ANÁLISIS Y GESTIÓN DE RIESGOS DE LOS SISTEMAS DE INFORMACIÓN DE LA ALCALDIA MUNICIPAL DE TULUÁ APLICANDO LA METODOLOGÍA MAGERIT

YAMILET BOCANEGRA QUINTERO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA

ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA

ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA

TULUÁ – VALLE DEL CAUCA

2015

ANÁLISIS Y GESTIÓN DE RIESGOS DE LOS SISTEMAS DE INFORMACIÓN DE LA ALCALDIA MUNICIPAL DE TULUÁ APLICANDO LA METODOLOGÍA MAGERIT

YAMILET BOCANEGRA QUINTERO

Trabajo de grado presentado para obtener el título:
Especialista En Seguridad Informática

Director de proyecto:
Fernando Barajas

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA

ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA

ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA

TULUÁ – VALLE DEL CAUCA

2015

CONTENIDO

pág.

1. LISTADO DE TABLAS

2. LISTADO DE FIGURAS

3. GLOSARIO

Se describen a continuación los elementos teóricos que permiten fundamentar el proceso de conocimiento en el cual se enmarca este proyecto de Análisis y gestión de riesgos de los sistemas de información de la Alcaldía Municipal de Tuluá aplicando la metodología MAGERIT.

Activo. Componente o funcionalidad de un sistema de información susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización. Incluye: información, datos, servicios, aplicaciones (software), equipos (hardware), comunicaciones, recursos administrativos, recursos físicos y recursos humanos. [UNE 71504:2008]

Análisis de Riesgos. El manejo de riesgos es el proceso de identificar el riesgo, evaluarlo y tomar las medidas para reducirlo a un nivel aceptable. La meta es ayudar a las organizaciones a manejar mejor los riesgos relacionados con las TI.

Amenaza. Causa potencial de un incidente que puede causar daños a un sistema de información o a una organización. [UNE 71504:2008].

En general el concepto de amenaza se refiere a un peligro latente o factor de riesgo externo, de un sistema o de un sujeto expuesto, expresada matemáticamente como la probabilidad de exceder un nivel de ocurrencia de un suceso con una cierta intensidad, en un sitio específico y durante un tiempo de exposición determinado.

Una amenaza informática es un posible peligro del sistema. Puede ser una persona (cracker), un programa (virus, caballo de Troya, etc.), o un suceso natural o de otra índole (fuego, inundación, etc.). Representan los posibles atacantes o factores que aprovechan las debilidades del sistema.

Confidencialidad. Es la privacidad y se refiere a que la información solo puede ser conocida por individuos autorizados.

Disponibilidad. Característica de la información de estar siempre disponible para su uso por personas autorizadas, también se ve afectada por los mismos problemas que la integridad.

EAR PILAR. Acrónimo de "Procedimiento Informático Lógico para el Análisis de Riesgos" es una herramienta desarrollada bajo especificación del Centro Nacional de Inteligencia para soportar el análisis de riesgos de sistemas de información siguiendo la metodología Magerit.

Gestión de los riesgos. Comprende la ejecución de dos tareas: el análisis y tratamiento de los riesgos.

La herramienta soporta todas las fases del método Magerit:

- Caracterización de los activos: identificación, clasificación, dependencias y valoración
- Caracterización de las amenazas
- Evaluación de las salvaguardas

La herramienta incorpora los catálogos del "Catálogo de Elementos" permitiendo una homogeneidad en los resultados del análisis:

- Tipos de activos
- Dimensiones de valoración
- Criterios de valoración
- Catálogo de amenazas

Integridad. Es la característica de permanecer intacta la información en su origen, a menos que sea modificada por personas con permiso para hacerlo, esta se puede ver afectada por problemas de hardware, software, virus o personas mal intencionadas.

Magerit. Es una metodología que responde a lo que se denomina "Proceso de Gestión de los Riesgos". 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.

Magerit persigue los siguientes objetivos:

Directos:

1. Concienciar a los responsables de las organizaciones de información de la existencia de riesgos y de la necesidad de gestionarlos.
2. ofrecer un método sistemático para analizar los riesgos derivados del uso de tecnologías de la información y comunicaciones (TIC).
3. Ayudar a descubrir y planificar el tratamiento oportuno para mantener los riesgos bajo control

Indirectos:

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

Riesgo. Es el grado de pérdidas esperadas, debido a la ocurrencia de un suceso particular y como una función de la amenaza y la vulnerabilidad

Riesgo acumulado. Dícese del calculado tomando en consideración el valor propio de un activo y el valor de los activos que depende de él. Este valor se combina con la degradación causada por una amenaza y la frecuencia estimada de la misma**.**

Riesgo Potencial. Riesgos potenciales. Los riesgos del sistema de información en la hipótesis de que no hubiera salvaguardas presentes.

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

Riesgo Residual. Riesgo remanente en el sistema después del tratamiento del riesgo

Seguridad Física. Se encarga del área de protección de los sistema informáticos como hardware, dispositivos de red, dispositivos electrónicos; todo el entorno que los rodea en el lugar que se hallan ubicados (edificios, sistemas eléctricos, seguridad en las cerraduras), además de controlar a las personas que están encargadas de la vigilancia de estos, y tanto de los sistemas informáticos como del entorno. Podemos tomar en cuenta algunos puntos como por ejemplo:

- Desastres naturales: está catalogado como desastre natural toda anomalía de la naturaleza. Ejemplos: los maremotos, terremotos, etc.

- Malas instalaciones: las instalaciones son un punto bastante importante, como los cables mal ubicados o en mal estado, la infraestructura en malas condiciones, un ejemplo bastante común de esta es que los cables eléctricos y de red estén muy juntos.

- Ataques hostiles: el 80% de los ataques a los sistemas de información provienen desde su interior, los entes más peligrosos son los empleados disconformes, éstos están dispuestos a vulnerar la seguridad de la organización.

- Control de acceso: con este se pueden manejar bitácoras, llevando un registro del ingreso a las instalaciones, viendo quien, a qué hora, lo que hizo y si está permitido su acceso al lugar.

Seguridad Lógica. Consiste en la "aplicación de barreras y procedimientos que resguarden el acceso a los datos y sólo se permita acceder a ellos a las personas autorizadas para hacerlo."1, estos son los puntos que la seguridad lógica debe proteger.

- Restringir el acceso a los programas y archivos.
- Asegurar que los operadores puedan trabajar sin una supervisión minuciosa y no puedan modificar los programas ni los archivos que no correspondan.
- Asegurar que se estén utilizados los datos, archivos y programas correctos en y por el procedimiento correcto.
- Que la información transmitida sea recibida sólo por el destinatario al cual ha sido enviada y no a otro.
- Que la información recibida sea la misma que ha sido transmitida.
- Que existan sistemas alternativos secundarios de transmisión entre diferentes puntos.
- Que se disponga de pasos alternativos de emergencia para la transmisión de información.

Seguridad de la información. Confianza en que los sistemas de información están libres y exentos de todo peligro o daño inaceptables**.**

Tratamiento de los riesgos. Son las actividades que en coordinación con los objetivos, estrategia y política de la Organización, permiten elaborar un plan de seguridad que, implantado y operado, satisfaga los objetivos propuestos con el nivel de riesgo que acepta la Dirección. La fase de tratamiento estructura las acciones que se acometen en materia de seguridad para satisfacer las necesidades detectadas por el análisis.

Vulnerabilidad. Es el grado de pérdida de un elemento o grupo de elementos bajo riesgo, resultado de la probable ocurrencia de un suceso desastroso expresada en una escala.

La vulnerabilidad se entiende como un factor de riesgo interno, expresado como la factibilidad de que el sujeto o sistema expuesto sea afectado por el fenómeno que caracteriza la amenaza.

En el campo de la informática, la vulnerabilidad es el punto o aspecto del sistema que es susceptible de ser atacado o de dañar la seguridad del mismo. Representan las debilidades o aspectos falibles o atacables en el sistema informático.

4. RESUMEN

El presente proyecto de grado se enfocará en la elaboración de un análisis y gestión de riesgos de seguridad de los sistemas de información en la Alcaldía Municipal de Tuluá, utilizando la metodología MAGERIT, la cual define la gestión de riesgo en dos fases: La etapa de análisis y la etapa de tratamiento del riesgo.

A través de la etapa de análisis se deberán desarrollar de forma metódica tres actividades principales:

- Identificación de los activos, indicando las dependencias que tiene con los demás activos de la organización y su valoración en cuanto a las dimensiones de disponibilidad, integridad, confidencialidad, autenticidad y trazabilidad.
- Identificación de las amenazas que afectan los activos y su valoración en cuanto a degradación y probabilidad.
- Determinación de salvaguardas que disminuyan el riesgo.

Una vez analizados estos elementos se determina el impacto generado en caso de materializarse la amenaza y el riesgo estimado.

La etapa de tratamiento conlleva a determinar las acciones que se deben tomar en materia de seguridad para suplir las necesidades identificadas en el análisis y cambiar la situación de riesgo.

Finalmente con los resultados obtenidos en el análisis y evaluados en la etapa de tratamiento, se definirán unas políticas que contribuyan al cumplimiento de las dimensiones de disponibilidad, integridad y confidencialidad de los activos informáticos de la entidad.

5. INTRODUCCIÓN

Las amenazas a las que se ven expuestas las organizaciones son cada vez mayores, y los ataques informáticos evolucionan continuamente a la par de los avances de las tecnologías de la información. La Alcaldía Municipal de Tuluá requiere garantizar la seguridad de la información teniendo en cuenta que es el activo más importante para el cumplimiento de sus objetivos constitucionales, razón por la cual se hace necesaria la elaboración de un estudio que le permita conocer y controlar los riesgos, vulnerabilidades y amenazas informáticas a las que está expuesta la información. Una vez identificados estos elementos se definirán unas estrategias que permitan la mitigación de los riesgos identificados.

El objetivo de la investigación es la identificación y gestión de los riesgos informáticos en la Alcaldía de Tuluá utilizando como guía la metodología de análisis y gestión de riesgos MAGERIT, teniendo en cuenta que ofrece un método sistemático para la gestión de riesgos, es una de las más utilizadas y está reconocida internacionalmente.

El alcance del proyecto está definido por el estudio de los siguientes sistemas de información de la Alcaldía de Tuluá: Sistema de Gestión Tributaria, sistema de información de Gestión documental y PQRSD, y el sistema de gestión administrativa que incluye los procesos de Contabilidad, Presupuesto, Tesorería, Proyectos de inversión, Gestión humana y gestión de recursos físicos.

6. PLANTEAMIENTO DEL PROBLEMA

En los últimos años el estado colombiano ha iniciado una transformación de sus entidades, en cuanto al aprovechamiento de las tecnologías de la información y las comunicaciones para satisfacción de necesidades y mejora en la calidad de vida de los ciudadanos.

Aprovechando los avances de la tecnología se ha mejorado la comunicación e interacción con la ciudadanía, mediante el desarrollo de aplicaciones y prestación de trámites y servicios en Línea.

Atendiendo las directrices del gobierno nacional, la entidad pública territorial objeto del presente estudio ha venido incorporando las TIC en su operación, innovando e implementando diferentes servicios y trámites electrónicos.

Este nuevo modelo exige que se realicen esfuerzos cada vez mayores que permitan, no solo aumentar el número y uso de servicios en línea, sino también mejorar la calidad, y el acceso a los mismos, de una forma segura y confiable.

Teniendo en cuenta el valor de la información que viaja a través de la red de datos, la protección de datos personales, el manejo de la reserva y la gestión segura de los trámites, se requiere garantizar las condiciones de accesibilidad, usabilidad, calidad, seguridad, reserva y privacidad.

La incorporación de la tecnología ha generado una creciente dependencia tecnológica, es decir se depende del óptimo desempeño de la tecnología para funcionar, pero al no existir medidas que reduzcan el impacto ante posibles eventualidades, es muy probable que se presente pérdida de operación de las actividades del negocio y de los procesos y por ende pérdida de dinero al suspender servicios misionales. Las probabilidades de ocurrencia de delitos informáticos y ataques por ingeniería social han ido en aumento.

No existe una adecuada identificación de las vulnerabilidades y amenazas a las se encuentra expuesta la infraestructura tecnológica de redes y comunicaciones, de modo que no se cuenta con las suficientes medidas preventivas y no se hace una medición de efectividad de los controles ya establecidos. No existen medidas que permitan el restablecimiento del servicio de manera oportuna ante la materialización de incidentes.

La falta de un análisis adecuado de riesgos y vulnerabilidades y tratamiento de los riesgos, no permitirá que la organización pueda gestionar eficientemente su seguridad, exponiendo sus activos con alto grado de vulnerabilidad a sufrir un ataque informático con resultados catastróficos. No se podrá dar cumplimiento al objeto principal de darle al ciudadano y a la misma entidad la tranquilidad de que su información, trámites y transacciones cuentan con las protecciones adecuadas.

Formulación del problema

¿Cómo se puede mejorar la seguridad de la información de La Alcaldía Municipal de Tuluá, a partir del análisis y gestión de riesgos informáticos de los sistemas de información?

7. JUSTIFICACIÓN DEL PROYECTO

La información es el activo más importante para cualquier organización, y debido a su importancia, las entidades requieren implementar medidas para su protección.

La Gestión de la seguridad de la información es un proceso mediante el cual se pretende alcanzar unos niveles adecuados de confidencialidad, integridad, disponibilidad, trazabilidad y autenticidad. El proceso de gestión de seguridad de la información incluye dentro de sus actividades identificar y analizar las amenazas, vulnerabilidades y gestionar los riesgos de los activos de información.

Teniendo en cuenta la naturaleza de los servicios y trámites prestados por las entidades territoriales gubernamentales se hace necesario cumplir con todos los requisitos de calidad, disponibilidad, accesibilidad y estándares de seguridad.

El cumplimiento de estas características contribuye a lograr avances significativos en la transformación de la entidad hacia la construcción de un Estado más eficiente, más transparente y participativo que preste mejores servicios.

8. OBJETIVOS DEL PROYECTO

8.1. OBJETIVO GENERAL

Aplicar una metodología de análisis y gestión de riesgos que permita medir la seguridad de los sistemas de información de la Alcaldía Municipal de Tuluá y que facilite al administrador de seguridad conocer las vulnerabilidades y obtener la información necesaria para crear políticas de seguridad que minimicen o eliminen los riesgos en el manejo de la información.

8.2. OBJETIVOS ESPECÍFICOS

- Identificar los riesgos de seguridad y vulnerabilidades de los sistemas de información de la Alcaldía Municipal de Tuluá mediante la aplicación de la metodología MAGERIT.

- Especificar los riesgos que presentan una mayor probabilidad de ocurrencia y que generan mayor impacto en caso de materializarse de acuerdo a los resultados obtenidos mediante el análisis de riesgos.

- Definir las políticas de seguridad para los sistemas de información de la Alcaldía de Tuluá que permitan mejorar el nivel de seguridad informática.

- Determinar el nivel de disminución de los riesgos de los sistemas de información de la Alcaldía de Tuluá mediante el establecimiento de políticas y medidas de seguridad que mitiguen los riesgos detectados.

9. MARCO REFERENCIAL

9.1. DIAGNOSTICO

El Departamento de tecnología de la Alcaldía Municipal de Tuluá fue creado en el año 1.989, mediante proceso de reestructuración administrativa de la entidad. Surgió como respuesta a la necesidad de contar con un organismo que se encargara de implementar los proyectos de las nuevas tecnologías nacientes en aquella época.

Desde su creación se emprendió un arduo camino de mejoramiento de la infraestructura tecnológica logrando posicionar al Municipio de Tuluá como modelo tecnológico gubernamental a nivel Nacional, haciéndose merecedor de muchos reconocimientos nacionales e internacionales como el premio Iberoamericano de ciudades digitales, en el cual ha sido ganador y finalista por varios años consecutivos.

Actualmente se adelantan procesos de modernización que buscan integrar las Tecnologías de Información y Comunicación (TICs) con los procesos internos de la entidad y los servicios y productos dirigidos a los ciudadanos.

En búsqueda del mejoramiento continuo se han implementado algunos controles y medidas de seguridad, pero no existe un diagnóstico ni análisis periódico de los riesgos y vulnerabilidades que nos permitan conocer con que niveles de seguridad cuenta la entidad y si los controles adoptados han sido efectivos. Los controles actualmente establecidos han sido implantados sin la realización de un estudio previo de las amenazas.

9.2. MARCO CONCEPTUAL

En la medida en que se avanza en la implementación de nuevas tecnologías de la información, las entidades han ido tomado conciencia de que deben proteger los activos tecnológicos. A la par de los adelantos tecnológicos surgen diversas amenazas que ponen en riesgo el activo más importante: “la información”. El estado Colombiano no es ajeno a

esta problemática, y en tal sentido el gobierno nacional a través del Ministerio de las Tecnologías de la Información y Comunicación ha emitido las directrices necesarias para mejorar el desempeño de las entidades gubernamentales, exigiendo la adopción de normas y estándares de seguridad de la información existentes y reconocidas a nivel internacional. Mediante decreto No. 2573 de 2014 el gobierno nacional estableció los lineamientos generales de la Estrategia de Gobierno en Línea de la República de Colombia y adoptó el *Marco de referencia de arquitectura empresarial para la gestión de las tecnologías de la información* - IT4, el cual consta de 6 dominios. El dominio de "Gobierno de TI" contempla dentro de sus principios la gestión de riesgos. Ese elemento ayuda a establecer y optimizar el valor de TI para la institución y sus procesos, permitiendo que las decisiones de inversión y esfuerzo de TI sean eficientes y efectivas, y tengan en cuenta criterios de seguridad de la información y riesgos.

En este sentido, la Alcaldía Municipal de Tuluá debe buscar la forma de gestionar de forma eficiente sus riesgos informáticos, garantizando la prestación de servicios a la comunidad. Mediante acto administrativo de 25 de julio de 2008 se conformó el "Comité de gobierno en línea" encargado de implementar la estrategia de Gobierno en Línea en el Municipio de Tuluá.

9.3. MARCO TEORICO

SEGURIDAD DE LA INFORMACION

De acuerdo con Cano (2004) en múltiples investigaciones realizadas se considera el tema de la seguridad informática como una disciplina del conocimiento donde se busca cerrar la brecha de los eventos inesperados que puedan comprometer los activos de una organización y así contar con estrategias para avanzar ante cualquier eventualidad. Se sugieren herramientas de análisis de situaciones extremas que lleven no solamente a considerar las vulnerabilidades, amenazas y riesgos de la información de los procesos de la organización,

sino repensar los procesos mismos para hacerlos más confiables. El análisis de riesgos permite a las organizaciones aprender de sus fallas de seguridad y fortalecer sus esquemas de seguridad.

RIESGOS INFORMATICOS

De igual forma Gómez, Pérez, Donoso y Herrera advierten que las organizaciones son cada vez más conscientes de lo que significan los riesgos informáticos y que han aprendido a aceptar la convivencia con algunos de forma controlada.

Los impactos que pueden generar los riesgos referentes a las Tecnologías de Información pueden afectar de manera significativa la reputación y la solidez financiera y operacional.

9.4. MARCO CONTEXTUAL

Nombre de la entidad
Municipio de Tuluá

Tuluá "Ciudad Región"

Tuluá es un municipio estratégicamente ubicado en el centro del Valle del Cauca, departamento al occidente de Colombia; de ahí que sea llamado "El Corazón del Valle". En la actualidad, se constituye en una de las ciudades intermedia más importantes de Colombia.

Con una población de más de 200.000 habitantes, su área de influencia abarca quince municipios, que suman no menos de 600 mil moradores, lo que le da el carácter de "ciudad

región", convirtiéndose en punto obligado de encuentro comercial y de servicios, para esta zona del país.

Tuluá cuenta con diversas vías de acceso y contacto con todos los municipios de la región; está ubicada en la ruta de la vía Panamericana, su ubicación geográfica es estratégica por su equidistancia a ciudades capitales como Cali a 100 km, Armenia a 105 km, Pereira a 125 km y Buenaventura el puerto sobre el Océano Pacífico más importante de Colombia a 172 km. Cuenta además con una vía en doble calzada de conexión interdepartamental hacia el sur y norte, destacándose por su excelente mantenimiento vial.

El desarrollo tecnológico también juega un papel determinante en Tuluá: ubicado en la Universidad Central del Valle del Cauca, está Parquesoft, uno de los proyectos más ambiciosos para generar empleo y prestación de servicios de software a escala internacional, de la misma manera que, en la Universidad del Valle sede Tuluá se encuentra una incubadora de empresas apoyada por diversas agencias locales e internacionales. Ambas están orientadas a abrir nuevos espacios para la prestación de servicios y la generación de empleo.

Reseña Histórica

El Palacio Municipal

Don Rufino Gutiérrez, consagrado historiador de principios del siglo XX, por mandato de la Biblioteca de Historia Nacional, recorrió el país escribiendo monografías de las ciudades colombianas.

Visitó a Tuluá a finales de la segunda década del siglo XX, y hace un excelente estudio de la "Villa de Céspedes", en su obra "MONOGRAFÍAS" de Biblioteca de Historia Nacional y editada en Bogotá por la Imprenta Nacional en 1921. Dice don Rufino Gutiérrez, que

llegó a Tuluá el 27 de Enero de 1918; en la página 146 agrega, "Tiene el Distrito estas propiedades: Casa Consistorial en construcción, apenas empezada, y por eso se paga arrendamiento por los locales que ocupan sus oficinas."

En esa edificación iniciada en la Alcaldía de don Abel Potes en 1918 y situada en la Carrera 26 con Calle 24, local que hoy ocupa EMPRESAS MUNICIPALES (EMTULUA), fue el primer edificio propio de Tuluá para su Alcaldía y Concejo Municipal.

El Concejo Municipal de Tuluá en su periodo de 1927 a 1929, inició la construcción de un nuevo edificio con especificaciones modernas de la época, situado en la Carrera 25 con Calle 25. La siguiente legislatura municipal, 1929 - 1931, continuó con esa obra que tiene la destinación para la escuela pública, con una inversión de $43.000,oo; su construcción duró 16 años.

Inicialmente el edificio fue ocupado por la Escuela Caldas para varones y destinado luego para oficinas públicas con el título de Palacio Municipal, en 1943. La ya antigua Casa Consistorial de la Carrera 26 con Calle 24 fue alquilada a Rentas Departamentales.

En el primer piso del nuevo edificio, funcionaron las oficinas del Jurado Electoral, Tesorería, Inspección Fiscal, Personería y Alcaldía Municipal.

En el segundo piso se instaló el Honorable Concejo Municipal, Secretaría del Concejo y la Jefatura de Estadística; los Juzgados 1° y 2° Municipales y Centro Cafetero de Higiene. Así vio la luz el Palacio Municipal.

Funciones

- Administrar los recursos y establecer los tributos necesarios para el cumplimiento de las funciones en el Municipio como entidad fundamental de la división político-administrativa del estado.

- Garantizar la prestación de los servicios públicos que determine la Ley y, en desarrollo y progreso local; promover la participación comunitaria para el mejoramiento social y cultural de los habitantes.

- Las demás funciones que le asigne la Constitución, la Ley, los Decretos del Gobierno, las Ordenanzas y los Acuerdos del Concejo Municipal Cumplir y garantizar el cumplimiento de los Planes de Desarrollo del Municipio acorde con el programa de Gobierno presentado.

Objetivos Estratégicos

Los Objetivos Estratégicos se encuentran articulados al cumplimiento de las metas establecidas dentro de los siete (7) ejes enmarcados en el Plan de Desarrollo “Tuluá un Territorio ganador”

1. Reactivar la economía y reducir el desempleo, mejorando las condiciones de competitividad para la inversión, la empresarialidad y los encadenamientos productivos

2. Reducir la pobreza e incrementar las condiciones para el bienestar de las poblaciones más vulnerables

3. Mejorar las condiciones de seguridad para la reducción de los índices de delitos de impacto que afectan la seguridad democrática y ciudadana de los habitantes, generando políticas que construyan un ambiente de sana convivencia.

4. Mejorar la calidad de vida urbana y rural del municipio, a través del ordenamiento territorial. la movilidad, el espacio público, la infraestructura, el desarrollo habitacional y la prestación de los servicios públicos, orientarán el desarrollo continuo en atención a las necesidades de la ciudad y la ciudadanía.

