ESPE

UNIVERSIDAD DE LAS FUERZAS ARMADAS

INNOVACIÓN PARA LA EXCELENCIA

VICERRECTORADO DE INVESTIGACIÓN Y VINCULACIÓN CON LA COLECTIVIDAD

MAESTRIA EN EVALUACION Y AUDITORIA DE SISTEMAS TECNOLOGICOS

IV – B – PROMOCION 2011 - 2012

Tesis de Grado MASTER EN EVALUACION Y AUDITORIA DE SISTEMAS TECNOLOGICOS

TEMA: “EVALUACIÓN DE RIESGOS DE LOS SISTEMAS DE INFORMACIÓN DE AUDIOAUTO S.A. UTILIZANDO MAGERIT V3.0 APOYADOS PARA EL ANALISIS DE LAS DIMENSIONES DE SEGURIDAD EN LOS OBJETIVOS DE CONTROL DE COBIT V4.1”

AUTORES:

CRUZ QUINZO BETHY JANNETH

CHAMORRO NOBOA JUAN CARLOS

DIRECTOR: ING. JAIRO NAVARRO

SANGOLQUI, 2014

CERTIFICADO

ESPE
UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

Sangolquí, 4 de julio de 2014

Sr. Ing. Rubén Arroyo MSc.
COORDINADOR DE LA MAESTRÍA EN EVALUACIÓN Y AUDITORÍA DE SISTEMAS TECNOLÓGICOS

ASUNTO: CULMINACION O FINALIZACIÓN DEL PROYECTO DE GRADUACIÓN

Por medio de la presente Yo, Ing. Jairo Navarro Bustos MSc., en calidad de Director del Proyecto de Graduación Titulado: "EVALUACIÓN DE RIESGOS DE LOS SISTEMAS DE INFORMACIÓN DE AUDIOAUTO S.A. UTILIZANDO MAGERIT 3.0 APOYADOS PARA EL ANÁLISIS DE LAS DIMENSIONES DE SEGURIDAD EN LOS OBJETIVOS DE CONTROL DE COBIR 4.1", desarrollado por los señores Ingenieros Juan Carlos Chamorro Noboa y Bethy Janneth Cruz Quinzo, egresados de la Maestría en Evaluación y Auditoría de Sistemas Tecnológicos, pongo en su conocimiento que el Proyecto se encuentra concluido y cumple con todos los parámetros de exigencia, por lo que solicito se digne disponer la evaluación correspondiente.

Solicito además, brindar las facilidades para la Defensa Final ante el Tribunal de Graduación.

Atentamente,

Ing. Jairo Navarro Bustos MSc.
DIRECTOR DEL PROYECTO

VICERRECTORADO DE INVESTIGACIÓN Y VINCULACIÓN CON LA COLECTIVIDAD

MAESTRIA EN EVALUACION Y AUDITORIA DE SISTEMAS TECNOLOGICOS

IV – B – PROMOCION 2011 - 2012

DECLARACION DE RESPONSABILIDAD

Cruz Quinzo Bethy Janneth

Chamorro Noboa Juan Carlos

DECLARAMOS QUE:

La Tesis de Grado denominada: "EVALUACIÓN DE RIESGOS DE LOS SISTEMAS DE INFORMACIÓN DE AUDIOAUTO S.A. UTILIZANDO MAGERIT V3.0 APOYADOS PARA EL ANALISIS DE LAS DIMENSIONES DE SEGURIDAD EN LOS OBJETIVOS DE CONTROL DE COBIT V4.1", ha sido desarrollada en base a una investigación exhaustiva, respetando derechos intelectuales de terceros, conforme a las citas que constan el pie de las paginas correspondientes, cuyas fuentes se incorporan en la bibliografía.

Consecuentemente este trabajo es de nuestra autoría.

En virtud de esta declaración, nos responsabilizamos del contenido, veracidad y alcance científico de la tesis de grado en mención.

Sangolqui, Diciembre 2014

Bethy Janneth Cruz Quinzo

Juan Carlos Chamorro Novoa

VICERRECTORADO DE INVESTIGACIÓN Y VINCULACIÓN CON LA COLECTIVIDAD

MAESTRIA EN EVALUACION Y AUDITORIA DE SISTEMAS TECNOLOGICOS

IV – B – PROMOCION 2011 – 2012

AUTORIZACION PUBLICACION EN LA BIBLIOTECA VIRTUAL

Cruz Quinzo Bethy Janneth

Chamorro Noboa Juan Carlos

AUTORIZAMOS:

A que la Tesis de Grado denominada: "EVALUACIÓN DE RIESGOS DE LOS SISTEMAS DE INFORMACIÓN DE AUDIOAUTO S.A. UTILIZANDO MAGERIT V3.0 APOYADOS PARA EL ANALISIS DE LAS DIMENSIONES DE SEGURIDAD EN LOS OBJETIVOS DE CONTROL DE COBIT V4.1", pueda ser publicada en la Biblioteca Virtual de la ESPE.

Sangolqui, Diciembre 2014

Bethy Janneth Cruz Quinzo

Juan Carlos Chamorro Novoa

DEDICATORIA

A mis seres queridos que siempre me apoyan.

Con amor. Bethy.

AGRADECIMIENTO

Queremos expresar nuestro reconocimiento y gratitud a nuestros profesores por compartir su conocimiento y experiencia, de igual forma agradecemos a nuestras familias que con su apoyo y comprensión nos permitieron realizar la maestría y desarrollar el tema de Tesis.

Al Ing. Jairo Navarro por su dirección.

Al Ing. Raúl Arroyo director de la Maestría.

Al Ing. Carlos Procel, oponente.

Al Ing. Mario Ron.

A Debbie Perez.

A todos, muchas gracias.

INDICE DE CONTENIDO

INDICE DE TABLAS

INDICE DE FIGURAS

RESUMEN.

TEMA: “EVALUACIÓN DE RIESGOS DE LOS SISTEMAS DE INFORMACIÓN DE AUDIOAUTO S.A. UTILIZANDO MAGERIT V3.0 APOYADOS PARA EL ANALISIS DE LAS DIMENSIONES DE SEGURIDAD EN LOS OBJETIVOS DE CONTROL DE COBIT V4.1”

La presente tesis tiene como objetivo realizar la Evaluación de Riesgos de los Sistemas de Información de Audioauto S.A mediante la aplicación de la metodología MAGERIT y apoyados en los Objetivos de control de COBIT con el fin de determinar la situación de riesgo en que la que se encuentran y establecer las acciones que se deben tomar para controlarlo y mitigarlo, para este análisis nos enfocarnos en la Disponibilidad, Integridad, Confidencialidad, Autenticidad y Trazabilidad como las dimensiones de Seguridad sugeridas por MAGERIT para Evaluar y Gestionar el Riesgo, en lo concerniente al proceso de evaluación de riesgos, determinamos los principales Activos de TI mediante un levantamiento de la estructura interna de la organización, los principales procesos del negocio y los Sistemas de Información que los soportan así como su interrelación y valor, aplicamos MAGERIT para realizar una caracterización y valoración cuantitativa de los Activos e identificamos las amenazas a las que están expuestos, las salvaguardas existentes y aquellas que se podrían implementar. Estimamos la efectividad de las salvaguardas frente al riesgo, el impacto derivado de la materialización de la amenaza y el riesgo, posteriormente desde la

perspectiva de la Optimización del Riesgo de COBIT en las dimensiones Financiera, Cliente e Interna, establecemos las debilidades relacionadas con el Gobierno y Gestión de TI, como resultado de esta evaluación, habiendo aplicado MAGERIT y COBIT determinamos el Riesgo a el que se encuentran expuestos los principales Activos de TI, y las áreas en las que se requiere priorizar la Optimización del Riesgo.

