridad Informática.

Procedimiento No. 13: Actualización del Software Antivirus en los ordenadores conectados a la Red local

1. Las PC Conectadas a la Red local se actualizarán diariamente a las 2:30 pm de forma programada conectándose al Servidor local
2. A partir de la primera actualización, el proceso se repite 5 veces cada 10 minutos.
3. En caso de estar apagados los ordenadores en el horario previsto, el antivirus se actualizara apenas se encienda el equipo.
4. Responsable: Informático del área.

5. Chequear la correcta actualización del Software Antivirus.
6. Responsable: Usuario del equipo y Especialista de Seguridad Informática.

Procedimiento No. 14: Descontaminación de programas malignos

1. Al detectarse un programa maligno en el ordenador, detener la actividad que se esté efectuando e informar al Jefe Inmediato y al Especialista de Seguridad Informática.
2. Responsable: Usuario del equipo infectado.
3. Desconectar el cable de red de la PC e identificar qué tipo de virus es el que se aloja en el ordenador.
4. Verificar que el Software Antivirus instalado esté debidamente actualizado. En caso de no cumplirse, actualizar el Software Antivirus y proceder con la descontaminación del equipo. De ser exitosa la descontaminación del virus poner en marcha el equipo.

5. Revisar los soportes removibles que pudieron ser afectados por el virus.
6. Investigar las causas de aparición del código maligno, identificar responsables y disponer acciones correctivas
7. Dejar constancia del suceso en el Registro de Incidencias del ordenador.

RESPALDO DE LA INFORMACIÓN

Medidas:

1. Se realizaran copias de seguridad de la información y del software que se determine y se comprobaran con regularidad.
2. Los Jefes de áreas son los responsables de organizar la salva de la información del área respectiva, definiendo la información a salvar y el trabajador encargado de esto.
3. En el caso de la información clasificada y/o limitada la salva debe ser hecha sólo por personal autorizado para el procesamiento de este tipo de información.
4. Cada área dispondrá de un disco externo para la salvaguarda de la información clasificada y/o limitada.

Procedimiento No. 19: Pruebas de Restauración Respaldo de la Información de los Servidores de la Red local

1. Con periodicidad mensual se restauraran los Servidores según la última salva programada realizada.
2. Dejar constancia en el campo Observaciones del Registro de Restauración de Salvas del éxito o fracaso de la restaura realizada.
3. Responsable: Administrador de Red.
4. Controlar periódicamente el cumplimiento de este procedimiento.
5. Responsable: Especialista de Seguridad Informática.

SEGURIDAD EN REDES

Medidas:

1. El Administrador de la red regularmente deberá chequear el tráfico de la red para detectar variaciones que pueden ser síntoma de mal uso de la misma.
2. El Administrador de la red es quien monitorea las conexiones activas y los puertos en la red para saber qué puertos están habilitados y chequear la seguridad de los mismos.
3. El Administrador de la red es quien controla la navegación en los Servidores Proxy-Firewall.
4. La navegación en los Servidores Proxy-Firewall será por nombre de usuario y contraseña.
5. Los Servidores Proxy-Firewall tendrán restricciones de acceso a determinados sitios Web basándose en su contenido.
6. No administrar remotamente la red mediante conexiones conmutadas a través de las redes públicas de transmisión de datos.
7. El Especialista de Seguridad Informática será el encargado de auditar los directorios para poder determinar los ataques que se realizan sobre ellos.
8. El Administrador de la red deberá actualizar el sistema periódicamente con los últimos Service Pack y parches de seguridad para resguardar el sistema de las últimas vulnerabilidades conocidas.
9. El Administrador de la red deberá establecer los permisos de acceso adecuados (administrador, system y usuarios autenticados).

Procedimiento No. 14: Auditoria de eventos.

1. Revisar diariamente los registros de los eventos generados.
2. Ante cualquier anomalía que se detecte, investigar las causas y determinar si se está ante algún incidente de seguridad.
3. Monitoreo de eventos.
4. Mantener la disponibilidad y la actualización de las herramientas que garantizan la auditoria de los eventos.
5. Responsable: Administrador de Red.
6. Controlar periódicamente el cumplimiento de este procedimiento.
7. Responsable: Especialista de Seguridad Informática.