5. Promover la integración territorial y el enfoque del desarrollo regional que permita la construcción de una agenda conjunta con los municipios vecinos en función de temas de interés estratégico para la subregión centro del valle del cauca.

6. Gestionar una política ambiental integral para la recuperación, restauración, sostenibilidad, gestión y mejoramiento de la calidad del medio ambiente.

7. Crear un entorno de cohesión social que permita el fortalecimiento del estado del bienestar, el estado de derecho, de los derechos humanos, la democracia, la igualdad de condiciones para todos y la justa repartición de los poderes, así como de los beneficios del desarrollo a través de reglas de juego claras que conduzcan a la comunidad tulueña por la senda de la equidad para el bienestar.

Misión

Ser un territorio generador de BIENESTAR, enmarcado en el desarrollo social, económico, institucional, territorial, ambiental, de convivencia pacífica, e integración regional y global, sustentado en unos principios rectores de gobernabilidad que permitan a la ciudadanía afianzar su credibilidad en el gobierno local, garantizando la inversión de los recursos con

criterios de prelación, igualdad, apoyo y desarrollo sostenible, para el cumplimiento de una gestión pública transparente y de calidad

Visión

Con el apoyo decidido de su ciudadanía, Tuluá será un municipio generador de BIENESTAR, desarrollando políticas y estrategias sociales, de seguridad, de infraestructura, ambientales y territoriales, dando atención a toda la comunidad, en especial a grupos vulnerables, consolidando una Sociedad ganadora de resultados que beneficien a todos los Tulueños.

Política de Calidad

Avanzar hacia el buen gobierno mediante la implementación de acciones integrales de mantenimiento y mejoramiento continuo del Sistema de Gestión Integrado SIGI, que fortalezcan la institucionalidad y el ejercicio de la función pública, propiciando credibilidad y bienestar a la ciudadanía Tulueña.

9.5. MARCO LEGAL

Dentro de las políticas del Estado colombiano están la investigación, el fomento, la promoción y el desarrollo de las Tecnologías de la Información y las Comunicaciones y es su deber promover el acceso eficiente y en igualdad de oportunidades, a todos los habitantes del territorio nacional.

Las entidades del orden nacional y territorial están obligadas a adoptar todas las medidas que sean necesarias para facilitar y garantizar el desarrollo de la infraestructura requerida, estableciendo las garantías y medidas necesarias que contribuyan en la prevención, cuidado y conservación para que no se deteriore el patrimonio público y el interés general

El Estado interviene en el sector las Tecnologías de la Información y las Comunicaciones Promoviendo la seguridad informática y de redes para desarrollar las Tecnologías de la Información y las Comunicaciones.

En acatamiento de los mandatos legales, la Alcaldía Municipal de Tuluá como entidad territorial deberá cumplir con la siguiente normatividad:

- LEY 1341 DE 2009. Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones –TIC–, se crea la Agencia Nacional de Espectro y se dictan otras disposiciones.

- Decreto No. 2573 de 2014 - Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en Línea de la República de Colombia, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones".

  Dentro de los fundamentos para el desarrollo de la Estrategia se encuentra el componente 4: “Seguridad y privacidad de la Información. Comprende acciones transversales a demás componentes enunciados, a proteger la información y sistemas de información, del acceso, divulgación, interrupción o destrucción no autorizada“

  Los plazos establecidos para el cumplimiento del componente 4 de las alcaldías de primera, segunda y tercera categoría son los siguientes:

Tabla 1. Plazos componente 4

COMPONENTE/AÑO	2015	2016	2017	2018	2019	2020
Seguridad y privacidad de la Información	10%	30%	50%	Mantener 65%	Mantener 80%	Mantener 100%

Fuente: Decreto No. 2573 de 2014

Los siguientes modelos y estándares nacionales e internacionales deberán ser tenidos en cuenta por la Alcaldía Municipal de Tuluá para su proceso de análisis y gestión de riesgos:

- Marco de Referencia de Arquitectura Empresarial para la gestión de Tecnologías de la Información: Es un modelo de referencia puesto a disposición las instituciones del Estado colombiano para ser utilizado como orientador estratégico de las arquitecturas empresariales, tanto sectoriales como institucionales. El Marco establece la estructura conceptual, define lineamientos, incorpora mejores prácticas y orienta la implementación para lograr una administración pública más eficiente, coordinada y transparente. a través del fortalecimiento de la Tecnologías de la Información.

- ISO/IEC 27000 series: La serie de normas ISO/IEC 27000 son estándares de seguridad publicados por la Organización Internacional para la Estandarización (ISO) y la Comisión Electrotécnica Internacional (IEC). La serie contiene las mejores prácticas recomendadas en Seguridad de la información para desarrollar, implementar y mantener Especificaciones para los Sistemas de Gestión de la Seguridad de la Información (SGSI).

  ISO 27000: Contiene términos y definiciones que se emplean en toda la serie 27000. La aplicación de cualquier estándar necesita de un vocabulario claramente definido.

ISO 27001 Es la norma principal de la serie y contiene los requisitos del Sistema de Gestión de Seguridad de la Información. En su Anexo A, enumera en forma de resumen los objetivos de control y controles que desarrolla la ISO 27002:2005 para que sean seleccionados por las organizaciones en el desarrollo de sus SGSI.

ISO 27002: Desde el 1 de Julio de 2007. Es una guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a Seguridad de la Información. No es certificable.

ISO 27003: Consiste en una guía de implementación de SGSI e información acerca del uso del modelo PDCA (Plan, Do, Check, Act) y de los requerimientos de sus diferentes fases.

ISO 27004: Especifica las métricas y las técnicas de medida aplicables para determinar la eficacia de un SGSI y de los controles relacionados.

ISO 27005: Consiste en una guía de técnicas para la gestión del riesgo de la Seguridad de la Información y sirve, por tanto, de apoyo a la ISO 27001 y a la implantación de un SGSI.

ISO 27006: Especifica los requisitos para la acreditación de entidades de auditoría y certificación de Sistemas de Gestión de Seguridad de la Información.

ISO 27007: Consiste en una guía de auditoría de un SGSI.

ISO 27011: Consiste en una guía de gestión de seguridad de la información específica para telecomunicaciones.

ISO 27031: Consiste en una guía de continuidad de negocio en cuanto a tecnologías de la información y comunicaciones.

ISO 27032: Consiste en una guía relativa a la ciberseguridad.

ISO 27033: Es una norma consistente en 7 partes: gestión de seguridad de redes, arquitectura de seguridad de redes,escenarios de redes de referencia, aseguramiento de las comunicaciones entre redes mediante gateways, acceso remoto, aseguramiento de comunicaciones en redes mediante VPNs y diseño e implementación de seguridad en redes.

ISO 27034: Consiste en una guía de seguridad en aplicaciones.

ISO 27799: Es un estándar para la seguridad de la información en el sector salud.

- MAGERIT. Es una metodología que responde a lo que se denomina “Proceso de Gestión de los Riesgos”. 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.

- Ley 1273 de 2009. Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones"

10. DISEÑO METODOLÓGICO PRELIMINAR

Para el desarrollo de la presente investigación se consultarán las fuentes de información existentes en la Alcaldía de Tuluá tales como planos, inventarios de activos de información, activos tecnológicos y sus configuraciones. Se realizará recolección de información mediante visitas exploratorias a las instalaciones y entrevistas con el personal responsable del área de tecnología.

La población objetivo del proyecto es el área de tecnología de la Alcaldía Municipal de Tuluá.

Las actividades requeridas para el proceso de análisis y gestión de riesgos de la Alcaldía de Tuluá, van a estar definidas por la metodología de gestión de riesgos MAGERIT, y son las siguientes:

1. Actividades preliminares

Antes de iniciar con el análisis y gestión de riesgo se deberán ejecutar unas actividades iniciales de planificación del proyecto. Comprende los siguientes puntos:

1.1. Estudio de oportunidad
1.2. Determinación del alcance del proyecto
1.3. Planificación del proyecto
1.4. Lanzamiento del proyecto

2. Análisis de Riesgo

Se realizará un diagnóstico para establecer la magnitud de los riesgos informáticos existentes en los sistemas de información de la Alcaldía de Tuluá, estableciendo su probabilidad de ocurrencia y el impacto generado. El estudio se llevará a cabo los siguientes pasos:

2.1. Realizar el inventario de activos de información

2.1.1. Identificar los activos que hacen parte de la red LAN.

2.1.2. Establecer las dependencias entre los activos, indicando cuales activos afectan a otros al ser impactados por una amenaza.

2.1.3. Valorar los activos en las dimensiones de integridad, disponibilidad, confidencialidad.

2.2. Identificar y valorar las amenazas a las que están expuestas los activos

2.2.1. Identificar las amenazas por cada activo de información, las cuales puede ser de origen natural, del entorno, defectos de las aplicaciones, causadas por las personas de forma accidental y causadas por las personas de forma deliberada.

2.2.2. Valorar las amenazas considerando que los activos no se afectan en la misma dimensión, ni en la misma cuantía. Se realiza la valoración teniendo en cuenta la degradación y probabilidad.

2.3. *Determinación del impacto potencial*

Se calculará la medida del daño sobre el activo derivado de la materialización de una amenaza. Se considerará el valor de los activos, la degradación, y la dependencia entre los activos.

2.4. Determinación del riesgo potencial

Se calcula con el valor del impacto por la probabilidad de ocurrencia de la amenaza y cuál es el activo que ha sido impactado.

2.5. Determinar Salvaguardas y su eficacia

2.5.1. Identificar los Salvaguardas que permitan reducir el riesgo

2.5.2. Valorar las salvaguardas de acuerdo su eficacia en la reducción del riesgo.

2.6. Estimar el estado del riesgo

2.6.1. Se estimará el impacto residual teniendo en cuenta la eficacia de las salvaguardas.

2.6.2. Estimar el riesgo residual teniendo en cuenta la eficacia de las salvaguardas.

3. Gestión del riesgo

Se desarrollarán las siguientes actividades:

3.1. Evaluación

3.2. Tratamiento

A partir del análisis disponemos de información para tomar decisiones conociendo lo que queremos proteger considerando los siguientes factores:

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

11. DESARROLLO DEL PROYECTO

11.1. ACTIVIDADES PRELIMINARES

Antes de iniciar la etapa de análisis y gestión de riesgos de la Alcaldía Municipal de Tuluá se llevaran a cabo las siguientes actividades:

- Estudio de oportunidad
- Determinación del alcance del proyecto
- Planificación del proyecto
- lanzamiento del proyecto

11.1.1. ESTUDIO DE OPORTUNIDAD

La Alcaldía Municipal de Tuluá es una entidad gubernamental que cuenta con una infraestructura tecnológica sobre la cual presta sus servicios internos y a la comunidad en general. Enmarcados dentro de la mejora continua ha venido implementando una serie de controles con el objeto de mitigar algunos inconvenientes de seguridad detectados. Sin embargo para el análisis de sus amenazas y vulnerabilidades no se ha desarrollado ninguna metodología estandarizada que le permita identificar de forma efectiva los riesgos tecnológicos que generan mayor impacto en la organización, tampoco se ejerce una verificación sobre la eficacia de los controles que se encuentran implantados.

Se cuenta con bases de datos de información muy relevantes para la entidad y la comunidad en general, que requieren de medidas de protección eficaces y cuya pérdida podría significar incumplimiento de los deberes legales e impacto económico y social.

Teniendo en cuenta los antecedentes sobre materialización de amenazas, y los impactos antes mencionados se hace necesaria la realización de un análisis y gestión de riesgos informáticos.

11.1.2. DETERMINACIÓN DEL ALCANCE DEL PROYECTO

Activos Esenciales

El alcance del proyecto está definido por el análisis y gestión de riesgos de los siguientes sistemas de información:

Sistema de información Tributaria: Gestiona la información catastral del Municipio, la cual es el insumo para la liquidación del impuesto predial unificado, liquidación del impuesto de industria y comercio y complementarios, liquidación de Reteica, liquidación de rentas varias, procesos de fiscalización y cobranzas, proceso de recaudo.

Sistema de información de gestión administrativa: Gestiona los procesos de Contabilidad, Presupuesto, Tesorería, Proyectos de inversión, contratación, Gestión humana y Gestión de recursos físicos.

Sistema de gestión documental y PQRSD: Gestiona el proceso de correspondencia interna y externa, y las peticiones, quejas, reclamos y denuncias de la comunidad.

Puntos de intercambio

El sistema de información tributaria se comunica con el sistema de gestión administrativa a través de interfaz en línea mediante la cual envía la información del recaudo Municipal para su ingreso al presupuesto, contabilización y gestión de tesorería.

Proveedores externos

Los sistemas de información se encuentran apoyados por los siguientes proveedores:

- Convenio TX
- Soluciones de Información
- Sistemas Asociados

Una vez realizado el análisis y gestión de riesgos se definirán una serie de políticas de seguridad para los sistemas de información de la Alcaldía de Tuluá que permitan mejorar el nivel de seguridad informática.

Las áreas de la organización impactadas con la ejecución del proyecto son Secretaría de Hacienda (Rentas, Tesorería, Presupuesto y Contabilidad), Secretaría de Desarrollo institucional (Almacén general, Gestión y Desarrollo Humano, Gestión documental), Planeación Municipal (Banco de proyectos) y todas las demás dependencias que generen procesos de contratación de la entidad.

El estudio se realizará en el área de tecnología de la entidad y el tiempo planificado para la ejecución del proyecto es de 45 días hábiles.

11.1.3. PLANIFICACIÓN DEL PROYECTO

Para la ejecución del proyecto se llevarán a cabo entrevistas con el personal del Departamento de tecnología donde se identificarán las principales fallas de seguridad de los sistemas.

En un término de 5 días se realizarán sesiones de trabajo para recoger información relevante. Cada sesión tendrá una duración de 3 horas diarias. Los entrevistados serán los técnicos operativos y el Director de tecnología.

Los recursos necesarios para el desarrollo son: Computador personal, escritorio, cuestionarios y acceso a las instalaciones.

11.1.4. LANZAMIENTO DEL PROYECTO

Se realiza proceso de socialización del proyecto con el equipo de trabajo del Departamento de tecnología con el objeto de dar a conocer los objetivos, responsables y duración.

Para la recolección de la información se utilizarán las fichas del apéndice 2 del libro "Catálogo de elementos – Magerit", por considerar que se ajusta al tipo de proyecto. Los cuestionarios se adaptan con el objetivo de identificar correctamente los elementos de trabajo: activos, amenazas, vulnerabilidades, impactos, salvaguardas existentes, restricciones generales, etc.

Se tomará como referencia el libro "Catálogo de elementos – Magerit" para el catálogo de tipos de activos y demás elementos.

Las dimensiones de valoración de activos serán: Disponibilidad, integridad, Confidencialidad.

11.2. ANALISIS DE RIESGOS

Durante esta fase se determinará el riesgo y el impacto que tiene sobre la organización en caso de que este llegue a materializarse para lo cual se identificarán y valorarán los elementos informáticos que posee la red LAN de la Alcaldía de Tuluá en su edificio central. Se realizará un análisis que permita identificar y valorar las amenazas a los que están expuestos considerando en cuánto se afecta el activo y la probabilidad de ocurrencia. El análisis se deberá realizar en función de la preservación de la seguridad de los activos que sean considerados como esenciales.

Al realizar esta etapa se alcanzarán los siguientes objetivos:

- Identificación de los activos, indicando las dependencias que tiene con los demás activos de la organización y su valoración en cuanto a las dimensiones de disponibilidad, integridad y confidencialidad.

- Identificación de las amenazas que afectan los activos y su valoración en cuanto a degradación y probabilidad.

- Determinación de salvaguardas que disminuyan el riesgo.

11.2.1. INVENTARIO DE ACTIVOS DE INFORMACION

11.2.1.1. IDENTIFICACIÓN DE ACTIVOS

Se realizó identificación de los activos que hacen parte de la red LAN de la Alcaldía Municipal de Tuluá y que se relacionan con los sistemas de información objeto del presente estudio, y se tipificaron de acuerdo a la clasificación del Libro II MAGERIT Catálogo De Elementos**:**

Tabla 2. Tipos de activos

Tipos de activos	Descripción del Tipo
(ESSENTIAL) Activos esenciales	Marcan los requisitos de seguridad para todos los demás componentes del sistema.
(S) servicios	Esta sección contempla servicios prestados por el sistema.
(K) Claves criptográficas	partes. Las claves criptográficas, combinando secretos e
(D) Datos/ informacion	servicios. La información es un activo abstracto que será
(SW) aplicaciones	etc.) este epígrafe se refiere a tareas que han sido automatizadas
(HW) equipos informáticos	directa o indirectamente los servicios que presta la organización,
(COM) Redes de comunica	comunicaciones contratados a terceros; pero siempre centrándose
(SI) Soportes de informaci	almacenar información de forma permanente o, al menos, durante
(AUX) Equipamento auxilia	a los sistemas de información, sin estar directamente relacionados
(L) Instalaciones	de información y comunicaciones.
(P) Personal	sistemas de información.

Fuente: libro II-MAGERIT- catálogo de elementos

Tabla 3. Listado de activos de información

Tipo	Descripción
(ESSENTIAL) Activos esenciales	(inf_T) Información tributaria
	(inf_G) Información de gestión admnistrativa
	(inf_D) Información de gestión documental
(S) servicios	(S_T) Servicios tributarios
	(S_A)Servicios de gestión administrativa
	(S_D)Servicios de gestión documental
	(idm) gestión de identidades y privilegios de los sistemas de información
	(internet) servicio de internet
	(sv_HD) Servicio de mesa de ayuda
(SW) aplicaciones	(SI _SI) Sistema de información integrado (Financiero, Proyecto, Gestion humana y Recursos físicos)
	(SI_GD) Sistema de gestión documental y PQRSD
	(SI_GT) Sistema de información tributaria
	(sf_HD) software de mesa de ayuda
	(dbms) sistema de gestión de bases de datos
	(av) antivirus
	(os_sv) sistema operativo
	(backup) sistema de backup
	(Fw) Software Firewall- proxy
(HW) Equipamiento informático (hardware)	(pc) Equipos de cómputo personal
	(hosts_ sv) Servidores
	(hosts_Das) DAS
	(switch) Switches administrables
	(router) Router
	(backup_T) Unidad de Tape backup
(COM) Redes de comunicaciones	(LAN) Red local
	(Intenet) Internet
(MEDIA) Soportes de información	(Tape) Cintas magnéticas
(AUX) Equipamento auxiliar	(Cab_es) Cableado estructurado
	(ups) Sistemas de alimentación ininterrumpida
	(planta) Planta eléctrica
	(Air) Equipos de aire acondicionado
	(mob) Mobiliario
(L) Instalaciones	(Edificio) Edificio central
(P) Personal	(Tec_Oper) Técnico Operativo
	(pu) Personal usuario

Fuente: Esta investigación

11.2.1.2. DEPENDENCIAS ENTRE ACTIVOS

Se establece la dependencia entre los activos, identificando la medida en que un activo superior impacta a otro activo inferior tras la materialización de una amenaza.

El análisis de dependencias de los activos de tipo ***Datos / Información*** se realiza con base a:

- Las aplicaciones que lo soporta.
- Los equipos que lo hospedan.
- El personal que tiene acceso

El análisis de dependencias de los activos de tipo ***Servicio*** se realiza con base a:

- Los datos que lo sustentan.
- Las aplicaciones que lo soportan.
- Los equipos que lo hospedan.
- El personal del que depende.
- Las redes de comunicaciones.

El análisis de dependencias de los activos de tipo ***Aplicaciones*** se realiza con base a:

- Los equipos que lo hospedan.
- El personal que tiene acceso

El análisis de dependencias de los activos de tipo ***Equipos Informáticos*** se realiza con base a:

- Las instalaciones que lo acogen.
- El personal que lo gestiona.

Las dependencias por cada uno de los activos de información es la siguiente:

Tabla 4. Dependencia entre activos

Tipo	Descripción	(inf_T)	(inf_G)	(inf_D)	(S_T)	(S_A)	(S_DS	(idm)	(internet)	(sv_HD)	(SI_SI)	(SI_GD)	(SI_GT)	(sf_HD)	(dbms)	(av)	(os_sv)	(backup)	(Fw)	(pc)	(hosts_ sv)	(hosts_Da	(switch)	(router)	(backup_T	(LAN)	(Tape)	(Cab_es)	(ups)	(planta)	(Air)	(mob)	(Edificio)	(Tec_Oper	(Pu)
(ESSENTIAL) Activos esenciales	(inf_T) Información tributaria							X					X		X	X	X	X			X				X		X						X	X
	(inf_G) Información de gestión admnistrativa							X			X				X	X	X	X			X				X		X						X	X
	(inf_D) Información de gestión documental							X				X			X	X	X	X			X				X		X						X	X
(S) servicios	(S_T) Servicios tributarios	X							X				X							X	X					X							X	X
	(S_A)Servicios de gestión administrativa		X								X									X	X					X							X	X
	(S_D)Servicios de gestión documental			X								X								X	X					x							X	X
	(idm) gestión de identidades y privilegios de los sistemas de información																																X		
	(internet) servicio de internet																		X							X									
	(sv_HD) Servicio de mesa de ayuda													X						x	X					X							X		
(SW) aplicaciones	(SI _SI) Sistema de información integrado (Financiero, Proyecto, Gestion humana y Recursos físicos)									X										x	X											X	X
	(SI_GD) Sistema de gestión documental y PQRSD									X										x	X											x	x
	(SI_GT) Sistema de información tributaria									X										x	X											X	X
	(sf_HD) software de mesa de ayuda																			x	X											X	X
	(dbms) sistema de gestión de bases de datos																				X											X		
	(av) antivirus																			X	X											X		
	(os_sv) sistema operativo																			X	X											X		
	(backup) sistema de backup																				X											X		
	(Fw) Software Firewall- proxy																				X											X		
(HW) Equipamiento informático (hardware)	(pc) Equipos de cómputo personal																															X	X	X
	(hosts_ sv) Servidores																					X										X	X	
	(hosts_Das) DAS																															X	X	
	(switch) Switches administrables																															X	X	
	(router) Router																															X	X	
	(backup_T) Unidad de Tape backup																															X	X	
(COM) Redes de comunicaciones	(LAN) Red local																						X				X	X	X	X	X	X	x	
	(Intenet) Internet																							X			X	x	X	x	X	X	x	
(MEDIA) Soportes de información	(Tape) Cintas magnéticas																															X	x	
(AUX) Equipamento auxiliar	(Cab_es) Cableado estructurado																															X	x	
	(ups) Sistemas de alimentación ininterrumpida																													X		X	x	
	(planta) Planta eléctrica																															X	x	
	(Air) Equipos de aire acondicionado																															X		
	(mob) Mobiliario																															X		
(L) Instalaciones	(Edificio) Edificio central																																	
(P) Personal	(Tec_Oper) Técnico Operativo																																	
	(Pu) Personal usuario																																	

Fuente: Esta investigación

11.2.1.3. VALORACIÓN DE ACTIVOS

Se determina en que dimensión es valioso el activo y el valor que tiene para la organización en que caso de sufrir destrucción. Como resultado se obtiene el informe ***Modelo de valor***.

La escala de valores que se manejará es la siguiente:

Tabla 5. criterio de valoración activos

Valor			Criterio
10	muy alto	MA	daño muy grave
7-9	alto	A	daño grave
4-6	medio	MA	daño importante
1-3	bajo	B	daño menor
0	despreciable	D	irrelevante a efectos prácticos

Fuente: Libro II- MAGERIT catálogo de elementos

Cada activo se valora con base a las dimensiones de [D] disponibilidad, [I] integridad de datos y [C] confidencialidad:

- Disponibilidad: Es el aseguramiento de que los activos que los usuarios autorizados tienen acceso cuando lo requieran a la información y sus activos asociados.

- Integridad: Es la garantía de la exactitud y completitud de la información y los métodos de su procesamiento.

- Confidencialidad: Es el aseguramiento de que la información es accesible sólo para aquellos autorizados a tener acceso.