PALABRES CLAVES:

- **EVALUACION DE RIEGOS**
- **SISTEMAS DE INFORMACION**
- **METODOLOGIA**
- **OBJETIVOS DE CONTROL**
- **SEGURIDAD.**

ABSTRACT

This thesis aims to perform Risk Assessment of Information Systems SA Audioauto by applying the methodology MAGERIT and supported in the COBIT control objectives in order to determine the level of the risk and establish actions to be taken to control and mitigate, for this analysis we focus on Availability, Integrity, Confidentiality, Authenticity and Traceability as the dimensions of Security suggested by MAGERIT for Evaluating and Managing Risk, with regard to the risk assessment process, we determine the main IT Assets through a lifting of the internal structure of the organization, key business processes and information systems that support their interrelation and value, we apply MAGERIT for characterization and quantitative assessment of the assets and identify the threats they are exposed, the existing safeguards and those that could be implemented. We estimate the effectiveness of safeguards against the risk, the impact of the realization of the threat and risk, subsequently, from the perspective of COBIT Optimization Risks in Financial, Client and Internal Dimensions, we establish weaknesses related to IT Governance and Management, as a result of this evaluation, after apply MAGERIT and COBIT, we determine the risk to which they are exposed major IT Assets, and the areas that require to be prioritized in risk optimization.

CAPÍTULO 1.- INTRODUCCIÓN Y MARCO TEÓRICO

1.1. INTRODUCCIÓN

Audioauto es una empresa dedicada a brindar servicios de Localización Satelital de todo tipo de vehículos y maquinaria pesada, siendo esta actividad dependiente directamente de tecnologías de información y comunicaciones.

Este tipo de actividades requieren plataformas tecnológicas que administren sistemas de información y comunicaciones que interactúan por una parte con los dispositivos de localización y por otra parte con los usuarios del servicio en tiempo real, debiendo mantener un alto grado de precisión y confidencialidad.

En base a estos antecedentes toma especial importancia la realización de la Evaluación de Riesgos de los Sistemas de Información como el primer paso para el establecer su adecuada Gestión, base fundamental del buen Gobierno de TI.

MAGERIT V3.0 nos brinda los procedimientos, técnicas y herramientas necesarias para la realización de esta Evaluación y apoyados en los Objetivos de Control de COBIT V4.1, lograremos un acertado nivel de análisis y determinación del Modelo de Valor, Mapa de Riesgos, Evaluación de las Salvaguardas, Estado del Riesgo y Cumplimiento de Normas Legales.

1.2. JUSTIFICACIÓN E IMPORTANCIA

1.2.1. Estado del arte a nivel mundial y local

A nivel mundial, así como en nuestro país y sobre todo en organizaciones que brindan servicios relacionados con tecnologías de información, la seguridad y disponibilidad de la información no son un valor agregado, si no que forma parte del servicio en sí mismo y por ende es un requisito fundamental.

De igual manera debemos estar conscientes que alta demanda y la dependencia cada vez más creciente de los servicios de TI en las actividades cotidianas, hace que ante una deficiencia en ellos, se ponga en riesgo a quien usa estos servicios y a la organización que los provee.

Microsoft expone en su metodología “Guía de Administración de Riesgos” (Kurt Dillard (MSS), Jared Pfost (SCOE), 2004) que las infraestructuras de TI extremadamente conectadas de hoy en día existen en un entorno que es cada vez más hostil debido a los ataques frecuentes, nuevas legislaciones que incluyen preocupaciones de privacidad, obligaciones financieras, gobierno corporativo, entre otras, obligan a que la seguridad se administre proactivamente, para minimizar o evitar los riesgos a los cuales están expuestos ejecutivos y las organizaciones.

En la presentación realizada por José Ángel Peña Ibarra Vicepresidente de ISACA (Ibarra, 2010) expone algunas de las Metodologías y Normas más relevantes para el análisis de riesgos como:

1.2.2. OCTAVE (Operationally Critical Thread, Asset and Vulnerability Evaluation).-

Está enfocada a que la organización sea capaz de:

- Dirigir y gestionar sus evaluaciones de riesgos.
- Tomar decisiones basándose en sus riesgos.
- Proteger los activos claves de información.
- Comunicar de forma efectiva la información clave de seguridad.

Es coadyuvante en el Aseguramiento de la continuidad del negocio. Apoya la definición del riesgo y amenazas basadas en los activos críticos. Establece las Estrategias de protección y mitigación de riesgos basada en prácticas. Recopilación de datos en función de los objetivos.

1.2.3. MAGERIT (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información)

Consta de cuatro fases:

- Planificación del Proyecto de Riesgos: estimaciones iniciales de los riesgos que pueden afectar al sistema de información así como del tiempo y los recursos que su tratamiento conllevará.

- Análisis de Riesgos: estimando el impacto que tendrán los riesgos en la organización.

- Gestión de Riesgos: se seleccionan posibles soluciones para cada riesgo.

- Selección de Salvaguardas: se seleccionan los mecanismos que implementarán las soluciones seleccionadas.

Objetivos Directos:

- Concienciar a los responsables de las organizaciones de información de la existencia de riesgos y de la necesidad de gestionarlos.

- Ofrecer un método sistemático para analizar los riesgos derivados del uso de Tecnologías de la Información y Comunicaciones (TIC).

- Ayudar a descubrir y planificar el tratamiento oportuno para mantener los riesgos bajo control.

Objetivos Indirectos:

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

1.2.4. Estándar Internacional ISO/IEC 27005

Describe las recomendaciones y directrices generales para la gestión de riesgos en sistemas de seguridad de la información, poniendo énfasis en la Identificación de riegos, su Evaluación, Análisis de Riesgo contrastado con la organización, Establecimiento de Escenarios de Riesgo y Respuesta a los Riesgos.

1.2.4.1. RiskITISACA

Establece las mejores prácticas con el fin de establecer un marco para las organizaciones para identificar, gobernar y administrar los riesgos

asociados a su negocio. Es utilizado para ayudar a implementar el gobierno de TI y, las organizaciones que han adoptado (o están planeando adoptar) COBIT como marco de su gobierno de TI.

Los eventos internos pueden incluir los incidentes operacionales, los fracasos del proyecto, cambios de la estrategia de TI y las fusiones. Los eventos externos pueden incluir, cambios en las condiciones del mercado, nuevos competidores, nuevas tecnologías disponibles y las nuevas regulaciones que le afectan. Estos eventos, plantean un riesgo y una oportunidad para evaluar el mismo y generar las soluciones oportunas. La dimensión del riesgo y, cómo gestionarlo, es el tema principal de RISK IT.

Luego de haber evaluado algunas de las metodologías existentes para el Análisis de Riesgo, hemos observado que para el objeto de estudio que vamos a realizar MAGERIT junto a los objetivos de control de COBIT, nos permitirán obtener un acertado enfoque y nivel de profundidad.

Entre las ventajas de MAGERIT tenemos que las decisiones que deban tomarse y que tengan que ser validadas por la dirección estarán fundamentadas y serán fácilmente defendibles.

La principal desventaja de MAGERIT es el hecho de que traducir de forma directa todos los activos de riesgo en valores económicos hace que la aplicación de esta metodología pueda ser costosa.

Según MAGERIT (Dirección General de Modernización Administrativa, 2012), Seguridad es la capacidad de las redes o de los sistemas de información para resistir, con un determinado nivel de confianza, los accidentes o acciones ilícitas o malintencionadas que comprometan la disponibilidad, autenticidad, integridad y confidencialidad de la información almacenada o transmitida y de los servicios que dichas redes y sistemas ofrecen o hacen accesibles.