GESTIÓN DE INCIDENTES DE SEGURIDAD.

Procedimiento No. 15: Acceso y/o divulgación de información no autorizada

1. Informar al Jefe del área, y al Especialista de Seguridad Informática.
2. Responsable: Persona que lo detecte
3. Cancelar la operación que está realizando la diseminación de información o la eliminará del lugar en que se encuentre una vez que sea posible eliminar la evidencia.
4. Chequeará los permisos y privilegios de cada usuario y de los Sistemas.
5. Trata de eliminar la posibilidad de que se repita el hecho.

6. Responsable: Especialista de Seguridad Informática
7. Crea Comisión para investigar los hechos.
8. Procede a aplicar las medidas disciplinarias que correspondan.
9. Responsable: Jefe de Área

Procedimiento No. 16: Acceso pirata a la red

1. Informa al Jefe del área y al Especialista de Seguridad Informática.
2. Responsable: Persona que lo detecte.
3. Informa al Director Administración Interna, Jefe del Departamento de Informática y al Administrador de la Red.
4. Responsable: Especialista de Seguridad Informática
5. Chequear periódicamente la red en busca de vulnerabilidades.
6. Si el ataque procede de la propia entidad: El administrador de la red revisa los permisos otorgados, las bitácoras en los servidores (log's) y gestiona o realiza un diagnóstico interno para precisar fallas que pudieran ser aprovechadas por el atacante.
7. Si el ataque procede del exterior: El administrador de la red revisa el firewall. Detecta, de existir, vulnerabilidades en los servidores efectuando o coordinando un diagnóstico.
8. Responsable: Administrador de red
9. Se anota el hecho en el Registro de Incidencias de la Seguridad Informática.
10. Responsable: Especialista de Seguridad Informática
11. Se investigan y analizan las vulnerabilidades en el sistema de seguridad que

propiciaron los hechos. De acuerdo con la trascendencia del ataque se involucra a los órganos competentes.

12. Responsable: Jefe de la Administración Interna

Procedimiento No. 17: Fallo de Hardware

1. Informa al Jefe de Área y este al Jefe del Departamento de Informática
2. Responsable: Persona que lo detecte.
3. Contacta a técnicos encargados de reparación y mantenimiento del equipamiento o a la entidad proveedora del equipamiento defectuoso.
4. Responsable: Jefe de Informática.
5. Si es necesario extraer el equipo y se trata de una máquina contentiva de información clasificada y/o limitada debe retirar el disco del equipo. Si esto no es posible, la información que contiene debe ser salvada por el personal autorizado en otro soporte y borrada físicamente del disco antes de su salida de la entidad.
6. Responsable: Analista de Seguridad Informática
7. Analizan el fallo ocurrido y ejecuta las acciones para la reparación del equipo.
8. Responsable: Técnico.
9. Hace las anotaciones correspondientes en el Registro de Incidencias
10. Responsable: Especialista de Seguridad Informática

Procedimiento No. 18: Fallo de comunicaciones

1. Informa al Jefe del Área quien a su vez informa al Jefe del Departamento de Informática.

2. Responsable: Persona que lo detecte.
3. Determina las causas del fallo de comunicaciones. De ser necesario contacta con el proveedor del servicio e informa de la situación presentada.
4. Responsable: Jefe de Informática.
5. Analiza el fallo ocurrido y ejecuta las acciones para restablecer el servicio.
6. Responsable: Proveedor de Servicios.

Procedimiento No. 19: Fallo de Software.

1. Apaga la microcomputadora y alerta que no se use la misma
2. Informa al Jefe de Área y éste al Jefe del Departamento de Informática.
3. Responsable: Persona que lo detecte.
4. Contacta a técnicos encargados de la administración de los sistemas de gestión de datos o al Administrador de Red, según corresponda.
5. Responsable: Jefe de Informática.
6. Restaura utilizando el software original o soportes con las salvas de los Sistemas Operativos o las Aplicaciones.
7. Informan que la microcomputadora está lista para el uso.
8. Responsable: Informático del área.
9. Realizan anotaciones de este hecho en el Registro de Incidencias.
10. Responsable: Analista de Seguridad Informática
11. Procedimiento No. 20: Destrucción o modificación de la información.
12. Informa al Jefe de Área
13. Responsable: Persona que lo detecte.