Tabla 6. Valoración de los activos

Tipo	Descripción	DIMENSIONES		
		D	I	C
(ESSENTIAL) Activos esenciales	(inf_T) Información tributaria (1)	[9]	[7]	[6]
	(inf_G) Información de gestión admnistrativa (2)	[7]	[7]	[6]
	(inf_D) Información de gestión documental (3)	[7]	[7]	[6]
(S) servicios	(S_T) Servicios tributarios (4)	[9]		
	(S_A)Servicios de gestión administrativa (5)	[7]		
	(S_D)Servicios de gestión documental (6)	[7]		
	(idm) gestión de identidades y privilegios de los sistemas de información (7)	[7]		
	(internet) servicio de internet (8)	[7]		
	(sv_HD) Servicio de mesa de ayuda (9)	[5]		
(SW) aplicaciones	(SI _SI) Sistema de información integrado (Financiero, Proyecto, Gestion humana y Recursos físicos) (10)	[9]		
	(SI_GD) Sistema de gestión documental y PQRSD (11)	[7]		
	(SI_GT) Sistema de información tributaria (12)	[9]		
	(sf_HD) software de mesa de ayuda (13)	[4]		
	(dbms) sistema de gestión de bases de datos (14)	[9]		
	(av) antivirus (15)	[7]	[7]	
	(os_sv) sistema operativo (16)	[9]		
	(backup) sistema de backup (17)	[5]		
	(Fw) Software Firewall- proxy (18)	[9]	[9]	[9]
(HW) Equipamiento informático (hardware)	(pc) Equipos de cómputo personal (19)	[4]		
	(hosts_ sv) Servidores (20)	[9]	[9]	
	(hosts_Das) DAS (21)	[9]		
	(switch) Switches administrables (22)	[9]		
	(router) Router (23)	[9]		
	(backup_T) Unidad de Tape backup (24)	[5]		
(COM) Redes de comunicaciones	(LAN) Red local (25)	[9]	[9]	[9]
	(Intenet) Internet (26)	[9]		
(MEDIA) Soportes de información	(Tape) Cintas magnéticas (27)	[7]	[7]	[7]
(AUX) Equipamento auxiliar	(Cab_es) Cableado estructurado (28)	[7]		
	(ups) Sistemas de alimentación ininterrumpida (29)	[7]		
	(planta) Planta eléctrica (30)	[7]		
	(Air) Equipos de aire acondicionado (31)	[7]		
	(mob) Mobiliario (32)	[4]		
(L) Instalaciones	(Edificio) Edificio central (33)	[9]	[9]	
(P) Personal	(Tec_Oper) Técnico Operativo (34)	[5]		
	(pu) Personal usuario (35)	[7]		

Fuente: Esta investigación

Explicación de la valoración

(1)

6.pi1 - probablemente afecte gravemente a un grupo de individuos

5.lro - probablemente sea causa de incumplimiento de una ley o regulación

9.cei.c -causa de pérdidas económicas excepcionalmente elevadas

3.da -Probablemente cause la interrupción de actividades propias de la Organización

7.olm -Probablemente perjudique la eficacia o seguridad de la misión operativa o logística

3.adm - probablemente impediría la operación efectiva de una parte de la Organización

7.lg.b -Probablemente causaría una publicidad negativa generalizada por afectar gravemente a las relaciones con el público en general

(2)

6.pi1 - probablemente afecte gravemente a un grupo de individuos

5.lro - probablemente sea causa de incumplimiento de una ley o regulación

3.da -Probablemente cause la interrupción de actividades propias de la Organización

7.olm -Probablemente perjudique la eficacia o seguridad de la misión operativa o logística

7.adm -probablemente impediría la operación efectiva de la Organización

7.lg.b -Probablemente causaría una publicidad negativa generalizada por afectar gravemente a las relaciones con el público en general

(3)

4.pi1 probablemente afecte a un grupo de individuos

5.lro - probablemente sea causa de incumplimiento de una ley o regulación

3.da -Probablemente cause la interrupción de actividades propias de la Organización

7.olm -Probablemente perjudique la eficacia o seguridad de la misión operativa o logística

7.adm -probablemente impediría la operación efectiva de la Organización

7.lg.b -Probablemente causaría una publicidad negativa generalizada por afectar gravemente a las relaciones con el público en general

(4)

6.pi1 - probablemente afecte gravemente a un grupo de individuos

5.lro - probablemente sea causa de incumplimiento de una ley o regulación

9.cei.c -causa de pérdidas económicas excepcionalmente elevadas

3.da -Probablemente cause la interrupción de actividades propias de la Organización

7.olm -Probablemente perjudique la eficacia o seguridad de la misión operativa o logística

3.adm - probablemente impediría la operación efectiva de una parte de la Organización

7.lg.b -Probablemente causaría una publicidad negativa generalizada por afectar gravemente a las relaciones con el público en general

(5)

6.pi1 - probablemente afecte gravemente a un grupo de individuos

5.lro - probablemente sea causa de incumplimiento de una ley o regulación

3.da -Probablemente cause la interrupción de actividades propias de la Organización

7.olm -Probablemente perjudique la eficacia o seguridad de la misión operativa o logística

7.adm -probablemente impediría la operación efectiva de la Organización

7.lg.b -Probablemente causaría una publicidad negativa generalizada por afectar gravemente a las relaciones con el público en general

(6)

4.pi1 probablemente afecte a un grupo de individuos

5.lro - probablemente sea causa de incumplimiento de una ley o regulación

3.da -Probablemente cause la interrupción de actividades propias de la Organización

7.olm -Probablemente perjudique la eficacia o seguridad de la misión operativa o logística

7.adm -probablemente impediría la operación efectiva de la Organización

7.lg.b -Probablemente causaría una publicidad negativa generalizada por afectar gravemente a las relaciones con el público en general

(7)

4.pi1 - probablemente afecte a un grupo de individuos

5.lro - probablemente sea causa de incumplimiento de una ley o regulación

3.da - Probablemente cause la interrupción de actividades propias de la Organización

7.olm - Probablemente perjudique la eficacia o seguridad de la misión operativa o logística

(8)

6.pi1-probablemente afecte gravemente a un grupo de individuos

5.lro- probablemente sea causa de incumplimiento de una ley o regulación

7.cei.c-causa de graves pérdidas económicas

3.da-Probablemente cause la interrupción de actividades propias de la Organización

7.olm - Probablemente perjudique la eficacia o seguridad de la misión operativa o logística

1.adm - pudiera impedir la operación efectiva de una parte de la Organización

7.lg.b -Probablemente causaría una publicidad negativa generalizada por afectar gravemente a las relaciones con el público en general

(9)

4.pi1-probablemente afecte a un grupo de individuos

5.lro-probablemente sea causa de incumplimiento de una ley o regulación

3.da - Probablemente cause la interrupción de actividades propias de la Organización

(10)

6.pi1 - probablemente afecte gravemente a un grupo de individuos

5.lro - probablemente sea causa de incumplimiento de una ley o regulación

9.cei.c -causa de pérdidas económicas excepcionalmente elevadas

3.da -Probablemente cause la interrupción de actividades propias de la Organización

7.olm -Probablemente perjudique la eficacia o seguridad de la misión operativa o logística

3.adm - probablemente impediría la operación efectiva de una parte de la Organización

7.lg.b -Probablemente causaría una publicidad negativa generalizada por afectar gravemente a las relaciones con el público en general

(11)

4.pi1 probablemente afecte a un grupo de individuos

5.lro - probablemente sea causa de incumplimiento de una ley o regulación

3.da -Probablemente cause la interrupción de actividades propias de la Organización

7.olm -Probablemente perjudique la eficacia o seguridad de la misión operativa o logística

7.adm -probablemente impediría la operación efectiva de la Organización

7.lg.b -Probablemente causaría una publicidad negativa generalizada por afectar gravemente a las relaciones con el público en general

(12)

6.pi1 - probablemente afecte gravemente a un grupo de individuos

5.lro - probablemente sea causa de incumplimiento de una ley o regulación

9.cei.c -causa de pérdidas económicas excepcionalmente elevadas

3.da -Probablemente cause la interrupción de actividades propias de la Organización

7.olm -Probablemente perjudique la eficacia o seguridad de la misión operativa o logística

3.adm - probablemente impediría la operación efectiva de una parte de la Organización

7.lg.b -Probablemente causaría una publicidad negativa generalizada por afectar gravemente a las relaciones con el público en general

(13)

4.pi1-probablemente afecte a un grupo de individuos

(14)

6.pi1 - probablemente afecte gravemente a un grupo de individuos

5.lro - probablemente sea causa de incumplimiento de una ley o regulación

9.cei.c -causa de pérdidas económicas excepcionalmente elevadas

3.da -Probablemente cause la interrupción de actividades propias de la Organización

7.olm -Probablemente perjudique la eficacia o seguridad de la misión operativa o logística

3.adm - probablemente impediría la operación efectiva de una parte de la Organización

7.lg.b -Probablemente causaría una publicidad negativa generalizada por afectar gravemente a las relaciones con el público en general

(15)

6.pi1 - probablemente afecte gravemente a un grupo de individuos

3.da -Probablemente cause la interrupción de actividades propias de la Organización

7.olm -Probablemente perjudique la eficacia o seguridad de la misión operativa o logística

7.adm -probablemente impediría la operación efectiva de la Organización

(16)

6.pi1 - probablemente afecte gravemente a un grupo de individuos

5.lro - probablemente sea causa de incumplimiento de una ley o regulación

9.cei.c -causa de pérdidas económicas excepcionalmente elevadas

3.da -Probablemente cause la interrupción de actividades propias de la Organización

7.olm -Probablemente perjudique la eficacia o seguridad de la misión operativa o logística

3.adm - probablemente impediría la operación efectiva de una parte de la Organización

7.lg.b -Probablemente causaría una publicidad negativa generalizada por afectar gravemente a las relaciones con el público en general

(17)

5.lro-probablemente sea causa de incumplimiento de una ley o regulación

3.da -Probablemente cause la interrupción de actividades propias de la Organización

(18)

4.pi1-probablemente afecte a un grupo de individuos

3.da- Probablemente cause la interrupción de actividades propias de la Organización

9.olm-Probablemente cause un daño serio a la eficacia o seguridad de la misión operativa o logística

7.adm- probablemente impediría la operación efectiva de la Organización

(19)

4.pi1-probablemente afecte a un grupo de individuos

(20)

6.pi1 - probablemente afecte gravemente a un grupo de individuos

5.lro - probablemente sea causa de incumplimiento de una ley o regulación

9.cei.c -causa de pérdidas económicas excepcionalmente elevadas

3.da -Probablemente cause la interrupción de actividades propias de la Organización

7.olm -Probablemente perjudique la eficacia o seguridad de la misión operativa o logística

3.adm - probablemente impediría la operación efectiva de una parte de la Organización

7.lg.b -Probablemente causaría una publicidad negativa generalizada por afectar gravemente a las relaciones con el público en general

(21)

6.pi1 - probablemente afecte gravemente a un grupo de individuos

5.lro - probablemente sea causa de incumplimiento de una ley o regulación

9.cei.c -causa de pérdidas económicas excepcionalmente elevadas

3.da -Probablemente cause la interrupción de actividades propias de la Organización

7.olm -Probablemente perjudique la eficacia o seguridad de la misión operativa o logística

3.adm - probablemente impediría la operación efectiva de una parte de la Organización

7.lg.b -Probablemente causaría una publicidad negativa generalizada por afectar gravemente a las relaciones con el público en general

(22)

6.pi1 - probablemente afecte gravemente a un grupo de individuos

5.lro - probablemente sea causa de incumplimiento de una ley o regulación

9.cei.c -causa de pérdidas económicas excepcionalmente elevadas

3.da -Probablemente cause la interrupción de actividades propias de la Organización

7.olm -Probablemente perjudique la eficacia o seguridad de la misión operativa o logística

3.adm - probablemente impediría la operación efectiva de una parte de la Organización

7.lg.b -Probablemente causaría una publicidad negativa generalizada por afectar gravemente a las relaciones con el público en general

(23)

6.pi1-probablemente afecte gravemente a un grupo de individuos

5.lro- probablemente sea causa de incumplimiento de una ley o regulación

7.cei.c-causa de graves pérdidas económicas

3.da-Probablemente cause la interrupción de actividades propias de la Organización

7.olm - Probablemente perjudique la eficacia o seguridad de la misión operativa o logística

1.adm - pudiera impedir la operación efectiva de una parte de la Organización

7.lg.b -Probablemente causaría una publicidad negativa generalizada por afectar gravemente a las relaciones con el público en general

(24)

5.lro-probablemente sea causa de incumplimiento de una ley o regulación

3.da -Probablemente cause la interrupción de actividades propias de la Organización

(25)

6.pi1-probablemente afecte gravemente a un grupo de individuos

7.lro-probablemente cause un incumplimiento grave de una ley o regulación

1.si-pudiera causar una merma en la seguridad o dificultar la investigación de un incidente

7.cei.c-causa de graves pérdidas económicas

3.da-Probablemente cause la interrupción de actividades propias de la Organización

7.olm-Probablemente perjudique la eficacia o seguridad de la misión operativa o logística

7.adm-probablemente impediría la operación efectiva de la Organización

7.lg.b-Probablemente causaría una publicidad negativa generalizada por afectar gravemente a las relaciones con el público en general

(26)

6.pi1-probablemente afecte gravemente a un grupo de individuos

5.lro- probablemente sea causa de incumplimiento de una ley o regulación

7.cei.c-causa de graves pérdidas económicas

3.da-Probablemente cause la interrupción de actividades propias de la Organización

7.olm - Probablemente perjudique la eficacia o seguridad de la misión operativa o logística

1.adm - pudiera impedir la operación efectiva de una parte de la Organización

7.lg.b -Probablemente causaría una publicidad negativa generalizada por afectar gravemente a las relaciones con el público en general

(27)

5.lro-probablemente sea causa de incumplimiento de una ley o regulación

3.da -Probablemente cause la interrupción de actividades propias de la Organización

(28)

6.pi1-probablemente afecte gravemente a un grupo de individuos

7.lro-probablemente cause un incumplimiento grave de una ley o regulación

1.si-pudiera causar una merma en la seguridad o dificultar la investigación de un incidente

7.cei.c-causa de graves pérdidas económicas

3.da-Probablemente cause la interrupción de actividades propias de la Organización

7.olm-Probablemente perjudique la eficacia o seguridad de la misión operativa o logística

7.adm-probablemente impediría la operación efectiva de la Organización

7.lg.b-Probablemente causaría una publicidad negativa generalizada por afectar gravemente a las relaciones con el público en general

(29)

6.pi1-probablemente afecte gravemente a un grupo de individuos

7.lro-probablemente cause un incumplimiento grave de una ley o regulación

1.si-pudiera causar una merma en la seguridad o dificultar la investigación de un incidente

7.cei.c-causa de graves pérdidas económicas

3.da-Probablemente cause la interrupción de actividades propias de la Organización

7.olm-Probablemente perjudique la eficacia o seguridad de la misión operativa o logística

7.adm-probablemente impediría la operación efectiva de la Organización

7.lg.b-Probablemente causaría una publicidad negativa generalizada por afectar gravemente a las relaciones con el público en general

(30)

6.pi1-probablemente afecte gravemente a un grupo de individuos

7.lro-probablemente cause un incumplimiento grave de una ley o regulación

7.cei.c-causa de graves pérdidas económicas

3.da-Probablemente cause la interrupción de actividades propias de la Organización

7.olm-Probablemente perjudique la eficacia o seguridad de la misión operativa o logística

7.adm-probablemente impediría la operación efectiva de la Organización

7.lg.b-Probablemente causaría una publicidad negativa generalizada por afectar gravemente a las relaciones con el público en general

(31)

6.pi1-probablemente afecte gravemente a un grupo de individuos

7.cei.c-causa de graves pérdidas económicas

3.da-Probablemente cause la interrupción de actividades propias de la Organización

7.adm-probablemente impediría la operación efectiva de la Organización

(32)

4.pi1-probablemente afecte a un grupo de individuos

3.pi1-probablemente afecte a un individuo

(33)

6.pi1 - probablemente afecte gravemente a un grupo de individuos

5.lro - probablemente sea causa de incumplimiento de una ley o regulación

9.cei.c -causa de pérdidas económicas excepcionalmente elevadas

3.da -Probablemente cause la interrupción de actividades propias de la Organización

7.olm -Probablemente perjudique la eficacia o seguridad de la misión operativa o logística

3.adm - probablemente impediría la operación efectiva de una parte de la Organización

7.lg.b -Probablemente causaría una publicidad negativa generalizada por afectar gravemente a las relaciones con el público en general

(34)

4.pi1-probablemente afecte a un grupo de individuos

3.pi1-probablemente afecte a un individuo

5.lro-probablemente sea causa de incumplimiento de una ley o regulación

3.da -Probablemente cause la interrupción de actividades propias de la Organización

(35)

1.da-Pudiera causar la interrupción de actividades propias de la Organización

7.olm-Probablemente perjudique la eficacia o seguridad de la misión operativa o logística

Valor acumulado de los activos

Se calcula teniendo en cuenta las dependencias entre activos. Se define el valor acumulado como el mayor valor entre el propio y el de cualquiera de sus superiores.

Tabla 7. Valor acumulado de los activos

Tipo	Descripción	DIMENSIONES		
		D	I	C
(ESSENTIAL) Activos esenciales	(inf_T) Información tributaria	[9]	[7]	[6]
	(inf_G) Información de gestión admnistrativa	[7]	[7]	[6]
	(inf_D) Información de gestión documental	[7]	[7]	[6]
(S) servicios	(S_T) Servicios tributarios	[9]		
	(S_A)Servicios de gestión administrativa	[7]		
	(S_D)Servicios de gestión documental	[7]		
	(idm) gestión de identidades y privilegios de los sistemas de información	[9]		
	(internet) servicio de internet	[9]		
	(sv_HD) Servicio de mesa de ayuda	[9]	[9]	[9]
(SW) aplicaciones	(SI _SI) Sistema de información integrado (Financiero, Proyecto, Gestion humana y Recursos físicos)	[9]		
	(SI_GD) Sistema de gestión documental y PQRSD	[7]		
	(SI_GT) Sistema de información tributaria	[9]	[7]	[6]
	(sf_HD) software de mesa de ayuda	[9]	[9]	[9]
	(dbms) sistema de gestión de bases de datos	[9]	[7]	[6]
	(av) antivirus	[9]	[7]	[6]
	(os_sv) sistema operativo	[9]	[7]	[6]
	(backup) sistema de backup	[9]	[7]	[6]
	(Fw) Software Firewall- proxy	[9]	[9]	[9]
(HW) Equipamiento informático (hardware)	(pc) Equipos de cómputo personal	[9]	[9]	[9]
	(hosts_ sv) Servidores	[9]	[9]	[9]
	(hosts_Das) DAS	[9]	[9]	[9]
	(switch) Switches administrables	[9]	[9]	[9]
	(router) Router	[9]		
	(backup_T) Unidad de Tape backup	[9]	[7]	[6]
(COM) Redes de comunicaciones	(LAN) Red local	[9]	[9]	[9]
	(Intenet) Internet	[9]		
(MEDIA) Soportes de información	(Tape) Cintas magnéticas	[9]	[7]	[7]
(AUX) Equipamento auxiliar	(Cab_es) Cableado estructurado	[9]	[9]	[9]
	(ups) Sistemas de alimentación ininterrumpida	[9]		
	(planta) Planta eléctrica	[9]		
	(Air) Equipos de aire acondicionado	[9]		
	(mob) Mobiliario	[9]	[9]	[9]
(L) Instalaciones	(Edificio) Edificio central	[9]	[9]	[9]
(P) Personal	(Tec_Oper) Técnico Operativo	[9]	[9]	[9]
	(Pu) Personal usuario	[9]	[9]	[9]

Fuente: Esta investigación

IDENTIFICACIÓN Y VALORACION DE LAS AMENAZAS

Se realizó proceso de identificación de las amenazas por cada tipo de activo, basados en el Libro II catálogo de elementos MAGERIT.

Las amenazas son clasificadas de acuerdo a la siguiente relación

- De origen natural (N)
- Del entorno (I)
- Causadas por las personas de forma accidental (E)
- Causadas por las personas de forma deliberada(A)

La valoración de las amenazas se realizó por cada una de las dimensiones de seguridad en las que el activo es relevante: Disponibilidad, Integridad y Confidencialidad de acuerdo a la degradación y probabilidad.

Degradación: Valor en porcentaje que indica en cuanto puede perjudicarse una activo si se materializa la amenaza.
Probabilidad: Posibilidad de que se materialice la amenaza.

Para asignación de los valores a las amenazas se utilizaron las siguientes tablas:

Tabla 8. Degradación de los activos

Valor	Criterio
90% - 100%	Degradación muy considerable del activo
25% – 89%	Degradación medianamente considerable del activo
1% - 24%	Degradación poco considerable del activo

Fuente: Esta investigación

Tabla 9. Probabilidad de ocurrencia

Valor	
5	Muy alta
4	Alta
3	Media
2	Baja
1	Muy baja

Fuente: Esta investigación

Una vez valoradas las amenazas se justifican los valores dados a cada una de ellas de acuerdo a la probabilidad y la degradación.