1.3. PLANTEAMIENTO DEL PROBLEMA

Las amenazas y vulnerabilidades derivadas de la complejidad tecnológica de Audioauto S.A., su necesidad por mantener un alto nivel de integridad, disponibilidad y confidencialidad de la información, generan la existencia un alto nivel de riesgo en los Sistemas de Información que puede impedir el cumplimiento de su misión y generar consecuencias financieras y legales.

1.3.1. Formulación del Problema a Resolver

Los riesgos relacionados con los Sistemas de Información no han sido evaluados metodológicamente y, por consiguiente no se han determinado los lineamientos sobre los cuales la organización realice una adecuada Gestión de Riesgos, por este motivo se realizará la Evaluación de Riesgos generando la los informes respectivos.

1.4. MARCO TEÓRICO

MAGERIT, señala que hay varias aproximaciones al problema de analizar los riesgos soportados por los sistemas TIC: guías informales, aproximaciones metódicas y herramientas de soporte. Todas buscan objetivar el análisis de riesgos para saber cuán seguros o inseguros son los sistemas y no llamarse a engaño.

El gran reto de todas estas aproximaciones es la complejidad del problema al que se enfrentan; complejidad en el sentido de que hay muchos elementos que considerar y que, si no se es riguroso, las conclusiones serán de poco fiar. Es por ello que en MAGERIT se persigue una aproximación metódica que no deje lugar a la improvisación, ni dependa de la arbitrariedad del analista.

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

Siguiendo la terminología de la normativa ISO 31000, Magerit responde a lo que se denomina “Proceso de Gestión de los Riesgos”, sección 4.4 (“Implementación de la Gestión de los Riesgos”) dentro del “Marco de Gestión de Riesgos”.

Para analizar el Riesgo MAGERIT nos plantea las siguientes definiciones:

- **Riesgo:** estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la Organización. El riesgo indica lo que le podría pasar a los activos si no se protegieran adecuadamente. Es importante saber qué características son de interés en cada activo, así como saber en qué medida estas características están en peligro, es decir, analizar el sistema.

- **Análisis de riesgos:** proceso sistemático para estimar la magnitud de los riesgos a que está expuesta una Organización. Sabiendo lo que podría pasar, hay que tomar decisiones.

- **Tratamiento de los riesgos:** es un proceso destinado a mitigar el riesgo.

Hay múltiples formas de tratar un riesgo: evitar las circunstancias que lo provocan, reducir las posibilidades de que ocurra, acotar sus consecuencias, compartirlo con otra organización (típicamente contratando un servicio o un

seguro de cobertura), o, en última instancia, aceptando que pudiera ocurrir y previendo recursos para actuar cuando sea necesario.

Nótese que una opción legítima es aceptar el riesgo. Es frecuente oír que la seguridad absoluta no existe; en efecto, siempre hay que aceptar un riesgo que, eso sí, debe ser conocido y sometido al umbral de calidad que se requiere del servicio.

Es más, a veces aceptamos riesgos operacionales para acometer actividades que pueden reportarnos un beneficio que supera al riesgo, o que tenemos la obligación de afrontar. Es por ello que a veces se emplean definiciones más amplias de riesgo: Efecto de la incertidumbre sobre la consecución de los objetivos.

Como todo esto es muy delicado, no es meramente técnico, e incluye la decisión de aceptar un cierto nivel de riesgo, deviene imprescindible saber en qué condiciones se trabaja y así poder ajustar la confianza que merece el sistema. Para ello, qué mejor que una aproximación metódica que permita tomar decisiones con fundamento y explicar racionalmente las decisiones tomadas.

Según MAGERIT, las dimensiones de seguridad a evaluar para Gestionar el Riesgo son:

Disponibilidad: O disposición de los servicios a ser usados cuando sea necesario. La carencia de disponibilidad supone una interrupción del servicio. La disponibilidad afecta directamente a la productividad de las organizaciones.

Integridad: O mantenimiento de las características de completitud y corrección de los datos. Contra la integridad, la información puede aparecer

manipulada, corrupta o incompleta. La integridad afecta directamente al correcto desempeño de las funciones de una Organización.

Confidencialidad: O que la información llegue solamente a las personas autorizadas. Contra la confidencialidad o secreto pueden darse fugas y filtraciones de información, así como accesos no autorizados. La confidencialidad es una propiedad de difícil recuperación, pudiendo minar la confianza de los demás en la organización que no es diligente en el mantenimiento del secreto, y pudiendo suponer el incumplimiento de leyes y compromisos contractuales relativos a la custodia de los datos.

De estas dimensiones primordiales de la seguridad se derivan otras que nos acerquen a la percepción de los usuarios de los sistemas de información:

Autenticidad: Propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos. Contra la autenticidad de la información podemos tener manipulación del origen o el contenido de los datos. Contra la autenticidad de los usuarios de los servicios de acceso, podemos tener suplantación de identidad.

Trazabilidad: Aseguramiento de que en todo momento se podrá determinar quién hizo qué y en qué momento. La trazabilidad es esencial para analizar los incidentes, perseguir a los atacantes y aprender de la experiencia. La trazabilidad se materializa en la integridad de los registros de actividad. Todas estas características pueden ser requeridas o no dependiendo de cada caso. Cuando se requieren, no es evidente que se disfruten sin más. Lo habitual que haya que poner medios y esfuerzo para conseguirlas.

El proceso que sigue MAGERIT para la evaluación de riesgos consiste en determinar los activos más relevantes, su interrelación y valor,

posteriormente se identifican las amenazas a las que están expuestos y las salvaguardas que se podrían implementar y su efectividad frente al riesgo. Con esto se estima el impacto sobre el activo derivado de la materialización de la amenaza y el riesgo, definido como el impacto ponderado con la tasa de ocurrencia. A continuación se muestra el diagrama de los procesos:

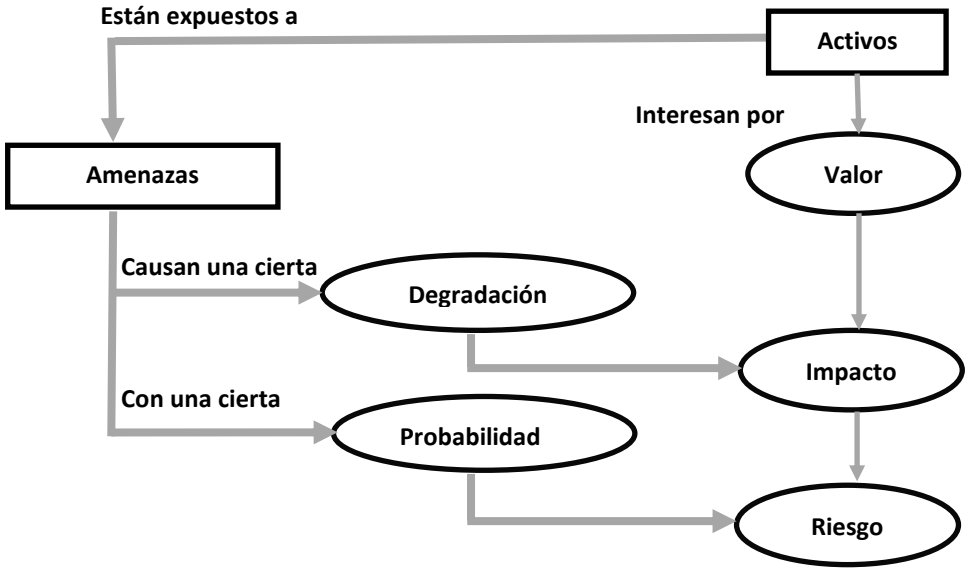

Figura 1. Procesos MAGERIT

COBIT, quiere decir Objetivos de Control para las Tecnologías de la Información y relacionadas.