14. Informa al Especialista de Seguridad Informática.
15. Responsable: Jefe de Área.
16. Trata de determinar las causas o debilidades en la Seguridad de los sistemas que propiciaron los hechos para corregirlas.
17. Responsable: Especialista de Seguridad Informática
18. Investiga los posibles causantes para tomar las medidas disciplinarias correspondientes.
19. Responsable: Jefe de Área.
20. Procede a orientar al personal encargado de la salva de la información afectada, su restaura a partir de las copias que se tienen.
21. Hace las anotaciones en el Registro de Incidencias.
22. Responsable: Analista de Seguridad Informática

CAPÍTULO 5

5.1 CONCLUSIONES Y RECOMENDACIONES

CONCLUSIONES

- ✓ Se detectó los activos críticos informáticos del Departamento Informático del GADMCLL, mediante levantamiento de información proporcionado por el personal del departamento con la aplicación de la metodología Magerit.
- ✓ Se detectó las amenazas y vulnerabilidades en el Departamento Informático del GADMCLL, aplicación de la metodología Magerit y la herramienta Pilar.
- ✓ Se realizó la Valoración de las amenazas, mediante la herramienta PILAR y se pude detectar dichas amenazas.
- ✓ Se estimó el riesgo informático con la utilización de la herramienta PILAR, con los resultados obtenidos se realizó los siguientes lineamientos de seguridad para el Departamento Informático del GADMCLL.

MAGERIT fue la metodología implementada en el caso de estudio realizado, para estar al tanto de las amenazas a los cuales se encuentran expuestos los activos informáticos que forman parte del departamento de informático del GADMCLL, optando por un análisis de riesgos de orden cualitativo se dio a conocer el nivel de madurez en la seguridad aplicada en la institución para posteriormente sugerir las salvaguardas necesarias para reducir los niveles de riesgo e impacto.

La utilización de la herramienta PILAR permitió ingresar las valoraciones para realizar las evaluaciones concernientes a los activos, amenazas y salvaguardas para posteriormente obtener los niveles de riesgo e impacto tanto acumulado como repercutido respectivamente, mostrados en las tres pestañas con la denominación potencial, current y PILAR estas varían de acuerdo a las salvaguardas aplicadas a cada activo informático del departamento informático del GADMCLL y finalmente se muestran en gráficas radiales con la finalidad de ver de manera más fácil la situación actual de la organización.

RECOMENDACIONES

Una vez terminado el análisis de riesgo y haber mostrado los niveles de riesgo a los que está expuesto la organización y que sin duda alguna es necesario tomar medidas de prevención que ayuden a disminuir el nivel de riesgo a los activos del GADMCLL lo cual dependerá del responsable del departamento informático darle la importancia necesaria a los resultados obtenidos ya que no tomarlas en cuenta provocaría lo siguiente al departamento informático del GADMCLL y a la institución entre estos tenemos:

- ✓ PÉRDIDA DE TIEMPO: la información debe estar siempre disponible.
- ✓ PÉRDIDA DE PRODUCTIVIDAD: ya que si no se dispone de la información, los diferentes departamentos no podrán desempeñar sus funciones de manera correcta.
- ✓ PÉRDIDA DE INFORMACIÓN CONFIDENCIAL: la información no puede ser divulgada públicamente

Ningún sistema informático es cien por ciento seguros, pero implementar buenas políticas de seguridad mitiga el impacto de las posibles amenazas y reducen el riesgo informático mediante la aplicación de salvaguardas.

En el análisis del riesgo informático realizado en el presente proyecto, se obtuvo que la información que se genera dentro del departamento informático del GADMCLL es considerada como el activo informático más preciado e importante, por lo que busca asegurarla mediante políticas, normas, procedimientos, métodos, herramientas y/o técnicas que permitan reducir el riesgo informático al que está expuesta, beneficiando al GADMCLL en mantener íntegra, disponible, auténtica y confiable toda la información que se genere en las distintas áreas.