Tabla 10. Valoración de las amenazas

Tipo de activo	Amenaza	Probabilidad	Degradación		
			D	I	C
(ESSENTIAL) Activos esenciales - Datos	[E.1] Errores de los usuarios	4	30%	100%	1%
	[E.2] Errores del administrador	1	90%	90%	1%
	[E.15] Alteración accidental de la información	1		90%	
	[E.19] Fugas de información	4			5%
	[A.5] Suplantación de la identidad del usuario	1	90%	90%	90%
	[A.15] Modificación deliberada de la información	1		90%	
	[A.18] Destrucción de información	1	100%		
(S) servicios	[E.24] Caída del sistema por agotamiento de recursos	2	90%		
	[A.18] Destrucción de información	1	60%		
	[A.24] Denegación de servicio	1	100%		
(SW) aplicaciones	[E.1] Errores de los usuarios	3	2%	2%	2%
	[E.2] Errores del administrador	1	90%	90%	90%
	[E.8] Difusión de software dañino	4	80%	30%	1%
	[E.21] Errores de mantenimiento / actualización de programas (software)	2	50%	30%	
	[A.6] Abuso de privilegios de acceso	2	1%	90%	5%
	[A.11] Acceso no autorizado	2	1%	90%	5%
(HW) Equipamiento informático (hardware)	[I.5] Avería de origen físico o lógico	2	10%		
	[I.7] Condiciones inadecuadas de temperatura o humedad	1	70%		
	[I.6] Corte del suministro eléctrico	1	100%		
	[E.2] Errores del administrador	1	90%	90%	1%
	[A.25] Robo	1	100%		5%
(COM) Redes de comunicaciones	[I.8] Fallo de servicios de comunicac	1	100%		
	[E.2] Errores del administrador	1	90%	1%	1%
	[E.24] Caída del sistema por agotamiento de recursos	2	90%		
	[A.7] Uso no previsto	5	80%	1%	1%
	[A.11] Acceso no autorizado	1		90%	1%
	[A.24] Denegación de servicio	1	100%		
(MEDIA) Soportes de información	[I.1] Fuego	1	100%		
	[N.7] Desastres naturales	1	100%		
(AUX) Equipamento auxiliar	[I.1] Fuego	1	100%		
	[N.7] Desastres naturales	1	100%		
(L) Instalaciones	[I.1] Fuego	1	100%		
	[N.7] Desastres naturales	1	100%		
	[I.*] Desastres industriales	1	100%		
(P) Personal	[E.28] Indisponibilidad del personal	3	100%		
	[A.30] Ingeniería social (picaresca)	3	20%	100%	5%

Fuente: Esta investigación

Tabla 11. Justificación amenazas Activos esenciales

Tipo de activo	Amenaza / Justificación	Dimensiones		
		D	I	C
(ESSENTIAL) Activos esenciales - Datos	[E.1] Errores de los usuarios: Se asigna el valor del 30% en la dimensión de disponibilidad teniendo en cuenta que los datos están relacionados directamente con los servicios prestados a través de los sistemas de información y pueden causar parálisis temporal en el servicio. La integridad del 100% indica que la información puede sufrir grandes daños. En la confidencialidad solo se asignó un 1% teniendo que la información es de caracter público	30%	100%	1%
	[E.2] Errores del administrador: Una incorrecta ejecución de un procedimiento por parte del administrador puede llevar a pérdida de información y afectar la disponiblidad, igualmente a modificar e insertar datos de forma errada afectando la integridad. La confidencialidad solamente se afecta en este porcentaje debido a que la información tiene caracter público.	90%	90%	1%
	[E.15] Alteración accidental de la información: Conlleva a modificar y eliminar de forma parcial o total un dato lo cual es bastante relevante para la integridad de la información.		90%	
	[E.19] Fugas de información: El mayor porcentaje de la información que se maneja en la administración municipal tiene carácter público, por lo cual puede ser conocida y comunicada al personal interno y externo			5%
	[A.5] Suplantación de la identidad del usuario: Afecta las tres dimensiones en alto porcentaje puesto que permite al atacante tener acceso a los datos y realizar sobre ellos cualquier operación que esté permitida para el usuario suplantado	90%	90%	90%
	[A.15] Modificación deliberada de la información: Afecta la integridad de los datos puesto que su valor no sería el correspondiente		90%	
	[A.18] Destrucción de información: No podrá ser accedida en el momento de requerirse lo cual afecta de forma completa la disponibilidad.	100%		

Fuente: Esta investigación

Tabla 12. Justificación amenazas Servicios

Tipo de activo	Amenaza / Justificación	Dimensiones		
		D	I	C
(S) servicios	[E.24] Caída del sistema por agotamiento de recursos: Teniendo en cuenta que los servicios son prestados a través de los sistemas de información, se genera una parálisis total en las operaciones de la gestión tributario y administrativa y de forma parcial en la gestión documental	90%		
	[A.18] Destrucción de información: No podrá ser accedida en el momento de requerirse, por lo cual el servicio podría afectarse de forma parcial para algunos servicios y total en otros	60%		
	[A.24] Denegación de servicio: Podría generar parálisis total en los servicios	100%		

Fuente: Esta investigación

Tabla 13. Justificación amenazas Aplicaciones

Tipo de activo	Amenaza / Justificación	Dimensiones		
		D	I	C
(SW) aplicaciones	[E.1] Errores de los usuarios: Es poco frecuente que sufran daños por uso de los usuarios finales.	2%	2%	2%
	[E.2] Errores del administrador: Un mal procedimiento en la ejecución de labores administrativaspuede afectar la disponibilidad y la integridad de las aplicaciones. Una inadeacuada administración de privilegios puede poner en riesgo la confidencialidad.	90%	90%	90%
	[E.8] Difusión de software dañino: Los daños ocasionados por virus y malware pueden dejar por fuera de servicio las aplicaciones afectando la disponibilidad. Podría ocasionars pérdida de documentos afectando la integridad.	80%	30%	1%
	[E.21] Errores de mantenimiento / actualización de programas (software):Un procedimiento errado en el proceso de actualizaciones o labores de mantenimiento puede afectar la disponibilidad y la integridad del software.	50%	30%	
	[A.6] Abuso de privilegios de acceso: La falta de trazabilidad de algunas aplicaciones puede contribuir a que se de el uso abusivo de las aplicaciones poniendo en riesgo la integridad de la información.	1%	90%	5%
	[A.11] Acceso no autorizado: El acceso no autorizado a las aplicaciones generalmente se da con el objeto de realizar modificaciones, inserciones o eliminación de los datos	1%	90%	5%

Fuente: Esta investigación

Tabla 14. Justificación amenazas Equipamiento informático

Tipo de activo	Amenaza / Justificación	Dimensiones		
		D	I	C
(HW) Equipamiento informático (hardware)	[I.5] Avería de origen físico o lógico: El daño parcial o total del hardware conlleva a que no esté disponible mientras se genera su reparación o cambio.	10%		
	[I.7] Condiciones inadecuadas de temperatura o humedad: Algunos equipos tiene funcionamiento 7/24 por lo cual pueden sufrir sobrecaliento y daño en sus componentes electrónicos haciendo necesario permanecer en condiciones específicas de temperatura para su correcto funcionamiento.	70%		
	[I.6] Corte del suministro eléctrico: Una interrupción prolongada en el servicio del fluido eléctrico podría dejar por fuera de operación los equipos informáticos	100%		
	[E.2] Errores del administrador: Una inadecuada instalación y manipulación de los equipos informáticos podría ocasionar daños dejándolos sin servicio y a su vez ocasionar pérdida o daño en la información	90%	90%	1%
	[A.25] Robo: Representa un total indisponibilidad del dispositivo o equipo informático. Para el caso de los equipos de cómputo personal representa una pérdida de confidencialidad de los datos almacenados en el al ser accedidos por terceras personas.	100%		5%

Fuente: Esta investigación

Tabla 15. Justificación amenazas Redes de comunicaciones

Tipo de activo	Amenaza / Justificación	Dimensiones		
		D	I	C
(COM) Redes de comunicaciones	[I.8] Fallo de servicios de comunicaciones: Un fallo en un componente puede dejar sin funcionamiento la Red Lan, lo cual es muy significativo puesto que afecta todos los servicios y sistemas de información.	100%		
	[E.2] Errores del administrador: Una inadecuada instalación, manipulación y/o configuración de los dispositivos que conforman la red LAN podría ocasionar indisponibilidad en el servicio	90%	1%	1%
	[E.24] Caída del sistema por agotamiento de recursos : Puede existir un aumento en el tráfico de la red o sobreutilización del canal de internet ocasionando bajo rendimiento de las comunicaciones o su parálisis total.	90%		
	[A.7] Uso no previsto : La utilización del internet para fines personales afecta el desempeño de los aplicativos web con salida a internet	80%	1%	1%
	[A.11] Acceso no autorizado: Este ataque puede perpetuarse para modificación, eliminación o borrado de datos o para causar daños en la prestación de los servicios.		90%	1%
	[A.24] Denegación de servicio: Pueden ser ocasionados por accesos no autorizados a la red de comunicaciones	100%		

Fuente: Esta investigación

Tabla 16. Justificación amenazas soportes de información

Tipo de activo	Amenaza / Justificación	Dimensiones		
		D	I	C
(MEDIA) Soportes de información	[I.1] Fuego : En caso de incendio podrían llegar a ser destruidos los medios existentes al interior del edificio, puesto que no tienen protección contra fuego	100%		
	[N.7] Desastres naturales: Podrían afectar las edificaciones y los medios considerando que se encuentran al interior del edificio	100%		

Fuente: Esta investigación

Tabla 17. Justificación amenazas equipamiento auxiliar

Tipo de activo	Amenaza / Justificación	Dimensiones		
		D	I	C
(AUX) Equipamento auxiliar	[I.1] Fuego : En caso de incendio podrían llegar a ser destruídos por encontrarse al interior del edificio	100%		
	[N.7] Desastres naturales: Podrían afectar las edificaciones y los medios considerando que se encuentran al interior del edificio	100%		

Fuente: Esta investigación

Tabla 18. Justificación amenazas Instalaciones

Tipo de activo	Amenaza / Justificación	Dimensiones		
		D	I	C
(L) Instalaciones	[I.1] Fuego: Puede dejar sin operación el edificio de forma parcial o total y destruir la infraestructura tecnológica	100%		
	[N.7] Desastres naturales: Puede dejar sin operación el edificio de forma parcial o total	100%		
	[I.*] Desastres industriales :Puede dejar sin operación el edificio de forma parcial o total	100%		

Fuente: Esta investigación

Tabla 19. Justificación amenazas personal

Tipo de activo	Amenaza / Justificación	Dimensiones		
(P) Personal	[E.28] Indisponibilidad del personal: Existen procesos fundamentes que solamente son conocidos y operados por una sola persona, la cual al ausentarse genera parálisis en los servicios	100%		
	[A.30] Ingeniería social (picaresca): No existe una concienciación de los usuarios acerda de este tipo de amenza y la gravedad de sus consecuencias, las cuales según los intereses mas frecuentes, están enfocados hacia alteración de información.	20%	100%	5%

Fuente: Esta investigación

11.2.2. DETERMINACION DE LOS SALVAGUARDAS Y SU EFICACIA

En esta fase se identificaron las contramedidas tecnológicas que existen en la organización para mitigar los riesgos y cuan eficaces resultan para contrarrestar las amenazas. Los salvaguardas fueron tomados del Libro II Catálogo de elementos – MAGERIT.

Tabla 20. Salvaguardas

Tipo	Descripción	Dimensiones			Evaluación
		D	I	C	
(ESSENTIAL) Activos esenciales	Identificación y autenticación	x	x	x	60%
	Protecciones Generales	x	x	x	80%
	Copias de seguridad de los datos (backup)	x	x		50%
	Aseguramiento de la integridad		x		80%
(S) servicios	Gestión de cambios (mejoras y sustituciones)	x			80%
	Protecciones Generales	x			80%
	Se aplican perfiles de seguridad	x			60%
(SW) aplicaciones	Se aplican perfiles de seguridad	x	x	x	60%
	Cambios (actualizaciones y mantenimiento)	x	x	x	75%
(HW) Equipamiento informático	Protecciones Generales	x			90%
	Cambios (actualizaciones y mantenimiento)	x	x		90%
(COM) Redes de comunicaciones	Protecciones Generales	x			90%
	Internet: uso de ? acceso a	x			80%
	Sistema de protección perimetral	x			90%
(MEDIA) Soportes de información	Aseguramiento de la disponibilidad	x			70%
(AUX) Equipamento auxiliar	Climatización	x			90%
(L) Instalaciones	Control de los accesos físicos	x			90%
(P) Personal	Formación y concienciación	x	x	x	40%
	Gestión del Personal	x			70%

Fuente: Esta investigación

Descripción de los salvaguardas

- **Identificación y autenticación:** Para acceder a los servicios informáticos se requiere identificación mediante usuario y autenticarse con contraseñas. Para los usuarios finales, el primer proceso de identificación y autenticación se realiza en el servidor de dominio y posteriormente en las aplicaciones y clientes de correo. Los usuarios administradores de los sistemas y recursos, poseen también identificaciones únicas para acceder a los recursos. Existen políticas de seguridad de contraseñas de carácter obligatorio aplicado en el de servidor de dominio, tales como uso de mayúsculas, minúsculas y números, cambio periódico y vencimiento.

- **Protecciones generales:** Existen procedimientos de forma transversal para la autorización de acceso a los dispositivos informáticos y sistemas de información, los cuales se encuentran documentados y son conocidos por toda la organización. Los sistemas de información cuentan con registro de transacciones. Existen políticas para el ingreso y retiro de equipos de cómputo del edificio. Se cuenta con planta eléctrica y ups de respaldo. Existen extintores contra incendio. El edificio cuenta con cámaras de seguridad y servicio de vigilancia para controlar el acceso de personal externo.

- **Copias de seguridad de los datos (backup):** Se ejecuta procedimiento periódico de copias de seguridad de la información relevante para la organización. Los backups se guardan en cintas magnéticas, las cuales son almacenadas algunas en las instalaciones del edificio central y otras son enviadas a un repositorio externo contratado por la entidad.

- **Aseguramiento de la integridad:** Para asegurar la integridad de la información las aplicaciones poseen procedimientos de confirmación, aprobación y autorización de cambios en los datos relevantes. Igualmente existen registros de auditoría que

permiten verificar el dato antes y después de modificación, y el usuario responsable de la modificación.

- **Gestión de cambios (mejoras y sustituciones):** La alcaldía Municipal de Tuluá lleva a cabo durante cada vigencia planes de mejoramiento de la infraestructura tecnológica de software, hardware y servicios como resultado de las evaluaciones internas y de las fallas reportadas.

- **Se aplican perfiles de seguridad:** A nivel de los servicios y aplicaciones se utilizan perfiles de usuario. Para los usuarios operadores del sistema los perfiles varían de acuerdo a los roles que desempeña cada uno en su puesto de trabajo. Existen perfiles de solo consulta e informes para los usuarios que ejercen funciones de control o gerenciales y existe los usuarios administradores quienes son los que poseen todos los privilegios. Los perfiles son aprobados por el jefe inmediato del proceso mediante formato de solicitud de acceso.

- **Cambios (actualizaciones y mantenimiento):** Para el caso de las aplicaciones, estas son frecuentemente actualizadas a la última versión estable liberada. Para las aplicaciones a la medida como el sistema de gestión tributaria, sistema de gestión integrado y sistema de gestión documental, se ejecutan contratos de soporte, mantenimiento, y actualización para la vigencia. Las contrataciones están sujetas a las aprobaciones presupuestales, razón por la cual, en algunas ocasiones el proceso es lento y ocasiona que los primeros meses del año no se cuente con el servicio otorgado por el proveedor del sistema impactando a los procesos. Anualmente se elabora la planificación del mantenimiento preventivo del equipamiento informático, no obstante su ejecución está sujeta a la disponibilidad de personal para realizar los mantenimientos y cumplir con los cronogramas establecidos.

- **Internet: uso de ? acceso a:** Existen políticas de utilización del servicio de internet. Se cuenta con sistemas de filtrado mediante firewall y proxy. Para la administración de los accesos a sitios web y horarios se tiene en cuenta las labores desempeñadas por los usuarios, pero falta un poco de cultura organizacional para la utilización del recurso.

- **Sistema de protección perimetral:** Las instalaciones del Departamento de tecnología y centros de datos cuentan con barreras de acceso tales como puertas, rejas y paredes en vidrio. Las chapas se encuentran en buenas condiciones y existen sistemas de autenticación dactilar.

- **Aseguramiento de la disponibilidad:** Los medios de copia de seguridad son almacenados algunos en repositorio del departamento de tecnología y otros en repositorio externo contratado por la entidad. Se lleva un control sobre los medios recibidos y entregados al personal encargado del transporte y almacenamiento externo.

- **Climatización:** Existen equipos de aire acondicionado para controlar la temperatura, considerando que los servidores y algunos dispositivos de equipamiento auxiliar permanecen encendidos 24 horas al día, 365 días del año.

- **Control de los accesos físicos:** Las instalaciones del Departamento de tecnología y centros de datos se encuentran protegidos por barreras de acceso y su ingreso es controlado mediante autenticación de huella dactilar. El acceso a centros de cableado, dispositivos de red y servidores está limitado al administrador de la red y para quienes sean autorizados. Existen espacios adecuados para la atención del personal visitante.

- **Formación y concienciación:** Existen planes de capacitación y formación de personal pero estos no son específicos para el área de tecnología y seguridad informática. El personal de tecnología no recibe capacitaciones de actualización. El usuario final no es consciente de las amenazas por ingeniería social.

- **Gestión del Personal:** Para suplir las necesidades de los procesos y que no alcanzan a ser cubiertos con el personal de planta, se realiza contratación de personal adicional.

11.2.2.1. VULNERABILIDADES

- **Contraseñas:** Las políticas de seguridad de contraseñas solamente son aplicadas para autenticarse en el servidor de dominio. Para los demás aplicativos no existen políticas que obligue al usuario a cambiar sus contraseñas periódicamente o que cumplan con los requisitos mínimos de complejidad.

- **Perfiles de usuario:** Dentro de los procedimientos internos del área de tecnología, se encuentra definido y documentada la actividad de denegación de privilegios por movimiento de personal o ausencia temporal o definitiva para el personal de planta. Sin embargo el usuario administrador del sistema no es notificado de las terminaciones de contrato del personal contratista para la denegación de accesos a los sistemas, quedando perfiles activos de usuarios que ya no laboran en la entidad o que han sido nuevamente contratados con labores diferentes.

- **Protecciones generales:** Existe poco conocimiento por parte de los funcionarios sobre el uso de extintores contra incendio y los existentes no son revisados con la frecuencia que indican las normas técnicas de seguridad.

- **Copias de seguridad:** No se realiza periódicamente el procedimiento de restauración de copias de seguridad para verificar su estado y calidad.

- **Aseguramiento de la disponibilidad de medios:** Los medios que se almacenan en el Departamento de Tecnología no cuentan con las protecciones suficientes contra personal interno tal como gavetas con seguridad o cajas fuertes.
- **Cambios y mantenimiento:** Los mantenimientos y cambios del equipamiento están sujetos a los procesos de contratación y estos a su vez a la disponibilidad presupuestal, por lo cual se hacen un poco lentos.

- **Formación:** El personal del área de tecnología no recibe por parte de la entidad capacitaciones para actualizar sus conocimientos en la disciplina de la informática, ni en seguridad. Los usuarios del sistema no son capacitados ni concientizados sobre la ingeniería social y sus consecuencias.

- **Internet:** No se cuenta con un proveedor de internet ISP alternativo en caso de fallas en el canal principal.

- **Equipos de Respaldo:** No se cuenta con equipos de hardware o equipos auxiliares para el respaldo en caso de daños físicos o lógicos.

- **Recuperación:** A pesar de que existe plan de contingencia, este no es conocido por todos los responsables del proceso. No se cuenta con plan de recuperación de desastres.

11.2.3. ESTIMACION DEL ESTADO DEL RIESGO

11.2.3.1. ESTIMACIÓN DEL IMPACTO

Se determina el impacto potencial y el impacto residual al que está sometido el sistema.

Impacto potencial: Es al que se expone el sistema teniendo en cuenta el valor de los activos y la valoración de las amenazas sin tener en cuenta las salvaguardas.

Impacto Residual: Es al que se expone el sistema teniendo en cuenta el valor de los activos, la valoración de las amenazas y la eficacia de las salvaguardas.

Se tomaron los siguientes valores para su medición:

- MB: muy bajo
- B: bajo
- M: medio
- A: alto
- MA: muy alto

Tabla 21. Impacto

Impacto		Degradación		
		0% - 24%	25% - 89%	90% - 100%
Valor del activo	MA (9-10)	M	A	MA
	A (7-8)	M	A	A
	M (4-6)	B	M	M
	B (2-3)	MB	B	B
	MB (0-1)	MB	MB	MB

Fuente: Esta investigación

Tabla 22. Valor del impacto potencial y residual

Tipo de activo	Amenaza	Impacto Potencial			Impacto Residual		
		D	I	C	D	I	C
(ESSENTIAL) Activos esenciales - Datos	[E.1] Errores de los usuarios						
	[E.2] Errores del administrador						
	[E.15] Alteración accidental de la información						
	[E.19] Fugas de información						
	[A.5] Suplantación de la identidad del usuario						
	[A.15] Modificación deliberada de la información						
	[A.18] Destrucción de información						
(S) servicios	[E.24] Caída del sistema por agotamiento de recursos						
	[A.18] Destrucción de información						
	[A.24] Denegación de servicio						
(SW) aplicaciones	[E.1] Errores de los usuarios						
	[E.2] Errores del administrador						
	[E.8] Difusión de software dañino						
	[E.21] Errores de mantenimiento / actualización de programas (software)						
	[A.6] Abuso de privilegios de acceso						
	[A.11] Acceso no autorizado						
(HW) Equipamiento informático (hardware)	[I.5] Avería de origen físico o lógico						
	[I.7] Condiciones inadecuadas de temperatura o humedad						
	[I.6] Corte del suministro eléctrico						
	[E.2] Errores del administrador						
	[A.25] Robo						
(COM) Redes de comunicaciones	[I.8] Fallo de servicios de comunicaciones						
	[E.2] Errores del administrador						
	[E.24] Caída del sistema por agotamiento de recursos						
	[A.7] Uso no previsto						
	[A.11] Acceso no autorizado						
	[A.24] Denegación de servicio						
(MEDIA) Soportes de información	[I.1] Fuego						
	[N.7] Desastres naturales						
(AUX) Equipamento auxiliar	[I.1] Fuego						
	[N.7] Desastres naturales						
(L) Instalaciones	[I.1] Fuego						
	[N.7] Desastres naturales						
	[I.*] Desastres industriales						
(P) Personal	[E.28] Indisponibilidad del personal						
	[A.30] Ingeniería social (picaresca)						

Fuente: Esta investigación

11.2.3.2. ESTIMACIÓN DEL RIESGO

Se determina el riesgo potencial y el riesgo residual al que está sometido el sistema.

Riesgo potencial: Es al que se expone el sistema teniendo en cuenta el valor de los activos y la valoración de las amenazas sin tener en cuenta las salvaguardas.

Riesgo Residual: Es al que se expone el sistema teniendo en cuenta el valor de los activos, la valoración de las amenazas y la eficacia de las salvaguardas.

Se tomaron las siguientes escalas para su medición:

Tabla 23. Escalas cualitativas

Escalas		
Impacto	**Probabilidad**	**Riesgo**
MA: muy alto	**MA:** prácticamente seguro	**MA:** crítico
A: alto	**A:** probable	**A:** importante
M: medio	**M:** posible	**M:** apreciable
B: bajo	**B:** poco probable	**B:** bajo
MB: muy bajo	**MB:** muy raro	**MB:** despreciable

Fuente: Libro III – MAGERIT-Guía de técnicas

Tabla 24. Criterios para estimación del riesgo

RIESGO		IMPACTO				
		MA	**A**	**M**	**B**	**MB**
PROBABILIDAD	**MB**	A	M	B	MB	MB
	B	MA	A	M	B	MB
	M	MA	A	M	B	MB
	A	MA	MA	A	M	B
	MA	MA	MA	A	M	B

Fuente: Esta investigación

Tabla 25. Valor del riesgo potencial y residual

Tipo de activo	Amenaza	Probabilidad	Riesgo Potencial			Riesgo Residual		
			D	I	C	D	I	C
(ESSENTIAL) Activos esenciales - Datos	[E.1] Errores de los usuarios	A	MA	MA	A	MA	MA	A
	[E.2] Errores del administrador	MB	A	MA	B	A	M	B
	[E.15] Alteración accidental de la información	MB		A			B	
	[E.19] Fugas de información	A			A		B	
	[A.5] Suplantación de la identidad del usuario	MB	A	A	A	M	M	M
	[A.15] Modificación deliberada de la información	MB		A			M	
	[A.18] Destrucción de información	MB		M			M	
(S) servicios	[E.24] Caída del sistema por agotamiento de recursos	B	MA			M		
	[A.18] Destrucción de información	MB	M			M		
	[A.24] Denegación de servicio	MB	A			A		
(SW) aplicaciones	[E.1] Errores de los usuarios	M	M	M	M	MB	MB	MB
	[E.2] Errores del administrador	MB	A	A	A	A	A	A
	[E.8] Difusión de software dañino	A	MA	MA	A	A	A	
	[E.21] Errores de mantenimiento / actualización de programas (software)	B	A	A		M	M	
	[A.6] Abuso de privilegios de acceso	B	M	MA	M		A	M
	[A.11] Acceso no autorizado	B	M	MA	M		A	M
(HW) Equipamiento informático (hardware)	[I.5] Avería de origen físico o lógico	B	M			M		
	[I.7] Condiciones inadecuadas de temperatura o humedad	MB	A			B		
	[I.6] Corte del suministro eléctrico	MB	A			B		
	[E.2] Errores del administrador	MB	A	A	B	B	B	
	[A.25] Robo	MB	A		B	B		
(COM) Redes de comunicaciones	[I.8] Fallo de servicios de comunicaciones	MB	A			B		
	[E.2] Errores del administrador	MB	A	A	A	B		
	[E.24] Caída del sistema por agotamiento de recursos	B	MA			M		
	[A.7] Uso no previsto	MA	MA	A	A	A		
	[A.11] Acceso no autorizado	MB		A	B		B	
	[A.24] Denegación de servicio	MB	A			B		
(MEDIA) Soportes de información	[I.1] Fuego	MB	A	M	M	A	M	M
	[N.7] Desastres naturales	MB	A	M	M	A	M	M
(AUX) Equipamento auxiliar	[I.1] Fuego	MB	A			B		
	[N.7] Desastres naturales	MB	A			A		
(L) Instalaciones	[I.1] Fuego	MB	A			A		
	[N.7] Desastres naturales	MB	A			A		
	[I.*] Desastres industriales	MB	A			A		
(P) Personal	[E.28] Indisponibilidad del personal	M	MA	MA	MA	A	MA	MA
	[A.30] Ingeniería social (picaresca)	M	M	MA	M	M	A	M

Fuente: Esta investigación

11.3. GESTION DEL RIESGO

11.3.1. EVALUACION

11.3.1.1. INTERPRETACIÓN DE LOS VALORES DE IMPACTO Y RIESGO RESIDUALES

El Impacto y riesgo residual son el resultado de la medición de la seguridad en el estado actual. Están calculados considerando el efecto de las salvaguardas existentes.