La Misión de COBIT: Es Investigar, desarrollar, hacer público y promover un marco de control de gobierno de TI autorizado, actualizado, aceptado internacionalmente para la adopción por parte de las empresas y el uso diario por parte de gerentes de negocio, profesionales de TI y profesionales de aseguramiento.

Nace de la necesidad de un marco de trabajo de control para el Gobierno de TI, esto debido a que cada vez más, la alta dirección se está dando cuenta del impacto significativo que la información puede tener en el éxito de una empresa.

La alta dirección necesita saber si con la información administrada en la empresa es posible que:

- Se pueda lograr que toda la estrategia de TI, así como las metas fluyan de forma gradual a toda la empresa.

- Garantice el logro de sus objetivos

- Tenga suficiente flexibilidad para aprender y adaptarse

- Cuente con un manejo juicioso de los riesgos que enfrenta

- Reconozca de forma apropiada las oportunidades y actúe de acuerdo a ellas.

Considerandos estas necesidades los componentes de COBIT dan un marco de trabajo integrado para la entrega de valor, administrando los riesgos y el control sobre los datos y la información, enfocándose en la mejora del gobierno de TI en las organizaciones, actúa como un integrador de todos estos materiales guía, alineando la estrategia de TI con la estrategia del negocio.

1.4.1. MARCO DE TRABAJO COBIT

El marco de trabajo COBIT se creó con las características principales de ser orientado a negocios, orientado a procesos, basado en controles e impulsado por mediciones.

Orientado al negocio: La orientación a negocios es el tema principal de COBIT. Está diseñado para ser utilizado no sólo por proveedores de servicios, usuarios y auditores de TI, sino también y principalmente, como guía integral para la gerencia y para los dueños de los procesos de negocio.

Orientado a Procesos: COBIT define las actividades de TI en un modelo genérico de procesos organizado en cuatro dominios. Estos dominios son Planear y Organizar, Adquirir e Implementar, Entregar y Dar Soporte y Monitorear y Evaluar. Los dominios se equiparan a las áreas tradicionales de TI de planear, construir, ejecutar y monitorear.

También brinda un marco de trabajo para la medición y monitoreo del desempeño de TI, comunicándose con los proveedores de servicios e integrando las mejores prácticas de administración.

Un modelo de procesos fomenta la propiedad de los procesos, permitiendo que se definan las responsabilidades.

Para gobernar efectivamente TI, es importante determinar las actividades y los riesgos que requieren ser administrados.

Normalmente se ordenan dentro de dominios de responsabilidad de plan, construir, ejecutar y Monitorear, el principio básico de COBIT, se muestra en el diagrama:

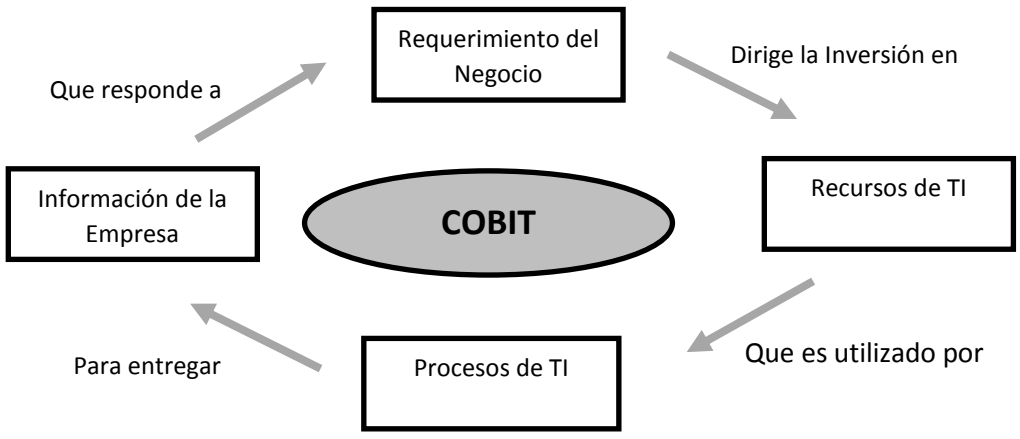

Figura 2. Principio Básico de COBIT

Para resumir, los recursos de TI son manejados por procesos de TI para lograr metas de TI que respondan a los requerimientos del negocio. Este es el principio básico del marco de trabajo COBIT, el cual se ilustra en el cubo:

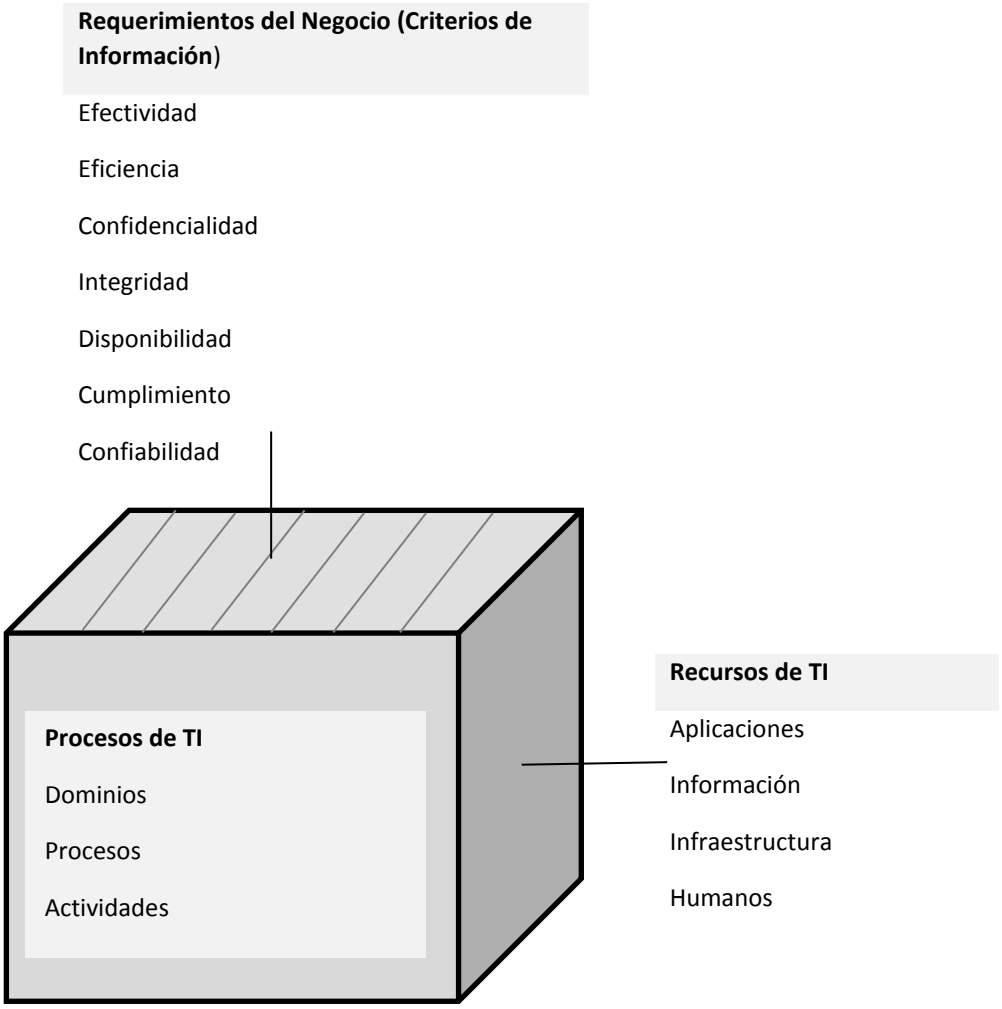

Figura 3. Ilustración Cubo COBIT

1.4.2. Cubo de COBIT - Criterios de Información:

Efectividad: Tiene que ver con que la información sea relevante y pertinente para los procesos del negocio, así como que sea entregada de manera oportuna, correcta, consistente y utilizable.