Se detalla las siguientes recomendaciones:

- ✓ Aplicar los lineamientos de seguridad propuesto en este proyecto debido a que siempre las amenazas van a estar presente a pesar de que existan las salvaguardas y estas sean implementadas. Se podrá conocer que activos informáticos están vulnerables y expuestos a éstas amenazas.
- ✓ Realizar cronograma de mantenimiento de equipos informáticos y de comunicación, ya que es esencial y de orden prioritario tener en buen funcionamiento estos equipos que son importantes para el buen funcionamiento de procesos internos del GADMCLL.
- ✓ Mapa de infraestructura de puntos de red, es necesario tener una buena administración de puntos de red y demás equipos informáticos, permitirá conocer características de la estandarización que mantiene.

- ✓ Diseñar manual de Políticas de seguridad, que permita establecer el canal formal de actuación del personal, en relación con los recursos y servicios informáticos, importantes de la organización.
- ✓ Realizar análisis de riesgo informático dos veces por año con esto se podrá disminuir el riesgo informático de la organización.
- ✓ Mantener el control de la administración de los equipos de cómputo para permitir que sólo personal del departamento informático del GADMCLL tenga acceso a los mismos.
- ✓ Administrar de manera periódica las copias de seguridad
- ✓ Implementar un Sistema de detección de intrusos
- ✓ Implementar sistemas de autenticación de dispositivos remota
- ✓ Activar la seguridad de GRUB, archivo de configuración del SO.
- ✓ Aplicar el Plan de Seguridad de la Información propuesto

Bibliografía

(s.f.). Obtenido de http://revistasic.com/revista93/propuestas_93.htm

Riesgos Informáticos. (2009). Obtenido de http://audisistemas2009.galeon.com/productos2229079.html;

A. Barco, G. d.-M. (s.f.).

Cartaya, M. (2014). *Curso Riesgo de Auditoria;*. Obtenido de http://www.oas.org/juridico/PDFs/mesicic4_ven_ries_aud_2014.pdf

ccn-cert. (s.f.). Recuperado el 2018, de https://www.ccn-cert.cni.es/soluciones-seguridad/ear-pilar/pilar.html

Cetro Criptologico Nacional - España. (s.f.). Obtenido de https://www.ccn.cni.es/index.php/es/

EAR/PILAR- Entorno de Anáilisis de Riesgo. (s.f.). Obtenido de https://www.pilar-tools.com/es/index.html

Hernández, E. (3 de Mayo de 2006). *Riesgos en auditoria*. Obtenido de http://www.gestiopolis.com/riesgos-en-auditoria/

https://administracionelectronica.gob.es. (s.f.). Recuperado el 2018

https://administracionelectronica.gob.es. (s.f.). *MAGERIT: versión 3,"Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información".*

La auditoría: concepto, clases y evolución. (s.f.). Obtenido de http://assets.mheducation.es/bcv/guide/capitulo/8448178971.pdf;

Omar, M. (31 de Marzo de 2013). *ITIL V3 Concepto y definición;*. Obtenido de [2] https://prezi.com/ld11hpu1nqaj/itil-v3-concepto-y-definicion/

PILAR. (s.f.). Obtenido de https://www.pilar-Tools.com/es/glossary/index.html#residual_risk

Romeral, L., & Torres, Á. (Enero de 2008). *Gestión de los Riesgos Tecnológicos*. Obtenido de http://www.aemes.org/index.php/revista-de-procesos-y-metricas/numeros-publicados/ano-2008-volumen-5/volumen-5-g-numero-1-g-enero-2008/183-gestion-de-los-riesgos-tecnologicos/download

Sanchez - Henarojeset, A. (s.f.). https://www.researchgate.net/publication/260483478_Guia_de_buenas_practicas_de_seguridad_informatica_en_el_tratamiento_de_datos_de_salud_para_el_personal_sanitario_en_atencion_primaria.

TCM. (s.f.). *El Mapa General de ITIL v.3 - Conceptos Clave*. Obtenido de http://www.proactivanet.com/UserFiles/File/Noticias/El%20Mapa%20general%20de%20ITIL%20-%20Conceptos%20Clave.pdf;