Para interpretar el resultado se tendrá en cuenta el siguiente análisis:

- Si el valor residual es igual al valor potencial, significan que las salvaguardas existentes no realizan ningún aporte a la seguridad, y existen elementos fundamentales sin hacer.

- Si el valor residual es aceptable significa que la salvaguarda es adecuada. Esto no quiere decir descuidar la guardia; pero si afrontar el día con cierta confianza.

- Mientras el valor residual sea más que despreciable, hay una cierta exposición.

El análisis no debe comprender solamente el valor numérico del impacto y riesgo residual, sino que para su correcta interpretación debe venir acompañado de la relación de lo que se debería hacer y no se ha hecho. Los responsables de la toma de decisiones deberán prestar cuidadosa atención a esta relación de tareas pendientes, es decir de las vulnerabilidades o insuficiencias detectadas.

11.3.1.2. RIESGOS QUE PRESENTAN MAYOR IMPACTO Y PROBABILIDAD DE OCURRENCIA

De acuerdo a los resultados obtenidos durante el análisis, los riesgos de mayor relevancia para la entidad son los siguientes:

Activos esenciales – Datos

1. Errores cometidos por los usuarios internos: Por parte de los sistemas de información, existen controles que permiten validar el tipo de dato almacenado, sin embargo no se realiza análisis y control de la calidad de la información ingresada a los sistemas de información.

2. Existen un alto riesgo de que el usuario administrador del sistema, en la manipulación o procesamiento de las bases de datos cometa errores que impacten en la disponibilidad de los datos y servicios. No se han tomado medidas por parte de la entidad para mitigar este riesgo.

Servicios

3. A pesar de que existen controles de identificación y autenticación mediante usuarios y contraseñas, no existen para todos los sistemas medidas de seguridad que obliguen al cumplimiento de políticas de contraseñas seguras. Los sistemas de autenticación presentan vulnerabilidades.

4. Existe un riesgo catalogado como alto, de sufrir un ataque de denegación del servicio, el cual puede sobrevenir por personal interno o externo que se conecte de forma ilegítima a la red de datos. Existe una vulnerabilidad de acceso a los sistemas informáticos a través de algunas de las subredes. No se han implementado controles para prevenir este tipo de ataque.

Aplicaciones

5. Los errores no intencionados por parte del administrador son considerados de tipo Alto, teniendo en cuenta que no existen servidores de pruebas que permitan ejecutar procedimientos de actualizaciones o cambios en el sistema, antes de ser ejecutados en los sistemas de producción, lo cual puede impactar la disponibilidad y la integridad de las aplicaciones de software.

6. A pesar de contar con herramienta antivirus y filtrado de páginas web visitadas, se presentan eventos de virus informáticos que afectan el rendimiento de las aplicaciones y ocasionan daños en archivos necesarios para el funcionamiento del sistema. Se encuentra que muchos de los virus son ingresados mediante el uso de medios extraíbles por parte de los usuarios.

7. Teniendo en cuenta que el procedimiento de accesos y privilegios a los sistemas de información presenta debilidades en cuenta a la gestión de roles del personal contratista, se genera desactualización de dichos perfiles y se evidencian usuarios con perfiles de acceso que no corresponden y que podrían utilizar el sistema para fines diferentes a los cuales se les ha contratado. Se puede originar el abuso de privilegios del sistema y acceso no autorizado.

Red de comunicaciones

8. La entidad cuenta con una herramienta firewall y proxy para evitar el uso no previsto del servicio de internet, sin embargo las políticas de uso no están claras y no se encuentran documentas, por lo cual es subjetiva su utilización.

Soportes de información

9. En caso de presentarse fuego o desastre natural existe un riesgo de pérdida o daño de las cintas magnéticas de copia de seguridad puesto que no se encuentran protegidas o almacenadas en repositorios contra fuego, impacto, temperatura y humedad.

Equipamiento auxiliar e instalaciones

10. Existe un riesgo alto en cuanto a los daños por incendio, considerando que los extintores no son verificados de forma periódica y se encuentran vencidos. Adicionalmente el personal no conoce sobre su uso. No se cuenta con sensores de humo.

11. Los desastres naturales, aunque no son muy frecuentes, su impacto puede llevar a ser catastrófico, razón por la cual se considera como un riesgo alto.

Personal

12. Algos procesos solo son conocidos por una sola persona, y cuando se ausenta por alguna razón, se genera parálisis temporal en el servicio.

13. No existe conocimiento por parte del personal sobre las técnicas de ingeniería social y frecuentemente se evidencia mal uso de usuarios y contraseñas, los apuntan en lugares visibles, las dan a conocer al personal de soporte técnico o las prestan a otros usuarios.

11.3.2. TRATAMIENTO

Una vez terminado la evaluación anterior se pueden evidenciar los riesgos a los que está expuesta la organización. La alta dirección determinará el plan de seguridad a seguir considerando los siguientes aspectos:

- cumplimiento de obligaciones
- Beneficios derivados de una actividad que incluye riesgos
- Factores técnicos, económicos, culturales, políticos, etc.
- Equilibrio con otros tipos de riesgos

El tipo del tratamiento que se le puede dar a los riesgos es el siguiente:

Eliminación: Cuando el riesgo no es aceptable se elimina la fuente que lo genera.

Mitigación: Se reduce la degradación o la probabilidad de ocurrencia de la amenaza mediante la implementación o mejora de las salvaguardas.

Compartición: Se refiere a transferir el riesgo de forma parcial o total.

Financiación: Consiste en la aceptación del riesgo, para lo cual la entidad reservará presupuesto en caso de que la amenaza se materialice.

Se recomienda el siguiente tratamiento para los riesgos identificados en el presente análisis:

Tabla 26. Tratamiento de los riesgos

Tratamiento	Riesgos
Eliminación	5, 9, 12
Mitigación	1 ,2, 3, 4, 6, 7, 8, 10 ,13
Compartición	10, 11
Financiación	

Fuente: Esta investigación

12. POLITICAS DE SEGURIDAD

Con el objeto de mejorar el nivel de seguridad de la información de la Alcaldía Municipal de Tuluá, se definen las siguientes políticas que permiten mitigar los riesgos 1, 2, 3, 4, 6, 7, 8, 10 y 13 identificados en el punto anterior del presente documento:

Información

- Se llevará a cabo la clasificación de la información de las bases de datos teniendo en cuenta las tres características de la información en las cuales se basa la seguridad: confidencialidad, integridad y disponibilidad.

Recurso Humano

- Se deberán especificar las responsabilidades en materia de seguridad en la etapa de reclutamiento de personal e incluirlas en los manuales de funciones o documentos contractuales y verificar su cumplimiento durante el desempeño como empleado o contratista.

- Establecer Compromisos de Confidencialidad con todo el personal y usuarios externos de las instalaciones de procesamiento de información.

- Establecer las herramientas y mecanismos necesarios para promover la comunicación de debilidades existentes en materia de seguridad, así como de los incidentes ocurridos, con el objeto de minimizar sus efectos y prevenir su reincidencia.

- Garantizar que el personal del Departamento de Tecnología estén al corriente de las amenazas e incumbencias en materia de seguridad de la información, y se encuentren capacitados para respaldar la Política de Seguridad del Organismo en el transcurso de sus tareas normales.
- Dentro de los planes de capacitación de la entidad se deberá incluir capacitaciones de actualización para los funcionarios del área de tecnología.
- Todos los empleados y contratistas de la alcaldía, recibirán una adecuada capacitación y actualización periódica en materia de la política, normas y procedimientos de la entidad. Esto comprende los requerimientos de seguridad y las responsabilidades legales, así como la capacitación referida al uso correcto de las

instalaciones de procesamiento de información y el uso correcto de los recursos en general, como por ejemplo su estación de trabajo, utilización de dispositivos de almacenamiento entre otros.

Accesos

- Cuando se produzcan eventos de desvinculación, el empleado saliente deberá hacer entrega de los activos asignados, se deberá dejar evidencia documentada de la entrega y se comunicará al Departamento de Tecnología. Esta medida aplica para personal de planta y contratistas.

- Se revisarán los derechos de acceso de un usuario a los activos asociados con los sistemas y servicios de información tras la desvinculación, esto determinará si es necesario remover los derechos de acceso.

- Con el cambio de un empleo deben removerse todos los derechos de acceso que no fueron aprobados para el nuevo empleo, comprendiendo esto accesos lógicos y físicos, llaves, tarjetas de identificación, instalaciones de procesamiento de la información, suscripciones, y remoción de cualquier documentación que lo identifique como un miembro de la entidad.

- Si un empleado, contratista o usuario que se está desvinculando tiene conocimiento de contraseñas para cuentas que permanecen activas, éstas deben ser cambiadas tras la finalización o cambio de empleo.

- Utilizar identificadores de usuario únicos, de manera que se pueda identificar a los usuarios por sus acciones evitando la existencia de múltiples perfiles de acceso para un mismo empleado. El uso de identificadores grupales sólo debe ser permitido cuando sean convenientes para el trabajo a desarrollar debido a razones operativas.
- Se deberá Verificar que el usuario tiene autorización del Propietario de la Información para el uso del sistema, base de datos o servicio de información. Quien autorice mediante formato de solicitud de acceso deberá ser el responsable directo de la información.
- Se deberán entregar a los usuarios un detalle escrito de sus derechos de acceso y se requerirá que firmen declaraciones señalando que comprenden y aceptan las condiciones para el acceso.

- Se efectuarán revisiones periódicas con el objeto de: cancelar identificadores y cuentas de usuario redundantes e inhabilitar cuentas inactivas
- Se requerirá que los usuarios firmen una declaración por la cual se comprometen a mantener sus contraseñas personales en secreto y las contraseñas de los grupos de trabajo exclusivamente entre los miembros del grupo.
- Se garantizará que los usuarios cambien las contraseñas iniciales que les han sido asignadas la primera vez que ingresan al sistema.
- Los usuarios olvidan su contraseña, sólo debe suministrarse una vez acreditada la identidad del usuario.
- Se deberá configurar los sistemas de tal manera que las contraseñas sean del tipo "password fuerte" (mínimo 8 caracteres, mayúsculas, minúsculas, números, símbolos).
- Se solicitará cambio de contraseña cada 30 días.
- El acceso a Internet será utilizado con propósitos autorizados o con el destino por el cual fue provisto.

Seguridad física y del entorno

- Se almacenará la información de resguardo (backup) en un sitio seguro y distante del lugar de procesamiento, para evitar daños ocasionados ante eventuales contingencias en el sitio principal. Los medios deberán ser almacenados en cajas fuertes protegidos contra daños ambientes, y accesos no autorizados.

- Se destinará anualmente una jornada de capacitación en el uso de extintores y prevención de incendios.

- Los equipos contra incendios deberán estar ubicados en lugares adecuados y deberán ser revisados de forma periódica para verificar su estado y cambiados cuando sea necesario.

- Estará prohibido comer, beber y fumar dentro de las instalaciones de procesamiento de la información.

- Se programarán y ejecutarán planes de mantenimiento preventivo a los equipos de aire acondicionado y correctivos cuando sea necesario.

- Se llevará control diario de las condiciones ambientales para verificar que no afecten el funcionamiento de las instalaciones de procesamiento de información y equipos de respaldo eléctrico.

- Se deberá contar con un equipo de respaldo de suministro de energía interrumpible (UPS) para asegurar el apagado regulado y sistemático o la ejecución continua del equipamiento que sustenta las operaciones críticas.

- Los equipos de UPS serán inspeccionados y probados periódicamente para asegurar que funcionan correctamente y que tienen la autonomía requerida.

Comunicaciones y operaciones

- Cuando se inicie el desempeño de un empleo nuevo o cuando surjan cambios en los sistemas se deberán entregar instrucciones relacionadas con el manejo de errores u otras condiciones excepcionales que puedan surgir durante la ejecución de tareas, restricciones en el uso del sistema, personas de soporte a contactar en caso de dificultades operativas o técnicas imprevistas.

- El reinicio del sistema y procedimientos de recuperación en caso de producirse fallas en el sistema se ejecutarán con base a lo descrito en el plan de contingencias y plan de recuperación.

- Se definirán procedimientos para el control de los cambios en el ambiente operativo y de comunicaciones. Todo cambio deberá ser evaluado previamente en aspectos técnicos y de seguridad.

- Se prohíbe el uso de software no autorizado o que no cuente con las licencias respectivas.

- Se deberá Instalar y actualizar periódicamente software de detección y reparación de virus, examinado computadoras y medios informáticos, como medida precautoria y rutinaria.

- Se deberán mantener los sistemas al día con las últimas actualizaciones de seguridad disponibles (probar dichas actualizaciones en un entorno de prueba previamente si es que constituyen cambios críticos a los sistemas).

- Se deberán redactar procedimientos para verificar toda la información relativa a software malicioso, garantizando que los boletines de alerta sean exactos e informativos.

- Se deberá concientizar al personal acerca del problema de los falsos virus (hoax) y de cómo proceder frente a los mismos.

- El Responsable del Área Informática dispondrá y controlará la realización de copias de seguridad, así como la prueba periódica de su restauración. Para esto se deberá contar con instalaciones de resguardo que garanticen la disponibilidad de toda la información y del software crítico.

- Almacenar en una ubicación remota copias recientes de información de resguardo junto con registros exactos y completos de las mismas y los procedimientos documentados de restauración, a una distancia suficiente como para evitar daños provenientes de un desastre en el sitio principal.

- Verificar y probar periódicamente los procedimientos de restauración garantizando su eficacia y cumplimiento dentro del tiempo asignado a la recuperación en los procedimientos operativos.

Políticas generales

- Se deben identificar las amenazas que ponen en riesgo la seguridad de los activos.

- Se debe realizar una adecuada gestión de los riesgos.

- Se deberá verificar la efectividad de los controles establecidos.

13. DISMINUCION DEL RIESGO

El nivel de disminución del riesgo en la Alcaldía de Tuluá se puede determinar a corto, mediano o largo plazo mediante el establecimiento de indicadores de los siguientes tipos:

- Indicadores de grado de efectividad de los controles: Para saber si los controles están implantados y están funcionando bien.
- Indicadores de medición del entorno: Para verificar si las amenazas han cambiado o ha cambiado su frecuencia de ocurrencia.
- Indicadores de gestión Interna: Eliminación de no conformidades, resultados de auditorías entre otros.

Algunos indicadores que se pueden implantar son:

A corto plazo:

- **Cantidad de incidentes informáticos de seguridad reportados**
- **Porcentaje de incidencias mejorados**

A mediano plazo:

- **Tiempo sin interrupciones / Tiempo total del servicio**
- **Tiempo sin violaciones a la seguridad reportadas // Tiempo total del servicio**

A largo plazo:

- **Valor del riesgo – valor de riesgos reincidentes en nuevo análisis**

La disminución del riesgo a corto plazo puede determinarse mediante revisión periódica de los controles implantados y comprobando si cumplen con lo esperado.

Para revisión de los controles se utilizó el siguiente indicador:

- **Porcentaje de incidencias mejoradas =**

  Incidentes con mejora proyectados / Incidentes reportados * 100

Incidentes reportados: Número de incidentes reportados en 10 días. Se tuvo en cuenta los reportes de incidencia hechos por los usuarios y por los funcionarios del Departamento de Tecnología, los cuales realizaron actividades de indagación, observación, inspecciones, supervisión, muestreo y consultas al sistema.

Incidentes con mejora proyectados: Se realizó proyección de los incidentes que se mejoran con controles de seguridad propuestos en el presente análisis por espacio de 10 días.

Resultado de la medición:

- Incidentes reportados: 21
- Incidentes con mejora proyectados: 13

Porcentaje de incidencias mejoradas = 62%

El resultado anterior nos indica que aplicando los controles propuestos, se mejora en un 62% los incidentes de seguridad presentados.

Se hace salvedad de que el impacto mayor sobre la disminución de los riesgos es posible visualizarse en mediciones a mediano o largo plazo.

14. CONCLUSIONES

- La Alcaldía Municipal de Tuluá no cuenta con un análisis metodológico para el análisis y tratamiento de riesgos informáticos, por lo cual el presente estudio será de gran utilidad para la correcta identificación y gestión de riesgos.

- El análisis y gestión de riesgos se hace necesario para aumentar los niveles de seguridad de la información de la Alcaldía de Tuluá

- Por medio de la aplicación de la metodología MAGERIT se logró llegar a una identificación acertada de las principales problemáticas existentes en materia de seguridad.

- Como resultado del presente estudio se genera un documento que permite dar inicio a la ejecución de un plan de seguridad que involucre a toda la entidad.

- El factor humano es fundamental para garantizar la seguridad de la información, por lo cual el establecimiento de políticas de seguridad se hace indispensable.

- Una adecuada gestión de los riesgos identificados durante el presente análisis impactará de forma positiva en la confiabilidad de los usuarios y la mejora de la imagen corporativa.

- El análisis y gestión de riesgos es un proceso esencial en la gobernabilidad de TI y su ejecución permite a la Alcaldía de Tuluá dar cumplimiento al componente número 4 de Gobierno En Línea: *Seguridad y privacidad de la Información - Implementación del plan de seguridad y privacidad de la información y de los sistemas de información - Gestión de riesgos de seguridad y privacidad de la información.*

15. RECOMENDACIONES

- Se sugiere incorporar dentro de los procesos de la entidad el análisis y gestión de riesgos informáticos para aumentar los niveles de seguridad de la información.

- Se aconseja la revisión de las amenazas, y riesgos detectados, considerando los diferentes factores que afectan su incidencia, tales como cambios tecnológicos, implementación de nuevos proyectos entre otros.

- Es importante crear un sistema de incidencias que recoja las notificaciones continuas por parte de los usuarios y que permitan identificar las nuevas amenazas

- Se recomienda realizar revisión periódica de los controles de seguridad establecidos para verificar su efectividad.

- Se sugiera la implementación de las políticas de seguridad definidas en el presente documento.

16. BIBLIOGRAFIA

Benavides M.C. y Solarte F. (2012). *Módulo de Riesgos y Control Informático.*

Cano J. (2004*) Hacia un concepto extendido de la mente segura*. Pensamiento sistémico en seguridad informática. Artículo de investigación (En revisión). Universidad de los Andes

Dirección de Estándares y Arquitectura de TI del Ministerio de las Tecnologías de Información y las Comunicaciones de la República de Colombia. (2014). *Generalidades del Marco de Referencia – versión 1.0.* Disponible en URL: http://www.mintic.gov.co/marcodereferencia/624/articles-8102_generalidades.pdf

Eterovic J. E. y Pagliari G. A. (2011). *Metodología de Análisis de Riesgos Informáticos.*

García Guevara C.A. (2012). *Establecimiento del sistema de seguridad de información en SFG bajo los estándares de la norma ISO 27001: 2005* - Informe final de investigación. Universidad EAN. Disponible en URL: http://repository.ean.edu.co/handle/10882/1457/browse?value=Garc%C3%ADa+Guevara%2C+Camilo+Augusto&type=author

Gómez R., Pérez D., Donoso Y. y Herrera A. (2010) M*etodología y gobierno de la gestión de riesgos de tecnologías de la información.* Artículo. Revista de Ingeniería. Universidad de los Andes.

Icontec internacional. (2013). *NTC- iso 27001. Sistemas de gestión de la Información.* Editada por el Instituto de Normas Técnicas y Certificación (ICONTEC): Autor

ISO/IEC 27000-series. (2014). Disponible en URL: http://es.wikipedia.org/wiki/ISO/IEC_27000-series

Matalobos Veiga J.M. (2009). *Análisis de riesgos de seguridad de la información* (Trabajo de fin de carrera). Universidad Politécnica de Madrid. Recuperado de: http://oa.upm.es/1646/

Ministerio de las tecnologías de la información y las comunicaciones. (2012). *Manual para la implementación de la Estrategia de Gobierno en línea en las entidades del orden nacional de la República de Colombia.* Disponible en URL: http://programa.gobiernoenlinea.gov.co/apc-aa-files/eb0df10529195223c011ca6762bfe39e/manual-3.1.pdf

Ministerio de Hacienda y Administraciones Públicas. Centro Criptológico Nacional. (2012). *MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Libro I – Método. Madrid.* Disponible en URL: https://www.ccn-cert.cni.es/publico/herramientas/pilar5/magerit/

Ministerio de las Tecnologías de la información y las Comunicaciones. (2014). *Decreto 2573 de 2014.* Disponible en URL: http://www.mintic.gov.co/marcodereferencia/624/articles-7663_recurso_1.pdf

Stoneburner G., Goguen A. & Jeringa A. (2002). *Risk Management Guide for Information Technology Systems*. Disponible en URL: http://www.revistavirtualpro.com/biblioteca/guia-de-gestion-de-riesgos-de-sistemas-informaticos-#sthash.g13kmGQd.dpuf

17. ANEXOS

17.1. ANEXO A: Dependencias entre activos

Para la interpretación de las figuras se deberá tener en cuenta el código de colores siguiente:

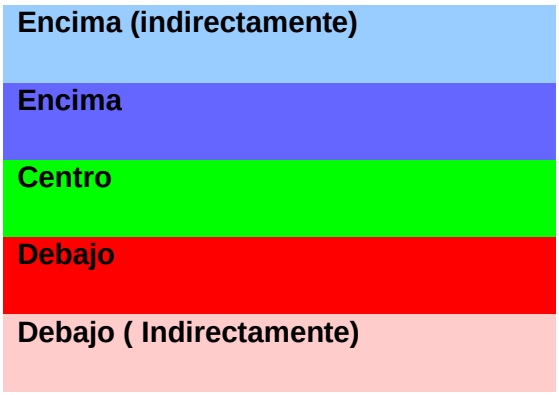

Figura 1: Colores de Dependencia de activos
Fuente: EAR/PILAR 5.4.5

Las dependencias por cada uno de los activos de información es la siguiente:

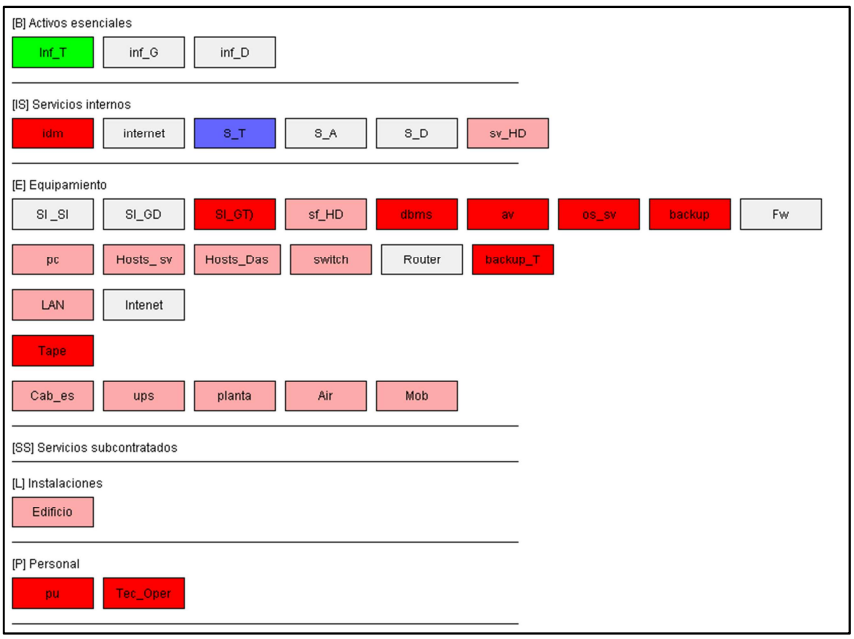

Figura 2: Dependencias (inf_T) Información tributaria
Fuente: Elaborado en EAR/PILAR 5.4.5