Eficiencia: Concierne con que la entrega de información se haga mediante la utilización óptima de los recursos

Confidencialidad: Tiene que ver con la protección de la información sensible contra divulgación no autorizada

Integridad: Se refiere a la precisión y completitud de la información, así como a su validez de acuerdo con los valores y expectativas del negocio

Disponibilidad: Se refiere a que la información debe estar disponible cuando la requieran los procesos del negocio ahora y en el futuro. También concierne a las salvaguardas de los recursos necesarios y sus capacidades necesarias asociadas.

Cumplimiento: Tiene que ver con al acatamiento de aquellas leyes, regulaciones y compromisos contractuales a los cuales están sujetos los procesos del negocio, es decir, criterios de negocio impuestos externamente así como políticas internas

Confiabilidad: Se relaciona con la provisión de la información apropiada para que la gerencia administre la entidad y ejerza sus responsabilidades de confianza y gobierno

1.4.3. Cubo de COBIT - Procesos de TI

Los procesos de TI manejan recursos tecnológicos para generar, entregar y almacenar la información que la organización necesita para alcanzar sus objetivos. Se ordenan dentro de dominios de responsabilidad de plan, construir, ejecutar y Monitorear. Dentro del marco de COBIT, estos dominios, se llaman:

Planear y Organizar: Proporciona dirección para la entrega de soluciones y la entrega de servicio.

Adquirir e Implementar: Proporciona las soluciones y las pasa para convertirlas en servicios.

Entregar y Dar Soporte: Recibe las soluciones y las hace utilizables por los usuarios finales.

Monitorear y Evaluar: Monitorear todos los procesos para asegurar que se sigue la dirección provista.

A lo largo de estos cuatro dominios, COBIT ha identificado 34 procesos de TI generalmente usados, y que tienen un enlace a las metas del negocio, que son utilizados para verificar que se completan las actividades y responsabilidades. Sin embargo, no es necesario que apliquen todos los procesos, y más aún, se pueden combinar como se necesite por cada empresa.

1.4.4. Cubo de COBIT - Recursos de TI

Los recursos de TI identificados en COBIT se definen así:

Aplicaciones: Son tanto los sistemas automatizados de usuario como los procedimientos manuales con los que se procesa la información.

Información: Son los datos de cualquier forma utilizados por el negocio, que entran a, son procesados por y salen de los sistemas de información.

Infraestructura: Es la tecnología y las instalaciones (hardware, sistemas operativos, sistemas de administración de base de datos, redes, multimedia, etc., así como el sitio donde se encuentran y el ambiente que los soporta) que permiten el procesamiento de las aplicaciones.

Humanos: Son los recursos humanos requeridos para planear, organizar, adquirir, implementar, entregar, soportar, monitorear y evaluar los sistemas y los servicios de información.

1.5.- TECNOLOGÍAS DE RASTREO SATELITAL

1.5.1. QUE ES EL RASTREO SATELITAL.

Es un sistema que integra varias tecnologías, que permiten al dueño de un vehículo saber dónde se encuentra éste en tiempo real, inclusive saber dónde estuvo durante los días anteriores y sus recorridos. También se puede utilizar el rastreo directo en monitoreo de personal, para lo cual se utilizan dispositivos adecuados para tal necesidad.

1.5.2. COMO FUNCIONA

Este sistema de rastreo hace uso de varias tecnologías de posicionamiento y telecomunicaciones, éste sistema funciona a través de equipos GPS (sistema de posicionamiento global), señales celulares, mapas digitalizados y comunicación vía Internet. Todos coordinados por un software

profesional con el respaldo de un staff de ingenieros altamente calificados y entrenados directamente de fábrica.

En el vehículo a rastrear se instala un dispositivo transmisor en un lugar secreto y convenientemente mimetizado (para evitar que sea saboteado). La instalación toma poco tiempo en un máximo de dos horas. El vehículo con el GPS instalado transmitirá constantemente su ubicación por medio de una señal celular que es recibida y computada por un servidor y subida en tiempo real a una página web. A dicha página web solamente acceder el propietario de dicho vehículo mediante un nombre de usuario y contraseña. También existen dispositivos para el rastreo de personas (fuerza de ventas, personal que trabaja fuera de oficina, etc.) y para el rastreo de carga, los que funcionan con AGPS (sistema de posicionamiento global asistido) que permite transmitir su ubicación aún desde el interior de estructuras sólidas como edificios o viviendas.

1.5.3. ACCESO VIA INTERNET

La persona interesada en conocer la posición y recorrido del vehículo, carga o personal puede ingresar a nuestra página web, teclear su usuario y contraseña y accederá a un mapa digital donde un icono representa la posición actual de su automóvil, camioneta, bus o camión. Puede usar zoom para alejarse y ver, si fuera el caso, toda una flota de vehículos en todo el país o acercarse más y ver por regiones, por ciudades o incluso hacer un acercamiento extremo y saber en qué calles está ubicado cada uno. La página web también genera reportes tabulados de tiempos y recorridos realizados en los días anteriores, hasta quince días atrás.

CAPÍTULO 2.- SITUACIÓN ACTUAL DE LA ORGANIZACIÓN

2.1. MISIÓN

La misión de Audioauto S.A, es: “Brindar tranquilidad a sus clientes cuando han sufrido un ataque por parte de la delincuencia, prestando la ayuda necesaria para localizar sus vehículos”.

2.2. VISIÓN

La visión de Audioauto S.A, es convertirse en la empresa líder para Latinoamérica y El Caribe en brindar servicios relacionados con tecnologías de localización satelital.

2.3. VALORES

Innovación: Pensando siempre en las necesidades del cliente, desarrollar e implementar tecnología para lograr nuevos y mejores servicios al cliente.

Respeto: A las personas y el medio ambiente para lograr una mejor forma de vida y el mejor lugar de trabajo.

Responsabilidad: Actuando con transparencia, eficiencia y eficacia en cada actividad.

Trabajo en Equipo: Generando la sinergia que necesaria para entregar servicios de calidad y en constante evolución.

Pasión: Por nuestro trabajo, siempre buscando y entregando los servicios con la calidad y calidez esperada.

2.4. ESTRUCTURA ORGANIZACIONAL

Audioauto S.A, es una organización con una estructura jerárquica con una Junta de Accionistas que se encargan de establecer los lineamientos que permitan encaminar la organización hacia el objetivo de lograr visión, así como evaluar los resultados de la gestión de la Gerencia General.

La Gerencia General se preocupa del cumplimiento de la misión, mediante la definición las de políticas organizacionales, el control y seguimiento de los objetivos estratégicos y financieros.

Las Gerencias de cada una de las áreas y regionales son las responsables por el cumplimiento de los objetivos específicos de cada función para que de forma armónica contribuyan para el cumplimiento de los objetivos estratégicos de la organización.