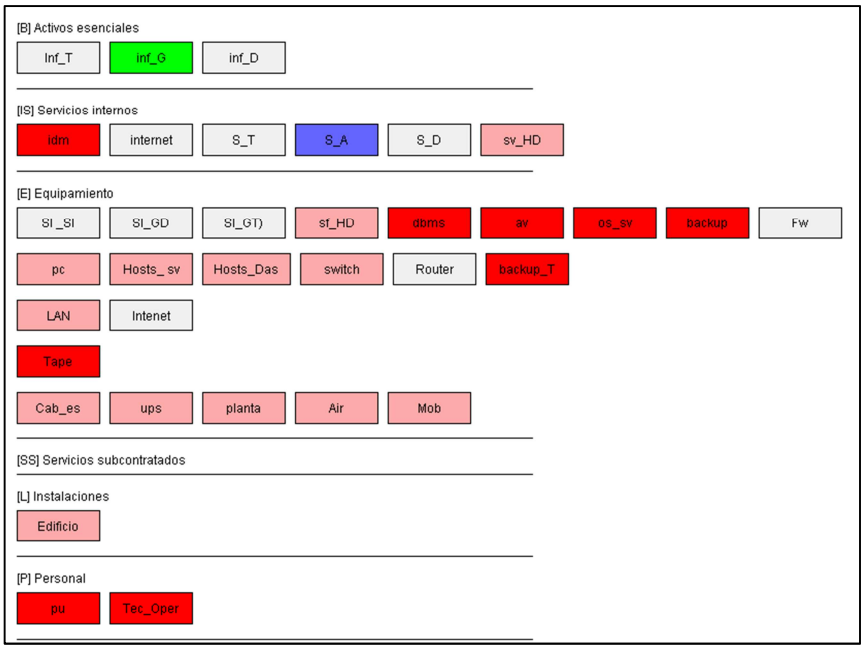

Figura 3: Dependencias (inf_T) Información tributaria
Fuente: Elaborado en EAR/PILAR 5.4.5

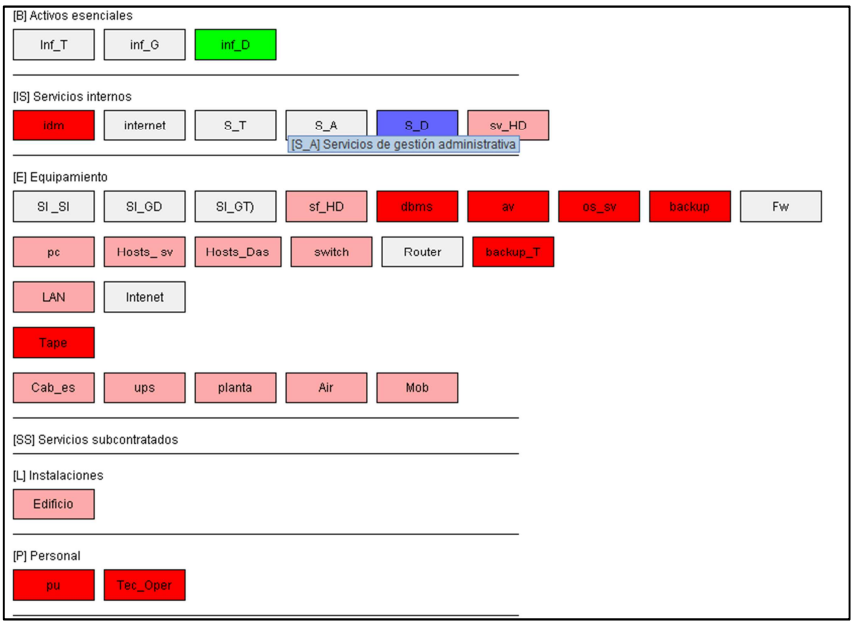

Figura 4: Dependencias (inf_D) Información de gestión documental
Fuente: Elaborado en EAR/PILAR 5.4.5

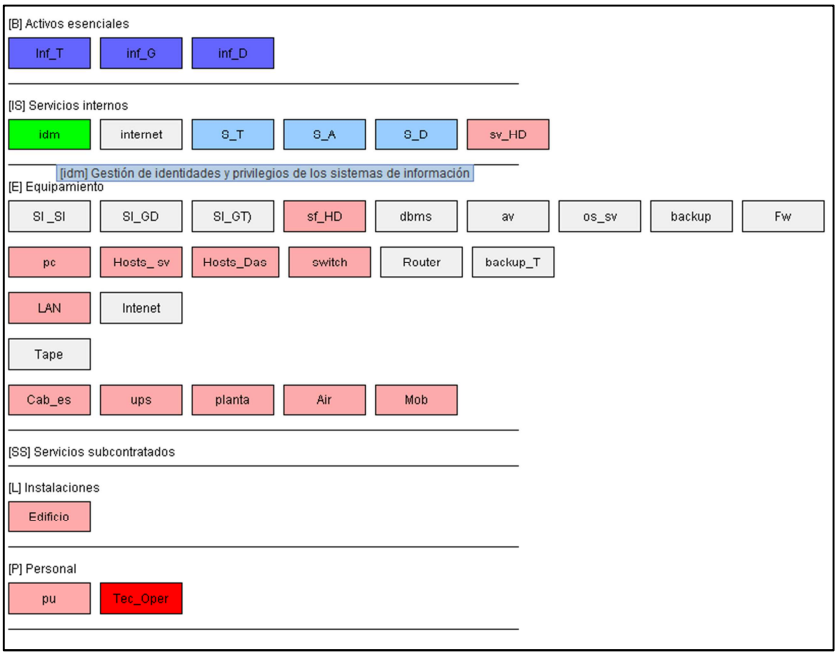

Figura 5: Dependencias (S_T) Servicios tributarios
Fuente: Elaborado en EAR/PILAR 5.4.5

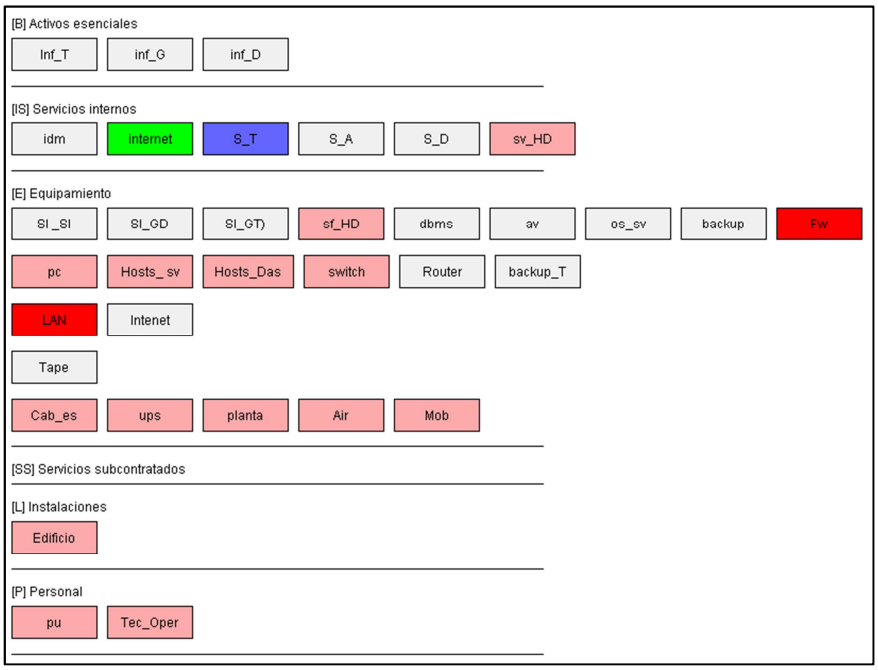

Figura 6: Dependencias (internet) servicio de internet
Fuente: Elaborado en EAR/PILAR 5.4.5

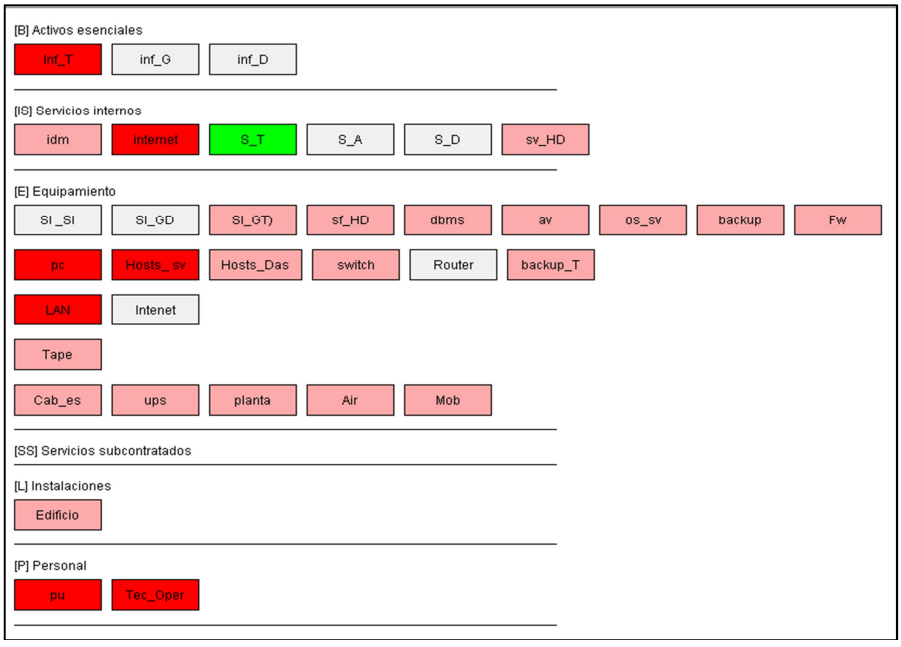

Figura 7: Dependencias (S_T) Servicios tributarios
Fuente: Elaborado en EAR/PILAR 5.4.5

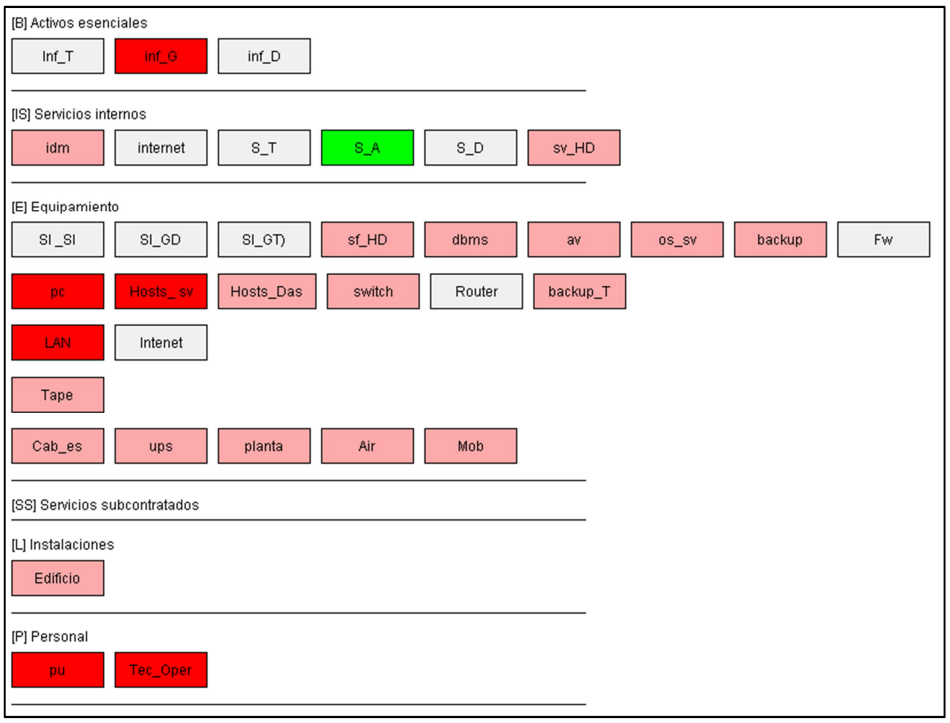

Figura 8: Dependencias (S_A) Servicios de gestión administrativa
Fuente: Elaborado en EAR/PILAR 5.4.5

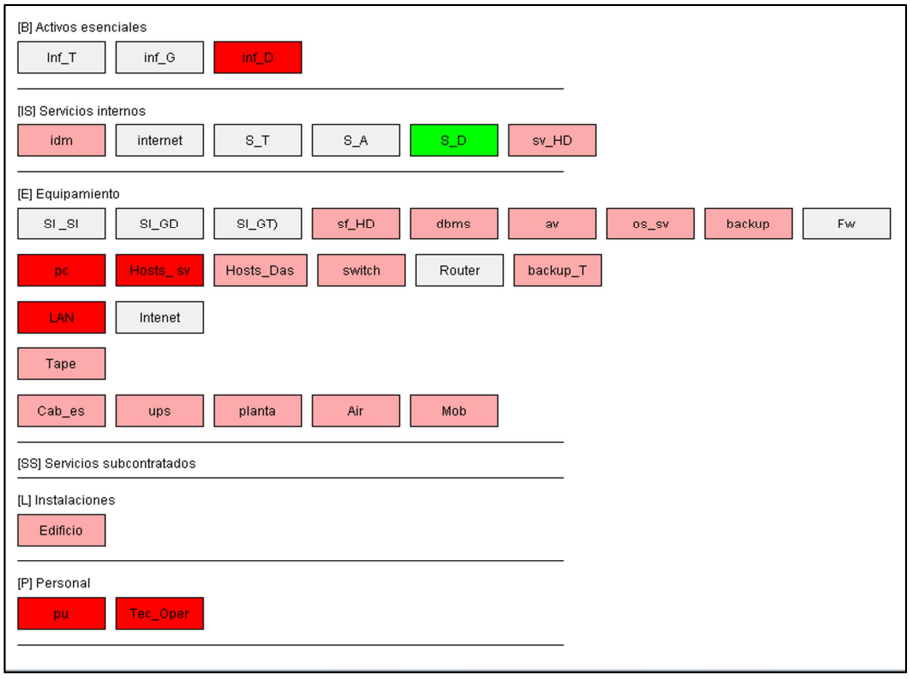

Figura 9: Dependencias (S_D) Servicios de gestión documental
Fuente: Elaborado en EAR/PILAR 5.4.5

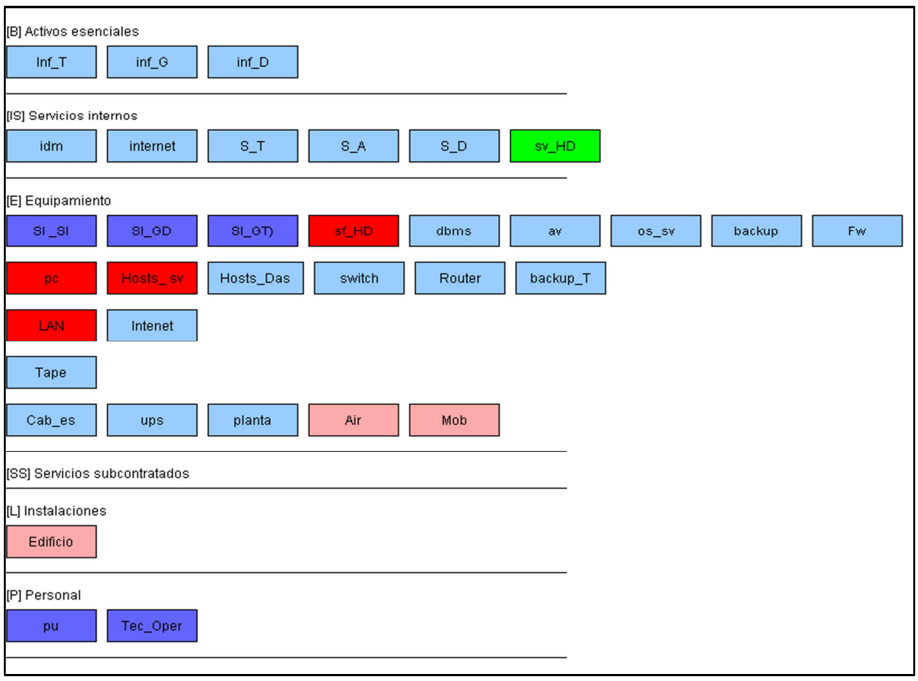

Figura 10: Dependencias (sv_HD) Servicio de mesa de ayuda
Fuente: Elaborado en EAR/PILAR 5.4.5

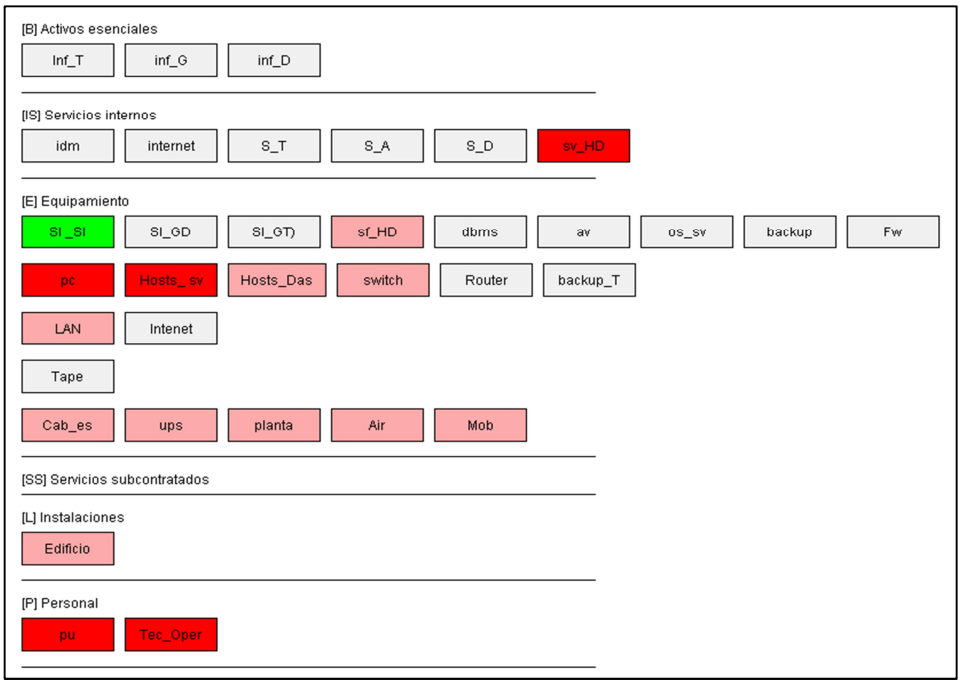

Figura 11: Dependencias (SI _SI) Sistema de información integrado
Fuente: Elaborado en EAR/PILAR 5.4.5

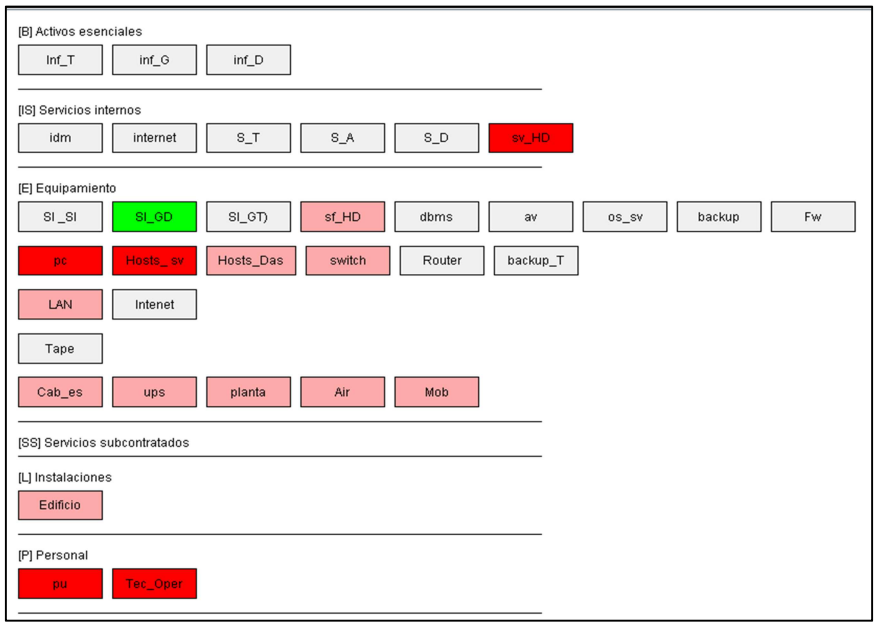

Figura 12: Dependencias (SI_GD) Sistema de gestión documental y PQRSD
Fuente: Elaborado en EAR/PILAR 5.4.5

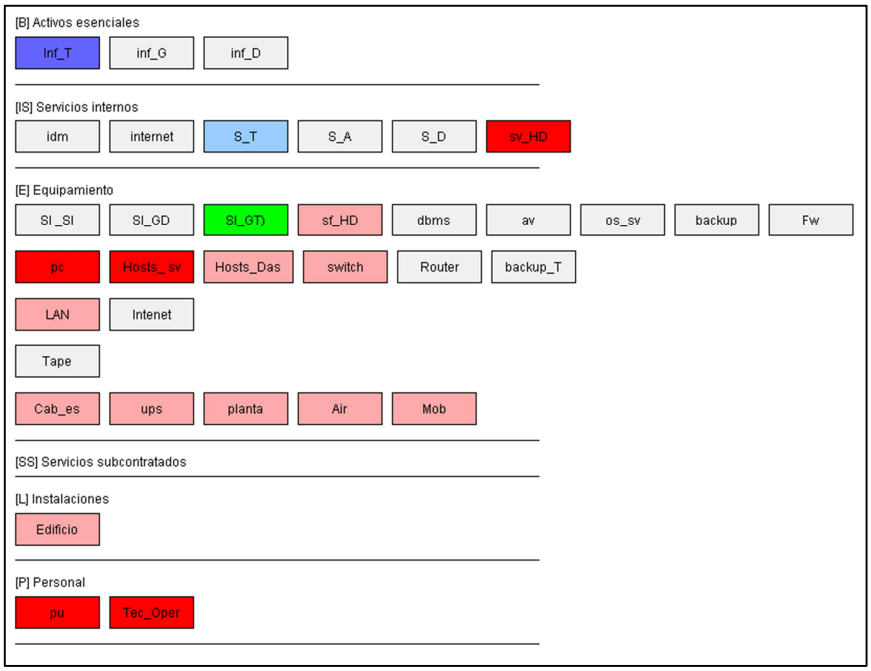

Figura 13: Dependencias (SI_GT) Sistema de información tributaria
Fuente: Elaborado en EAR/PILAR 5.4.5

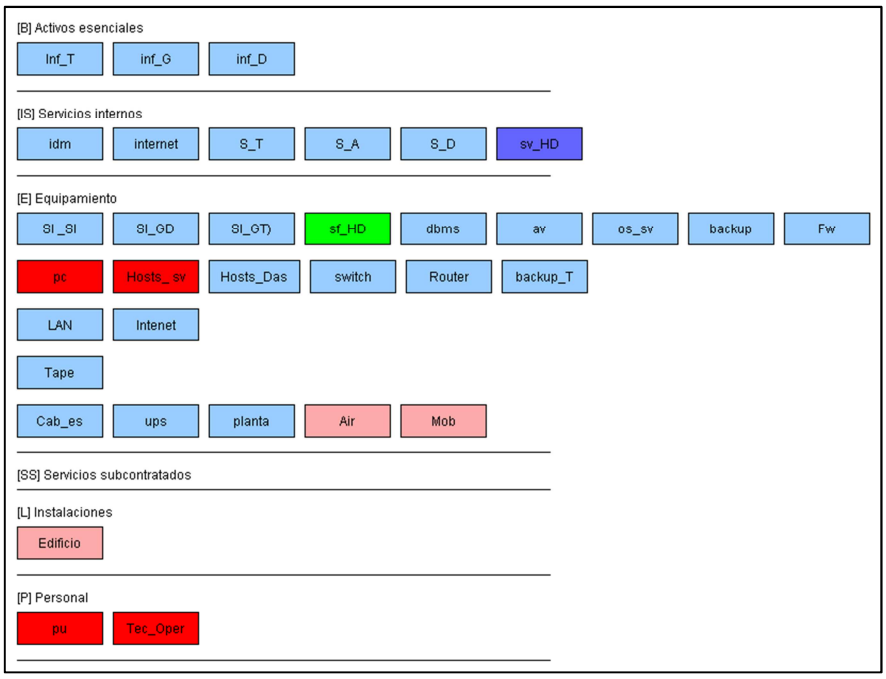

Figura 14: Dependencias (sf_HD) software de mesa de ayuda
Fuente: Elaborado en EAR/PILAR 5.4.5

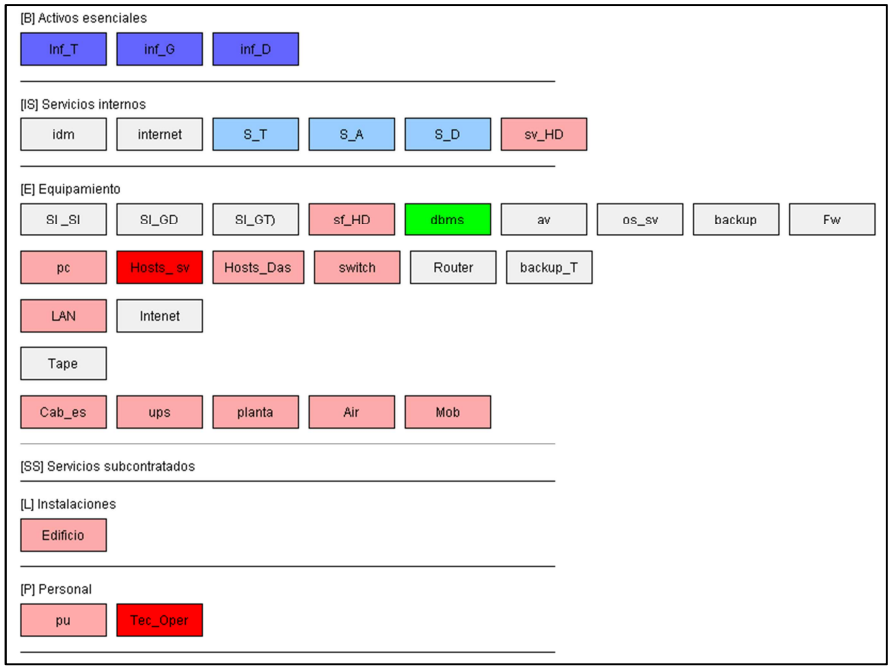

Figura 15: Dependencias (dbms) sistema de gestión de bases de datos
Fuente: Elaborado en EAR/PILAR 5.4.5

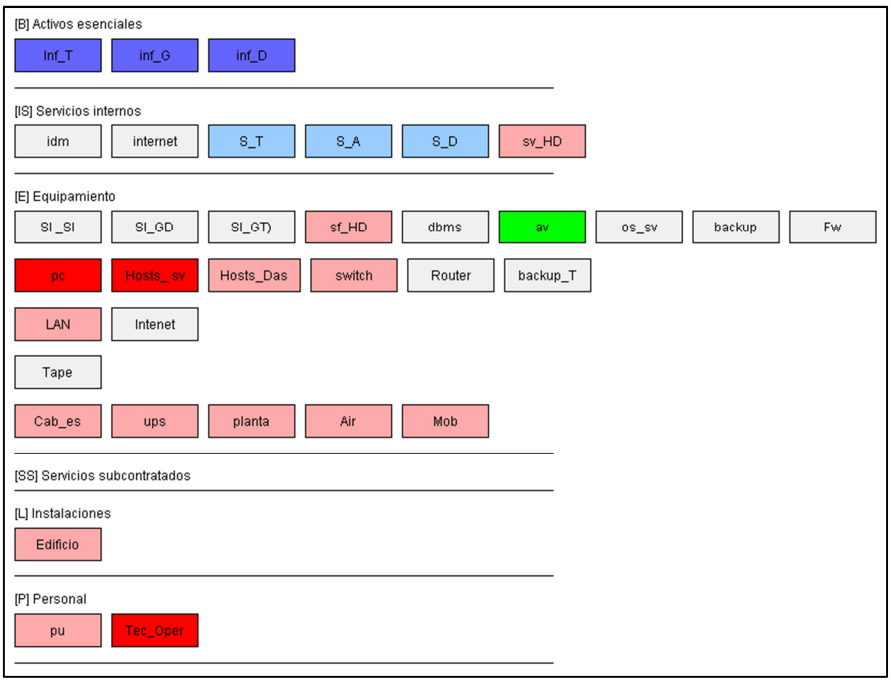

Figura 16: Dependencias (av) antivirus
Fuente: Elaborado en EAR/PILAR 5.4.5

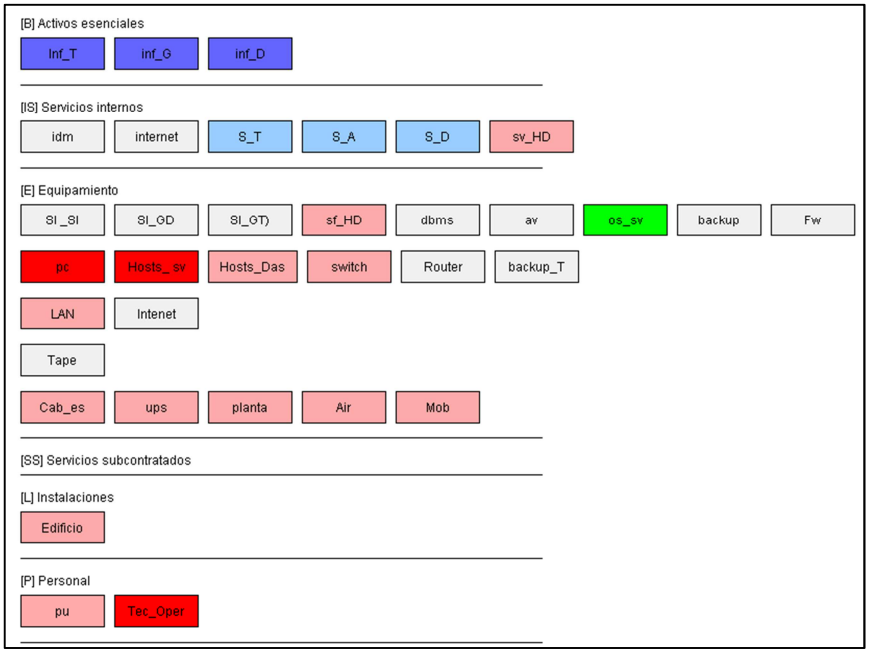

Figura 17: Dependencias (os_sv) sistema operativo servidor
Fuente: Elaborado en EAR/PILAR 5.4.5

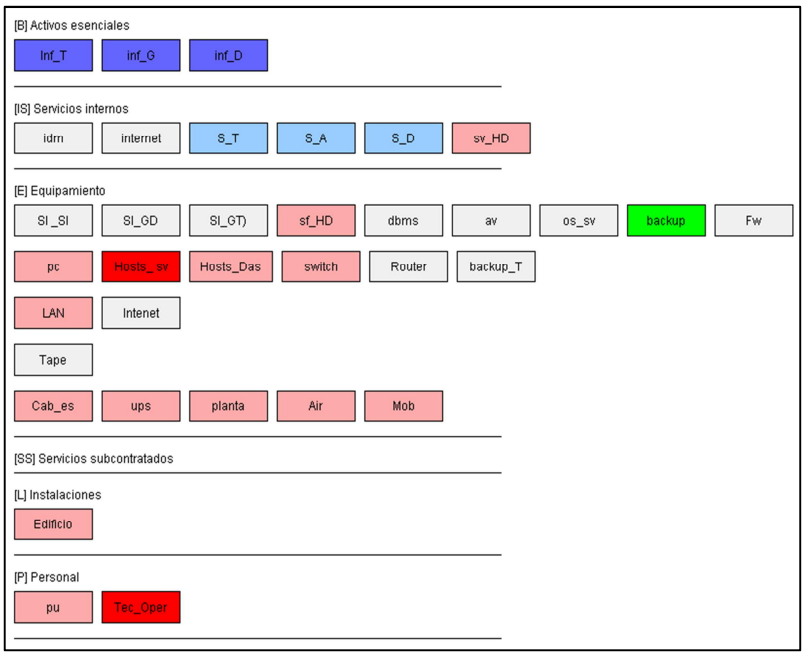

Figura 18: Dependencias (backup) sistema de backup
Fuente: Elaborado en EAR/PILAR 5.4.5

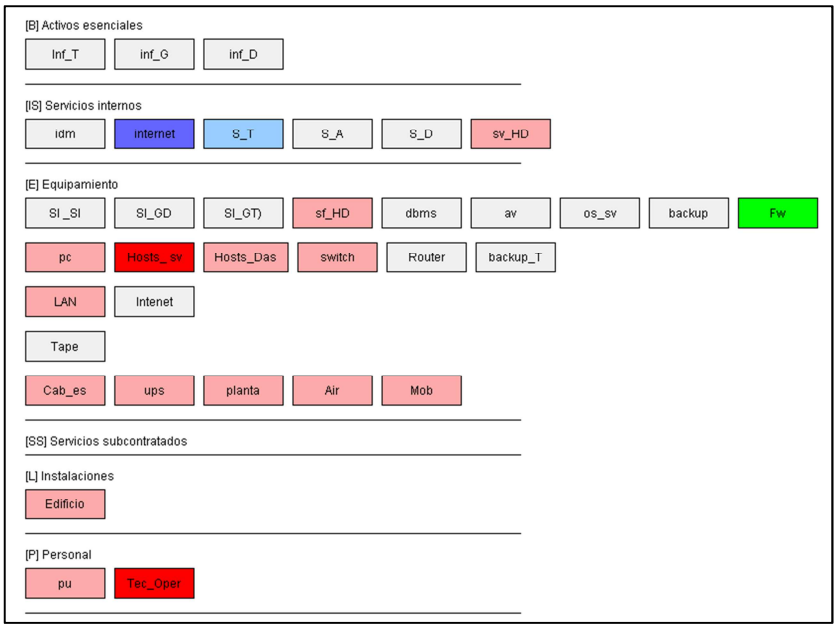

Figura 19: Dependencias (Fw) Software Firewall- proxy
Fuente: Elaborado en EAR/PILAR 5.4.5

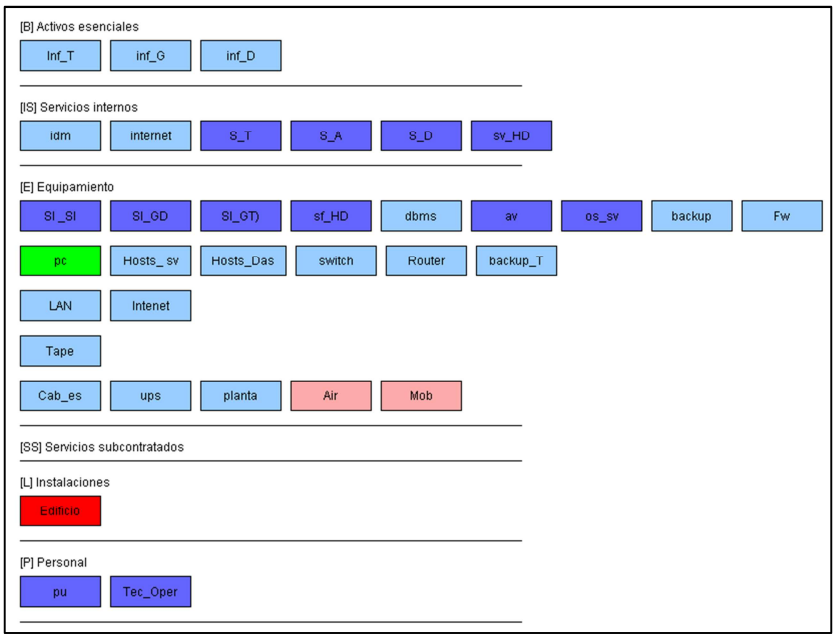

Figura 20: Dependencias (pc) Equipos de cómputo personal
Fuente: Elaborado en EAR/PILAR 5.4.5

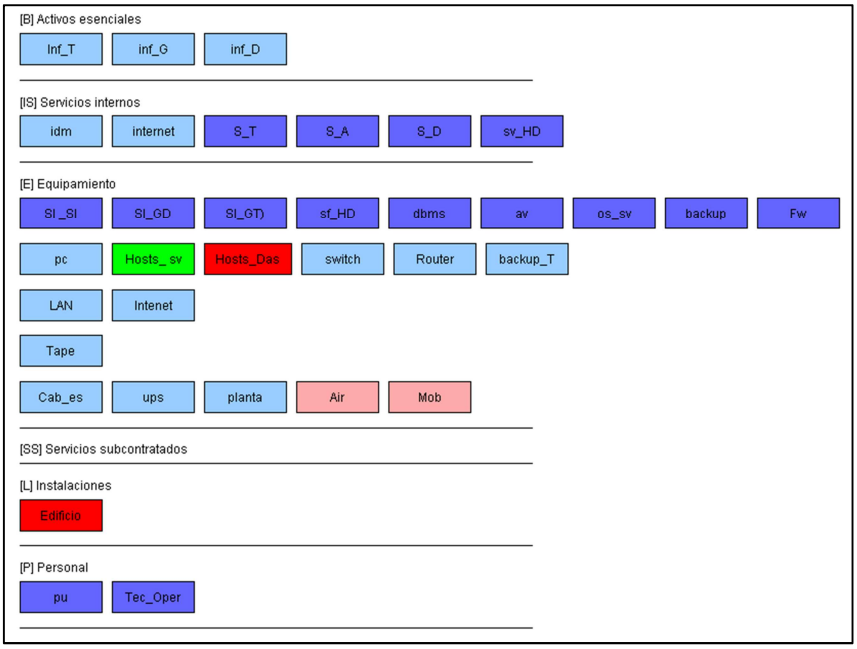

Figura 21: Dependencias (Host_sv) Servidor
Fuente: Elaborado en EAR/PILAR 5.4.5

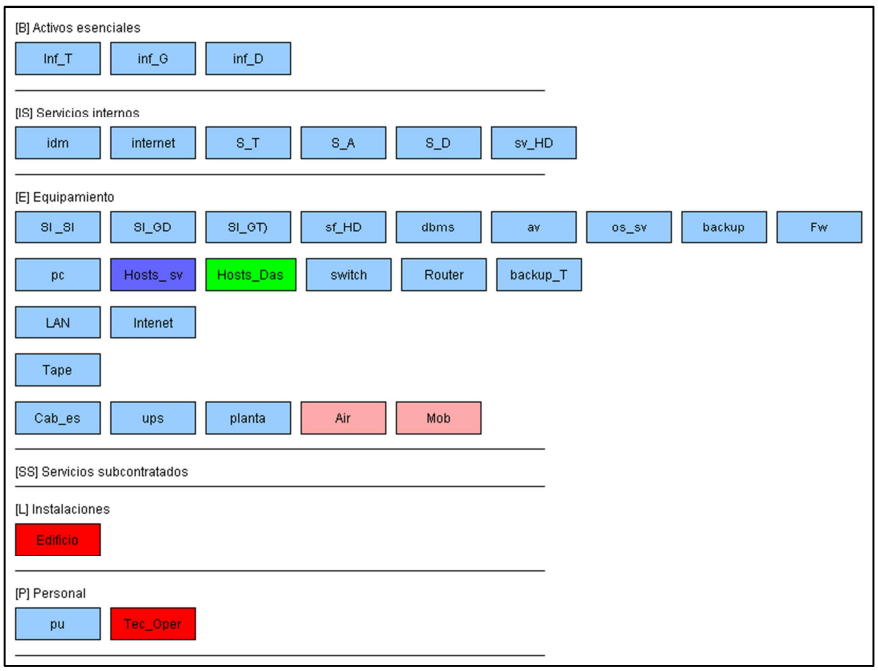

Figura 22: Dependencias (hosts_Das) DAS
Fuente: Elaborado en EAR/PILAR 5.4.5

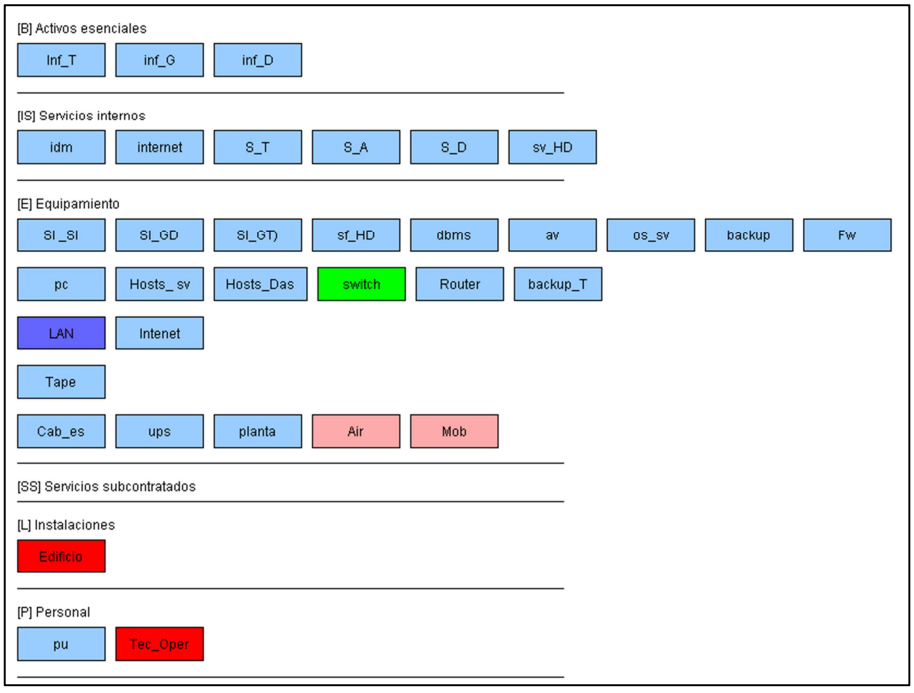

Figura 23: Dependencias (switch) Switches administrables
Fuente: Elaborado en EAR/PILAR 5.4.5

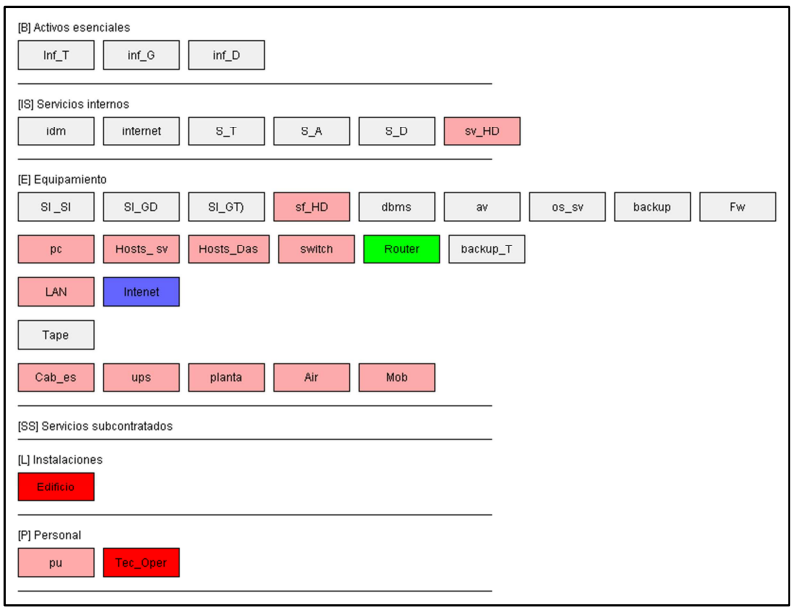

Figura 24: Dependencias (router) Router
Fuente: Elaborado en EAR/PILAR 5.4.5

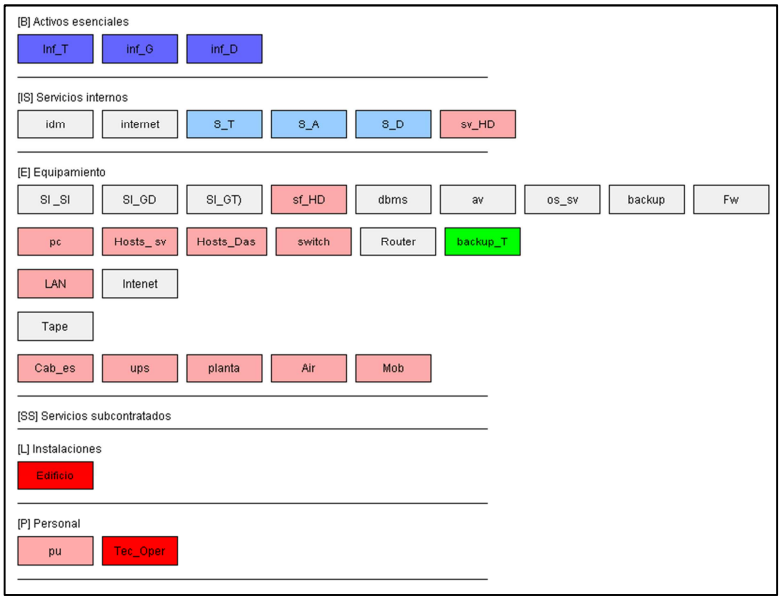

Figura 25: Dependencias (backup_T) Unidad de Tape backup
Fuente: Elaborado en EAR/PILAR 5.4.5

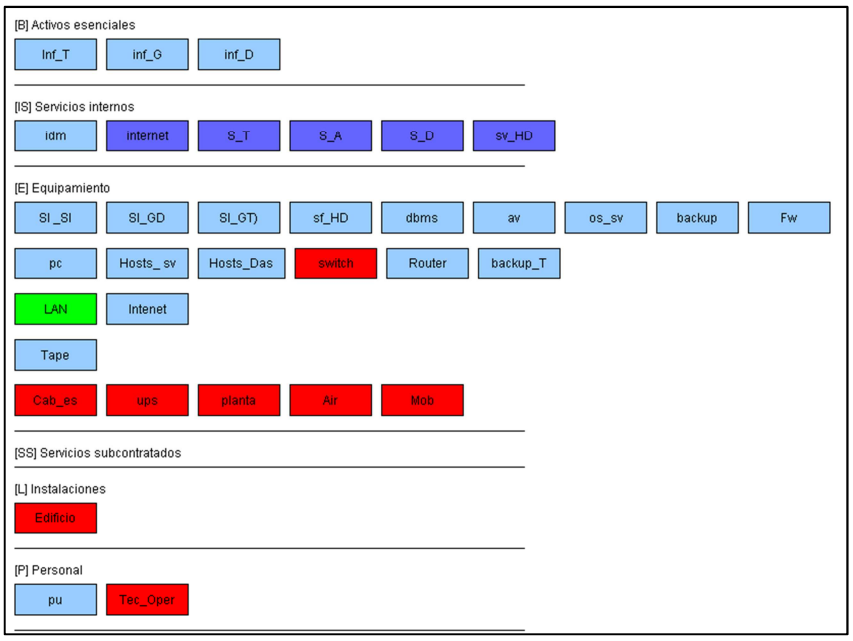

Figura 26: Dependencias (LAN) Red local
Fuente: Elaborado en EAR/PILAR 5.4.5

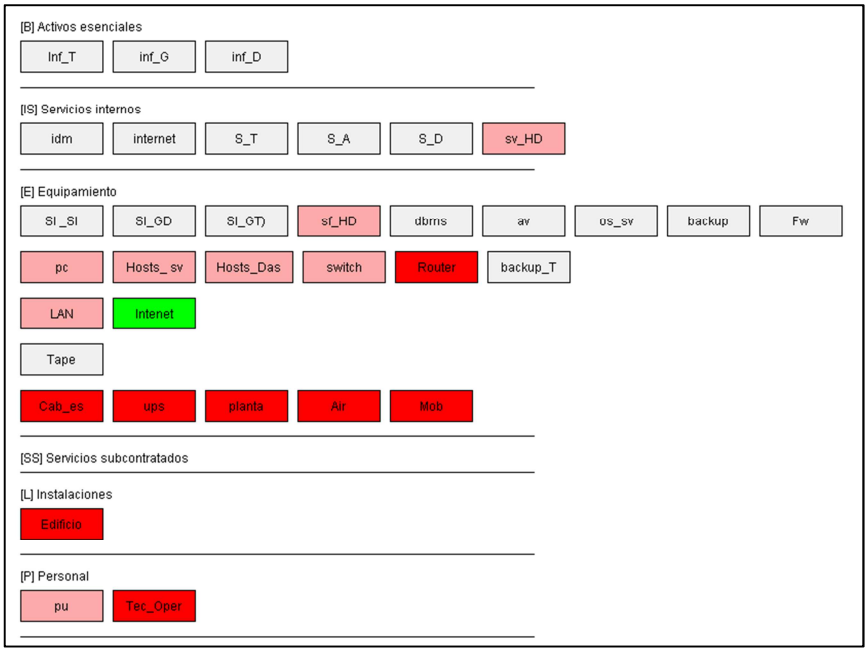

Figura 27: Dependencias (Intenet) Internet
Fuente: Elaborado en EAR/PILAR 5.4.5

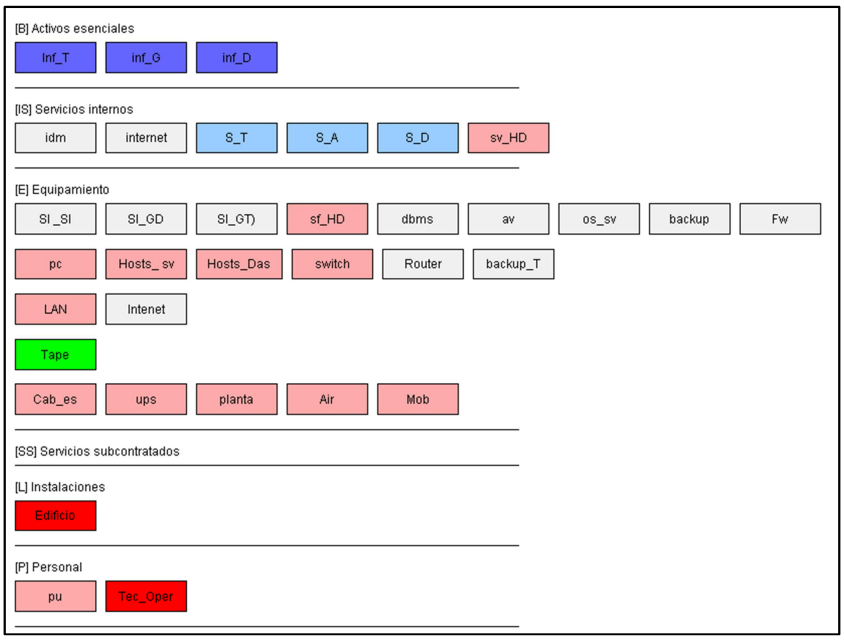

Figura 28: Dependencias (Tape) Cintas magnéticas
Fuente: Elaborado en EAR/PILAR 5.4.5