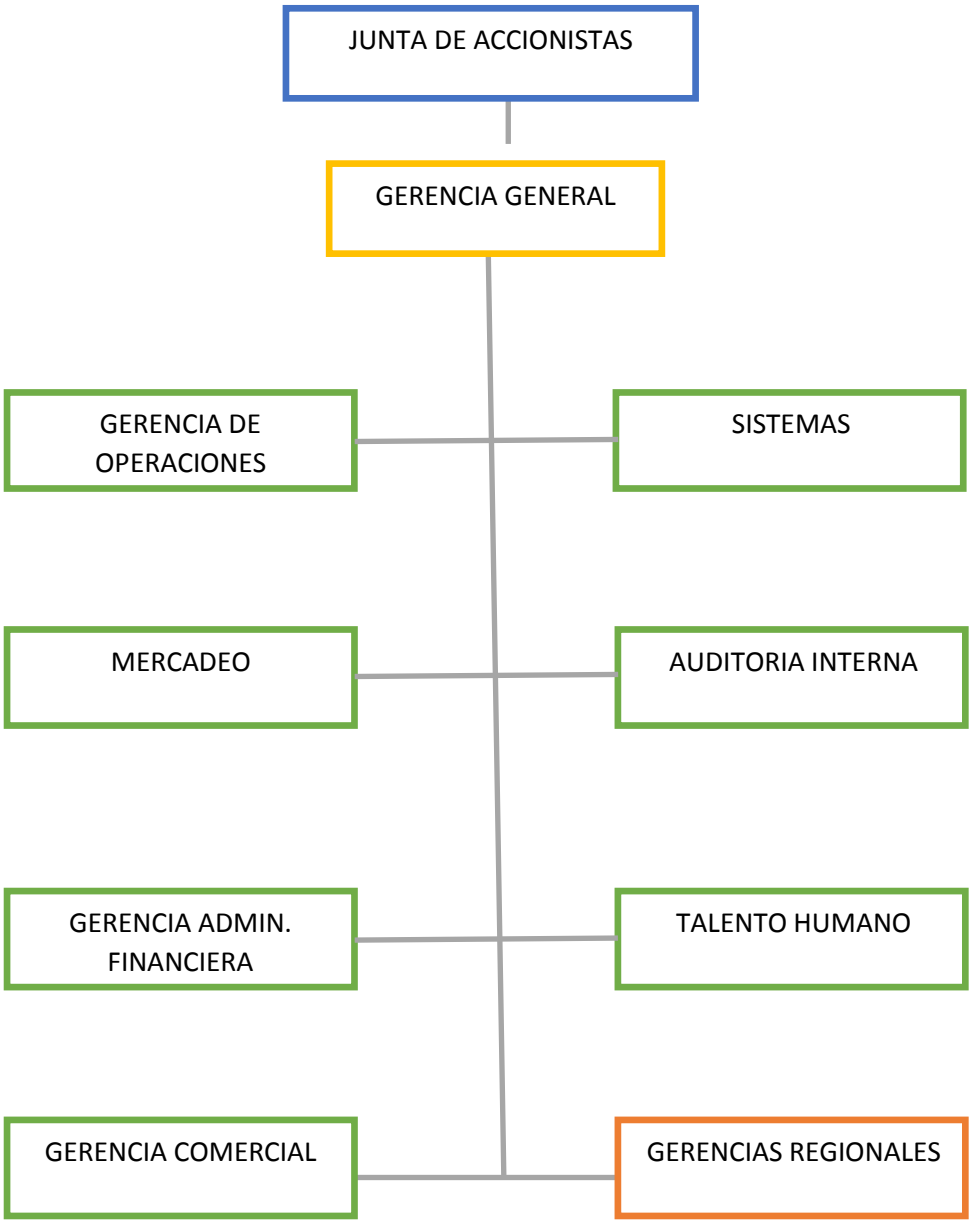

Figura 4. Estructura Organizacional

2.4.1. GERENCIA DE OPERACIONES

La gerencia de operaciones se encarga de los procesos relacionados con la producción de los sistemas de localización su configuración, instalación, así como la entrega de los servicios que ofrece la compañía a los clientes.

Entre sus responsabilidades también se encuentra el diseño e implementación de nuevas características funcionales y nuevos servicios relacionados con las tecnologías de localización satelital.

Los departamentos bajo su control son:

Ensamblaje: Se dedica a la producción de kits de dispositivos de localización y componentes electrónicos necesarios para soportar el catálogo de servicios de la compañía.

Instalaciones / Taller: Su tarea consiste en realizar la instalación de los dispositivos de localización en los vehículos, equipos y maquinarias que lo requieren, tanto dentro como fuera de las instalaciones.

Logística: Se encarga de coordinar las importaciones y compras de los componentes necesarios para la producción de los kits de dispositivos de localización.

Monitoreo: Es responsable de brindar el servicio de call center para dar soporte a los clientes cuando lo requieran, así como el gestionar la recuperación de los vehículos, equipos y maquinaria que hubiere sido robada, mediante la localización satelital y en coordinación con la fuerza de recuperación que es un servicio externo.

Innovación: Se encarga de diseñar los dispositivos electrónicos necesarios para implementar nuevas funcionalidades con nuevas tecnologías en los equipos de localización.

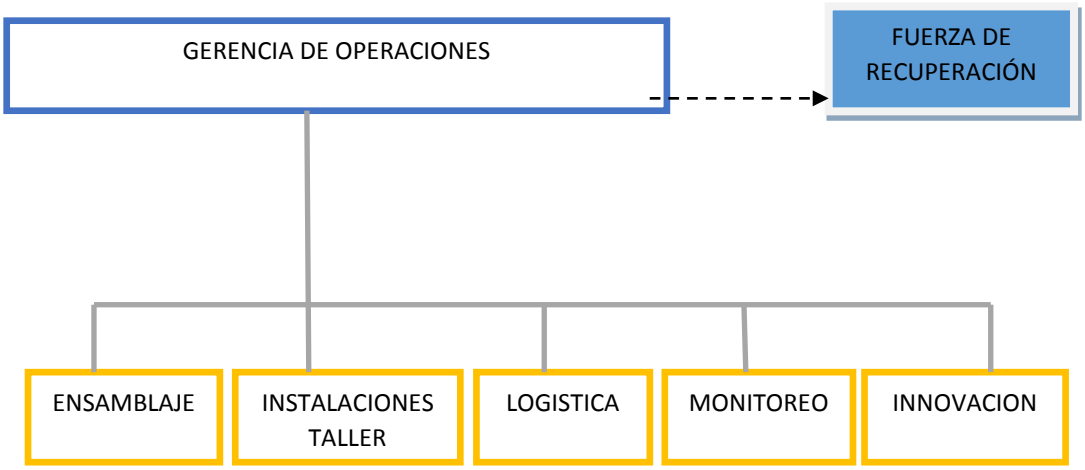

Figura 5. Estructura Gerencia Operaciones

2.4.2. MERCADEO

Mediante el análisis del mercado y sus tendencias busca lograr posicionar la marca, mediante el diseño y puesta en marcha de estrategias y tácticas que ayuden a conseguir este fin.

2.4.3. GERENCIA FINANCIERA Y ADMINISTRATIVA

Es responsable de velar por la adecuada administración de los recursos físicos y financieros, así como del seguimiento de los objetivos económicos y presupuestarios. Los departamentos bajo su control son:

Compras e Importaciones: Se encarga de proformar y realizar las compras e importaciones solicitadas por los diferentes departamentos en cumplimiento de las políticas y presupuesto establecido.

Inventarios: Se encarga del control del ingreso, egreso y transferencias de equipos y materiales entre las diferentes bodegas, así como del control del inventario de Activos Fijos.

Facturación y Caja: Es responsable por la emisión de las facturas por los bienes y servicios que brinda la organización, además la custodia del dinero y documentos recaudados por efecto de las ventas, así como también de la entrega de los valores correspondientes a los pagos a los proveedores.

Crédito y Cobranzas: Es responsable por la cobranza de los valores dados a crédito a los clientes y de otorgar créditos de acuerdo a las políticas de establecidas por la gerencia.