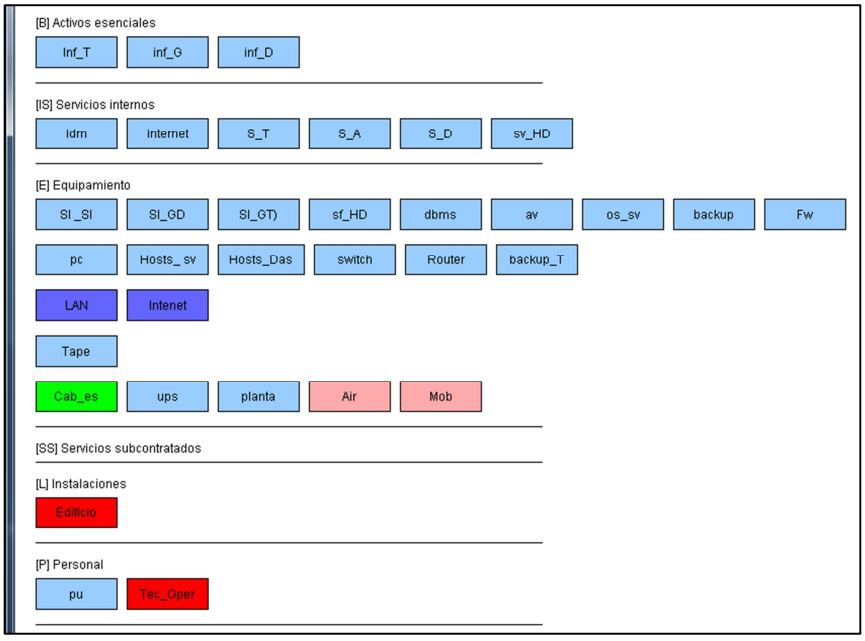

Figura 29: Dependencias (Cab_es) Cableado estructurado
Fuente: Elaborado en EAR/PILAR 5.4.5

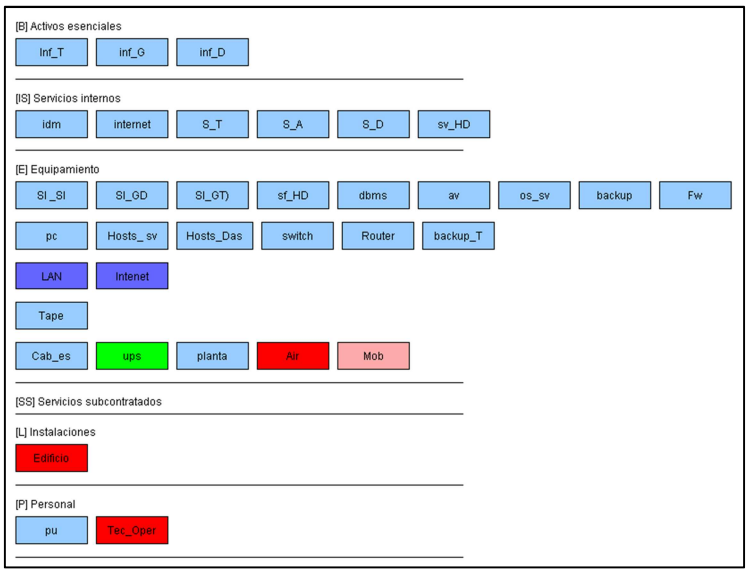

Figura 30: Dependencias (ups) Sistemas de alimentación ininterrumpida
Fuente: Elaborado en EAR/PILAR 5.4.5

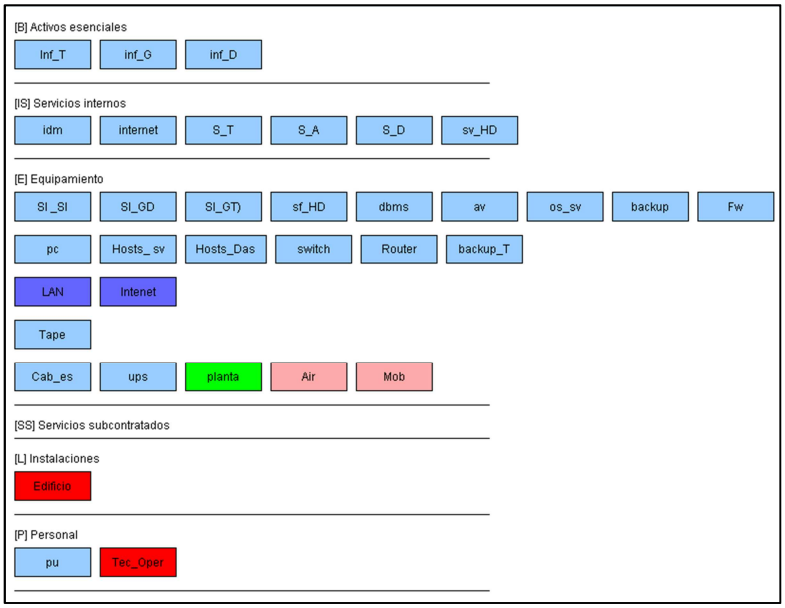

Figura 31: Dependencias (planta) Planta eléctrica
Fuente: Elaborado en EAR/PILAR 5.4.5

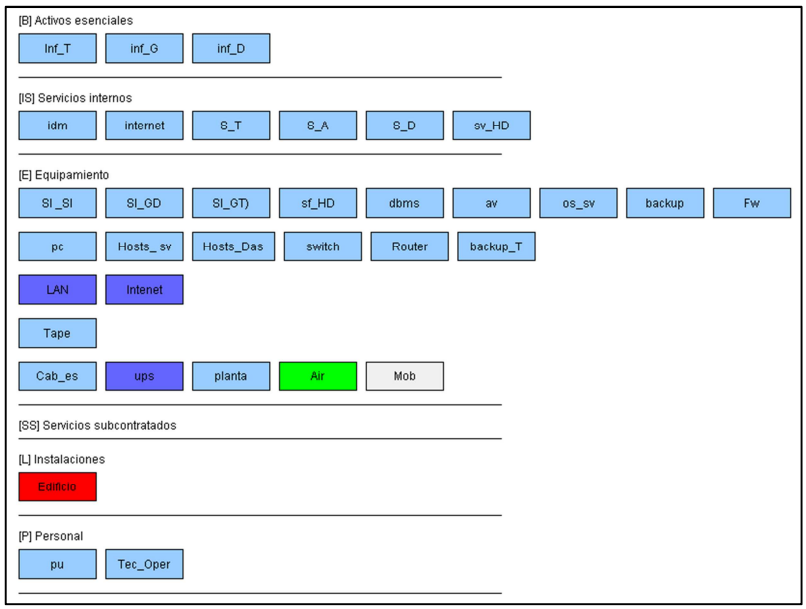

Figura 32: Dependencias (Air) Equipos de aire acondicionado
Fuente: Elaborado en EAR/PILAR 5.4.5

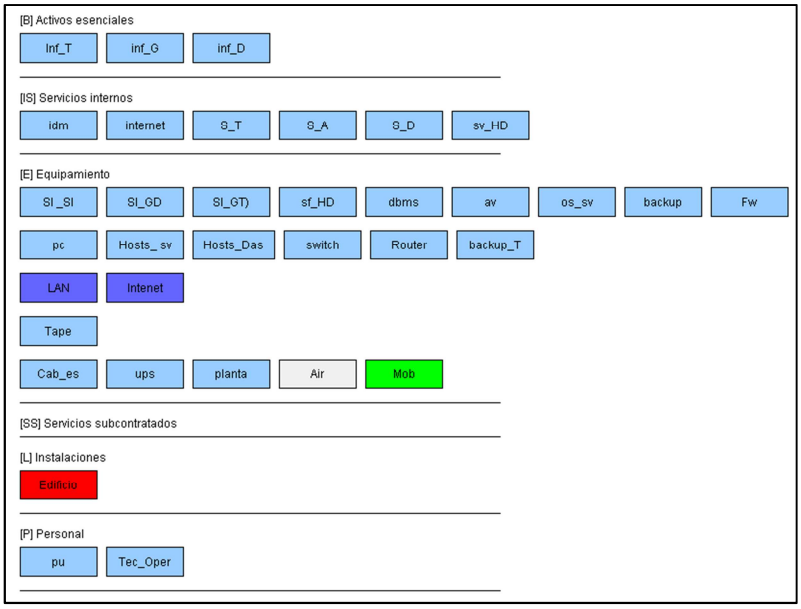

Figura 33: Dependencias (mob) Mobiliario
Fuente: Elaborado en EAR/PILAR 5.4.5

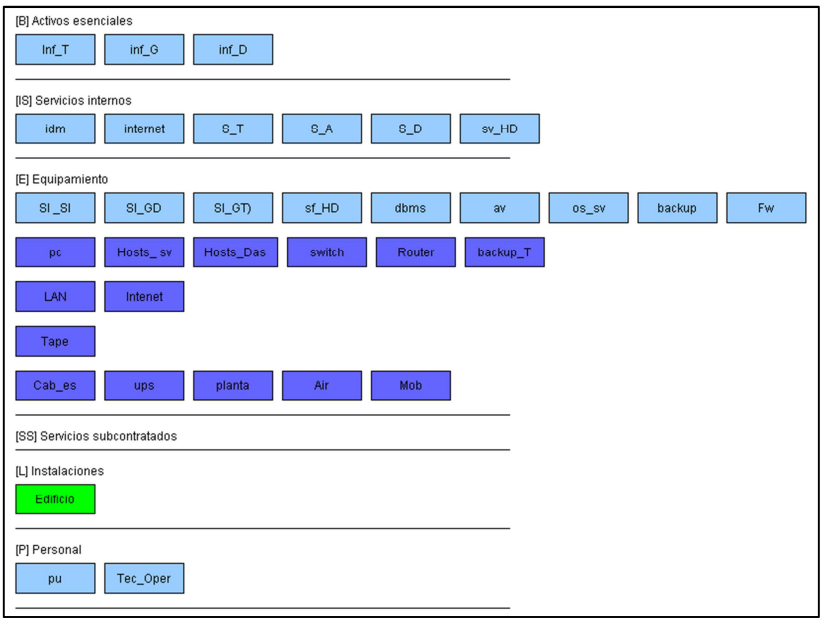

Figura 34: Dependencias (Edificio) Edificio central
Fuente: Elaborado en EAR/PILAR 5.4.5

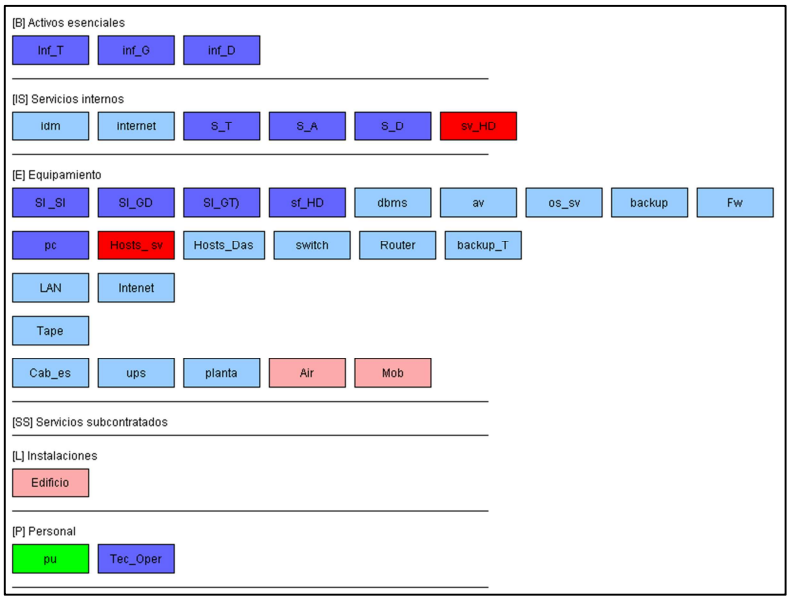

Figura 35: Dependencias (pu) Personal usuario
Fuente: Elaborado en EAR/PILAR 5.4.5

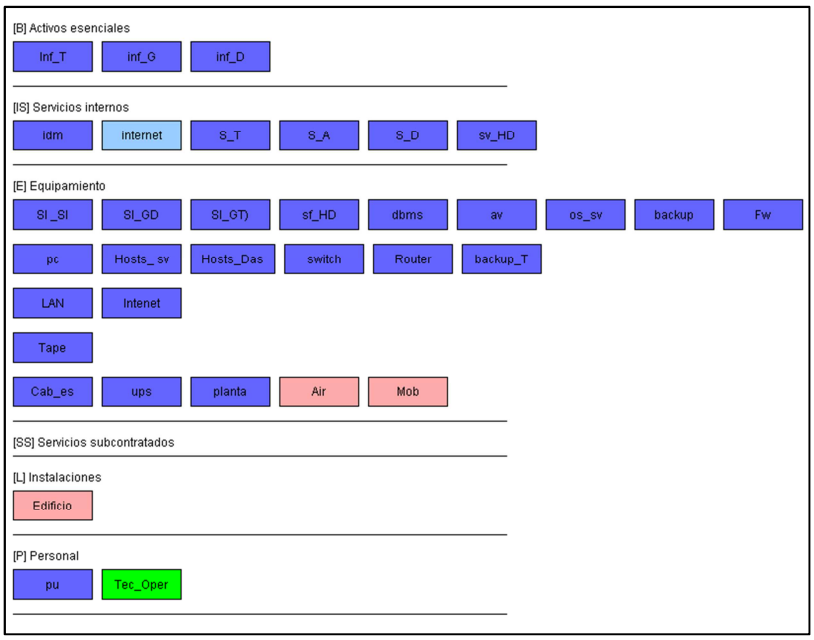

Figura 36: Dependencias (Tec_Oper) Técnico Operativo
Fuente: Elaborado en EAR/PILAR 5.4.5

17.2. ANEXO B: Mapa de Riesgos

Tabla 27. Mapa de riesgos

Tipo de activo	Amenaza	Proba-bilidad	Degradación			Impacto Residual			Riesgo Residual			Salvaguarda	Efecti-vidad	Salvaguarda Propuesta
			D	I	C	D	I	C	D	I	C			
(ESSENTIAL) Activos esenciales - Datos	[E.1] Errores de los usuarios	A	30%	100%	1%	A	A	M	MA	MA	A	Aseguramiento de la integridad	80%	Capacitación y concienciación
	[E.2] Errores del administrador	MB	90%	90%	1%	MA	A	M	A	M	B	Ninguna		*Capacitación y concienciación *Servidor para pruebas, actualizaciones y cambios antes de aplicar en producción
	[E.15] Alteración accidental de la información	MB		90%			M			B		Copias de seguridad de los datos (backup)	50%	*Capacitación y concienciación *Servidor para pruebas, actualizaciones y cambios antes de aplicar en producción
	[E.19] Fugas de información	A			5%		M			B		Ninguna		Firma de acuerdos de confidencialidad durante el proceso de contratación
	[A.5] Suplantación de la identidad del usuario	MB	90%	90%	90%	A	A	A	M	M	M	Identificación y autenticación	60%	*Aplicación de políticas de contraseñas seguras. *Capacitación y concienciación
	[A.15] Modificación deliberada de la información	MB		90%			A			M		Protecciones Generales	80%	*Proteger la red LAN de accesos no autorizados
	[A.18] Destrucción de información	MB	100%				A			M		Ninguna		*Proteger la red LAN de accesos no autorizados
(S) servicios	[E.24] Caída del sistema por agotamiento de recursos	B	90%			M			M			*Gestión de cambios (mejoras y sustituciones) *Protecciones generales *Se aplican perfiles de seguridad	80%	Políticas de seguridad de uso de los recursos
	[A.18] Destrucción de información	MB	60%			A			M			Ninguna		*Proteger la red LAN de accesos no autorizados
	[A.24] Denegación de servicio	MB	100%			MA			A			Ninguna		*Proteger la red LAN de accesos no autorizados. Aplicación de políticas de contraseñas seguras

Fuente: Esta investigación

Tabla 27. Mapa de riesgos

Tipo de activo	Amenaza	Proba-bilidad	Degradación			Impacto Residual			Riesgo Residual			Salvaguarda	Efecti-vidad	Salvaguarda Propuesta
			D	I	C	D	I	C	D	I	C			
(S) servicios	[A.18] Destrucción de información	MB	60%			A			M			Ninguna		*Proteger la red LAN de accesos no autorizados
	[A.24] Denegación de servicio	MB	100%			MA			A			Ninguna		*Proteger la red LAN de accesos no autorizados. Aplicación de políticas de contraseñas seguras
(SW) aplicaciones	[E.1] Errores de los usuarios	M	2%	2%	2%	MB	MB	MB	MB	MB	MB	Cambios (actualizaciones y mantenimiento)	75%	* Capacitación a los usuarios sobre el uso de los aplicativos
	[E.2] Errores del administrador	MB	90%	90%	90%	MA	MA	MA	A	A	A	Ninguna		*Capacitación *Servidor para pruebas, actualizaciones y cambios antes de aplicar en producción
	[E.8] Difusión de software dañino	A	80%	30%	1%	M	M		A	A		Cambios (actualizaciones y mantenimiento)	75%	* Aplicación de políticas de seguridad para evitar proliferación de malware. *Capacitación sobre malware al usuario final
	[E.21] Errores de mantenimiento / actualización de programas (software)	B	50%	30%		M	M		M	M		Cambios (actualizaciones y mantenimiento)	75%	Mantener vigentes los contratos de mantenimiento de software
	[A.6] Abuso de privilegios de acceso	B	1%	90%	5%		A	M		A	M	Se aplican perfiles de seguridad	60%	* Mantener actualizados los perfiles de usuario. *Aplicación de políticas de acceso a los sistemas que incluyan accesos, denegación y verificación de perfiles. *Modificación al procedimiento de control de acceso, donde se incluya personal contratista.
	[A.11] Acceso no autorizado	B	1%	90%	5%		A	M		A	M	Se aplican perfiles de seguridad	60%	* Mantener actualizados los perfiles de usuario. *Aplicación de políticas de acceso a los sistemas que incluyan accesos, denegación y verificación de perfiles. *Modificación al procedimiento de control de acceso, donde se incluya personal contratista.
(HW) Equipamiento informático (hardware)	[I.5] Avería de origen físico o lógico	B	10%			M			M			Cambios (actualizaciones y mantenimiento)	90%	*Contar con equipos de respaldo
	[I.7] Condiciones inadecuadas de temperatura o humedad	MB	70%			M			B			Protecciones Generales	90%	Contar con equipos de aire condicionado de respaldo
	[I.6] Corte del suministro eléctrico	MB	100%			M			B			Protecciones Generales	90%	* Ejecutar planes de mantenimiento preventivo a la planta eléctrica y a las UPS. *Contar con UPS de respaldo
	[E.2] Errores del administrador	MB	90%	90%	1%	M	M		B	B		Cambios (actualizaciones y mantenimiento)	90%	Entrenamiento sobre el uso correcto del equipamiento
	[A.25] Robo	MB	100%		5%	M			B			Protecciones Generales	90%	Aquirir póliza de seguros contra robo

Fuente: Esta investigación

Tabla 27. Mapa de riesgos

Tipo de activo	Amenaza	Proba-bilidad	Degradación			Impacto Residual			Riesgo Residual			Salvaguarda	Efecti-vidad	Salvaguarda Propuesta
			D	I	C	D	I	C	D	I	C			
(COM) Redes de comunicaciones	[I.8] Fallo de servicios de comunicaciones	MB	100%			M			B			Protecciones Generales	90%	*Elaborar y establecer plan de recuperación de desastres y plan de contingencias. Entrenar al personal al respecto
	[E.2] Errores del administrador	MB	90%	1%	1%	M			B			Protecciones Generales	90%	Entrenamiento sobre el uso correcto del equipamiento
	[E.24] Caída del sistema por agotamiento de recursos	B	90%			M			M			Sistema de protección perimetral	90%	*Capacitar al personal de teconología en seguridad Informática
	[A.7] Uso no previsto	MA	80%	1%	1%	M			A			Internet: uso de ? acce	80%	*Definir políticas claras de navegación.
	[A.11] Acceso no autorizado	MB		90%	1%		M			B		Sistema de protección perimetral	90%	*Implementar medidas de• Autenticación e identificación de usuarios y accesos para toda la red LAN
	[A.24] Denegación de servicio	MB	100%			M			B			Protecciones Generales	90%	*Proteger la red LAN de accesos no autorizados. Aplicación de políticas de contraseñas seguras
(MEDIA) Soportes de información	[I.1] Fuego	MB	100%			MA	A	A	A	M	M	Aseguramiento de la disponibilidad	70%	*Disponer extintores que cumplan con las normas técnicas. *Capacitar al personal sobre uso de extitores e incendios
	[N.7] Desastres naturales	MB	100%			MA	A	A	A	M	M	Aseguramiento de la disponibilidad	70%	*Utilizar cajas fuertes para medios almacenado en el Departamento de Tecnología
(AUX) Equipamento auxiliar	[I.1] Fuego	MB	100%			M			B			Climatización	90%	*Disponer extintores que cumplan con las normas técnicas. *Capacitar al personal sobre uso de extitores e incendios
	[N.7] Desastres naturales	MB	100%			MA			A			Ninguna		*Contar con equipos de respaldo *Incluír en póliza de seguros
(L) Instalaciones	[I.1] Fuego	MB	100%			MA			A			Control de los accesos físicos	0%	*Disponer extintores que cumplan con las normas técnicas. *Capacitar al personal sobre uso de extitores e incendios
	[N.7] Desastres naturales	MB	100%			MA			A			Ninguna		Incluir en póliza de seguros
	[I.*] Desastres industriales	MB	100%			MA			A			Ninguna		*Disponer extintores que cumplan con las normas técnicas. *Capacitar al personal sobre uso de extitores e incendios
(P) Personal	[E.28] Indisponibilidad del personal	M	100%			A	MA	MA	A	MA	MA	Gestión del Personal	70%	*Entrenar a varias personas sobre un mismo procedimiento.
	[A.30] Ingeniería social (picaresca)	M	20%	100%	5%	M	A	M	M	A	M	Formación y concienciación	40%	*Comunicar y hacer cumplir las políticas de seguridad informáticas

Fuente: Esta investigación