Contabilidad y Presupuesto: Es responsable del control y registro de todas las transacciones que generen información financiero contable, así como de velar por el cumplimiento de todas las normas contables y tributarias requeridas por el estado y organismos de control. Adicionalmente es responsable de controlar que todas las transacciones estén sujetas a los límites presupuestarios establecidos y de la administración de los recursos financieros de la organización.

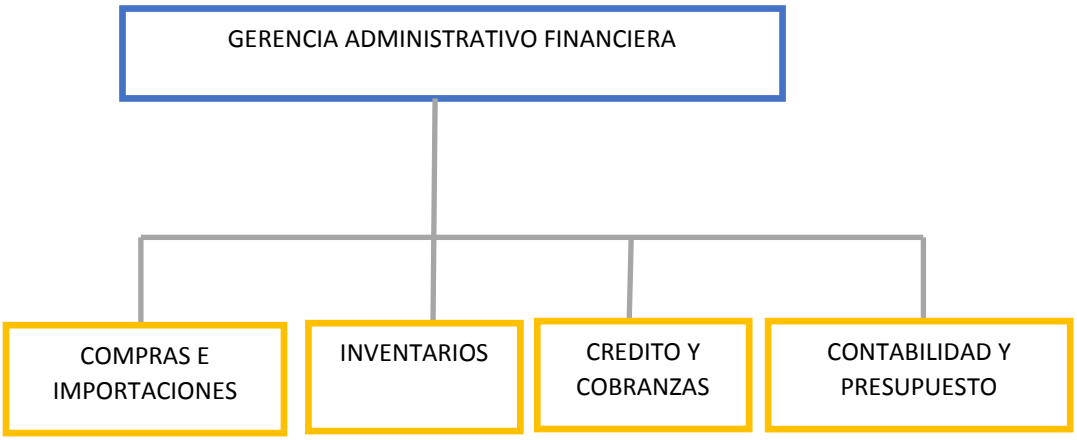

Figura 6. Estructura Gerencia Administrativo Financiera

2.4.4. GERENCIA COMERCIAL - GERENCIAS REGIONALES

La Gerencia Comercial, es responsable de velar por el cumplimiento de las metas de ventas que sustentan la operación de la compañía. Para este fin se han establecido las gerencias regionales encargadas de las ventas en un determinado territorio y al mismo tiempo tres departamentos encargados impulsar las ventas de sus líneas de negocio.

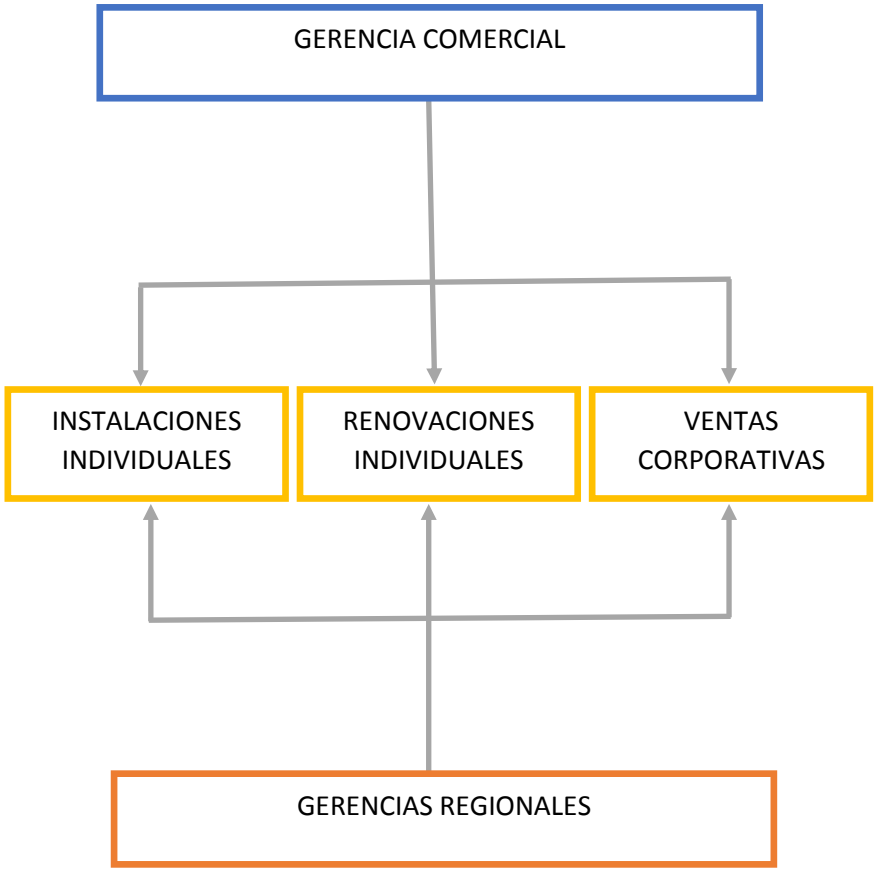

Figura 7. Estructura Gerencia Comercial – Gerencias Regionales

2.4.5. TALENTO HUMANO

Es responsable por impulsar las políticas necesarias para lograr el bienestar de los recursos humanos y su óptimo desempeño que permitan alcanzar los objetivos individuales, indispensables para el logro de los objetivos de la organización.

2.4.6. AUDITORIA INTERNA

En Audioauto S.A. la Auditoría Interna depende directamente de la Gerencia General y tiene a su cargo realizar el análisis sistemático de las actividades operativas y financieras de la organización para determinar si están enmarcadas en las Leyes, Normas, Reglamentos Públicos, así como del cumplimiento de las Políticas internas, para determinar anomalías y/o posibles deficiencias que puedan poner en riesgo a la organización. Esta actividad es apoyada también por las actividades que realizan las auditorías externas.

2.4.7. SISTEMAS

Es responsable del control y mantenimiento de toda la infraestructura de hardware y software. Entre sus actividades existen algunas soportadas directamente por su personal y otras mediante contratos con proveedores externos de servicios ocasionales y en otros casos mediante outsourcing.

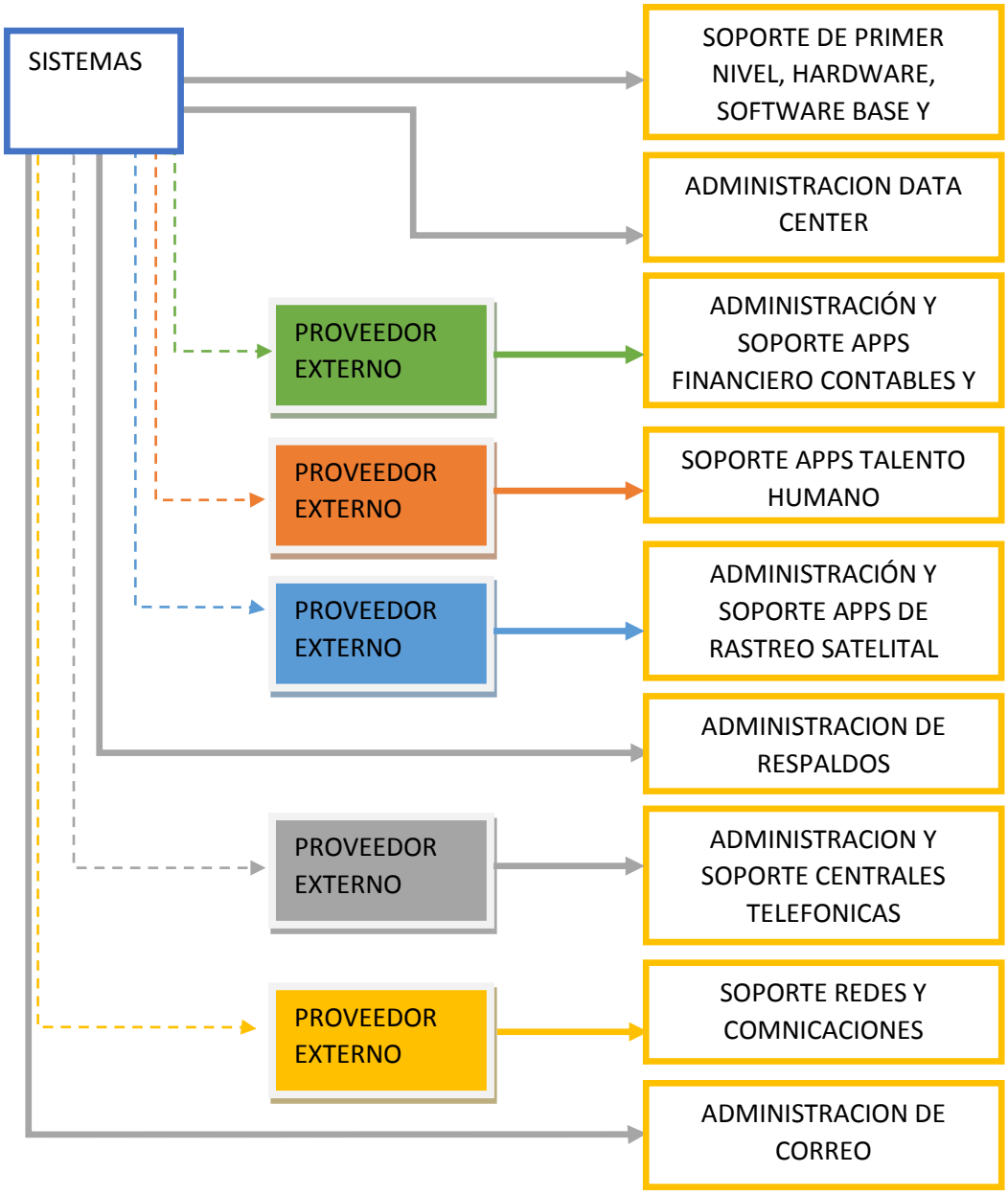

Figura 8. Estructura Sistemas

Soporte de Primer Nivel: Corresponde a aquellas actividades de configuración de hardware y software base, corresponde a PCs, Monitores, Impresoras, Sistemas Operativos, Herramientas de Oficina, Internet, Correo

y Mensajería y soporte para creación de usuarios, asignación de roles, accesos, etc.

Administración Data Center: Corresponde a un servicio tercerizado mediante contrato de mantenimiento para aquellas actividades orientadas a mantener en optimo estado el Data Center tanto a nivel físico como lógico en lo referente a Aire Acondicionado, Ups, Servidores, Discos, Switchs, Ruteadores, Bases Celulares, Actualización de Firmware y Sistemas Operativos en el área del Data Center.

Administración y Soporte de Aplicaciones Financiero Contables y Operaciones: Corresponde a un servicio tercerizado mediante contrato de outsourcing para el soporte, mantenimiento, desarrollo e implantación de los aplicativos que soportan la operación interna de la organización en lo referente a las Áreas Financiero, Contable, Auditoría, Operaciones, Comercial y Marketing.

Soporte de Aplicaciones de Talento Humano: Corresponde a un servicio tercerizado mediante contrato para el soporte y versionamiento de las aplicaciones de Talento Humano, como son: Selección, Evaluaciones, Recursos Humanos, Nomina.

Soporte de Aplicaciones de Rastreo Satelital: Corresponde a un servicio tercerizado de outsourcing para el soporte, mantenimiento, desarrollo e implantación de los aplicativos que soportan la extranet, la localización, mensajería entre los sistemas de localización satelital y los servidores de la compañía.

Aplicaciones de Respaldos: Corresponde a un las actividades relacionadas con la obtención de respaldos que permitan recuperar las operaciones en caso de un desastre.

Administración y Soporte de Centrales Telefónicas: Es un servicio externo, mediante contrato de soporte que se dedica al mantenimiento y configuración de las centrales telefónicas Elastix y Alcatel.

Soporte en Redes y Comunicaciones: Corresponde a un las actividades relacionadas con la obtención de respaldos que permitan recuperar las operaciones en caso de un desastre.

Administración de Correo: Es un servicio brindado por directamente por el departamento de Sistemas, para la administración de las cuentas de usuario.

2.5. ESTRUCTURA GEOGRÁFICA

Audioauto S.A. se distribuido geográficamente de la siguiente manera:

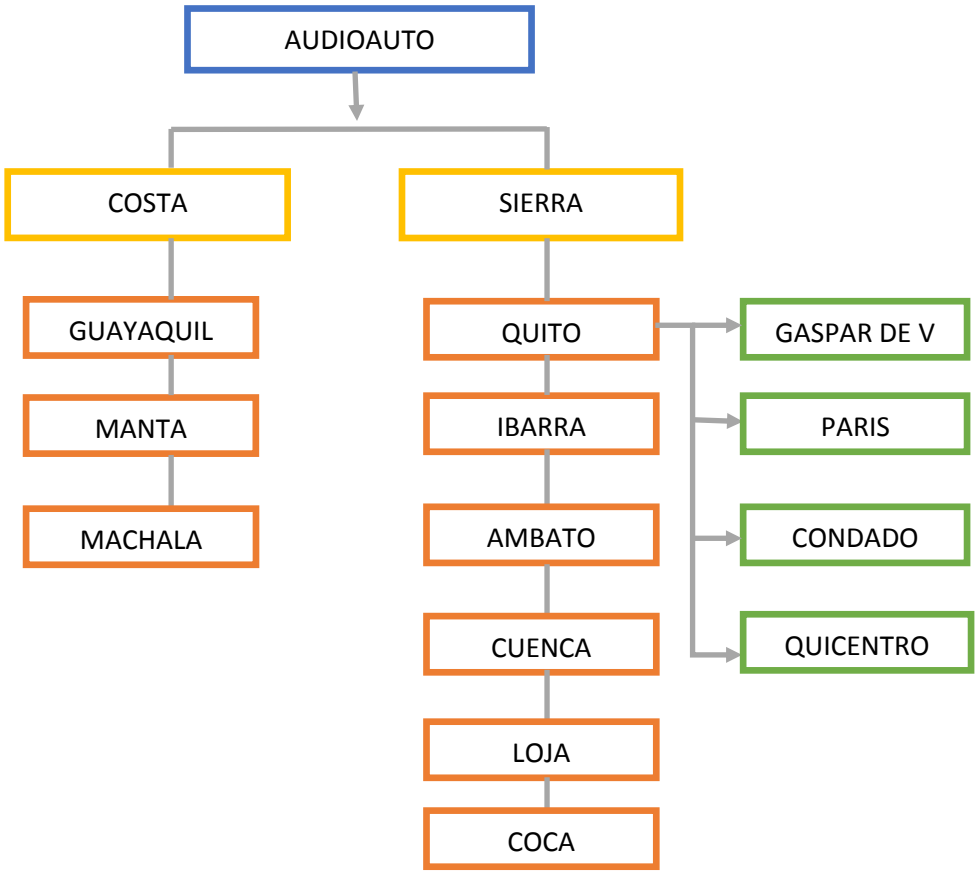

Figura 9. Estructura Geográfica

El centro de datos se encuentra ubicado en Quito, prestando servicios a todas las localidades mediante un enlace dedicado a Guayaquil y demás localidades de la sierra. A su vez desde Guayaquil se mantienen enlaces a las localidades de la costa.

2.6. DIAGRAMA DE RED

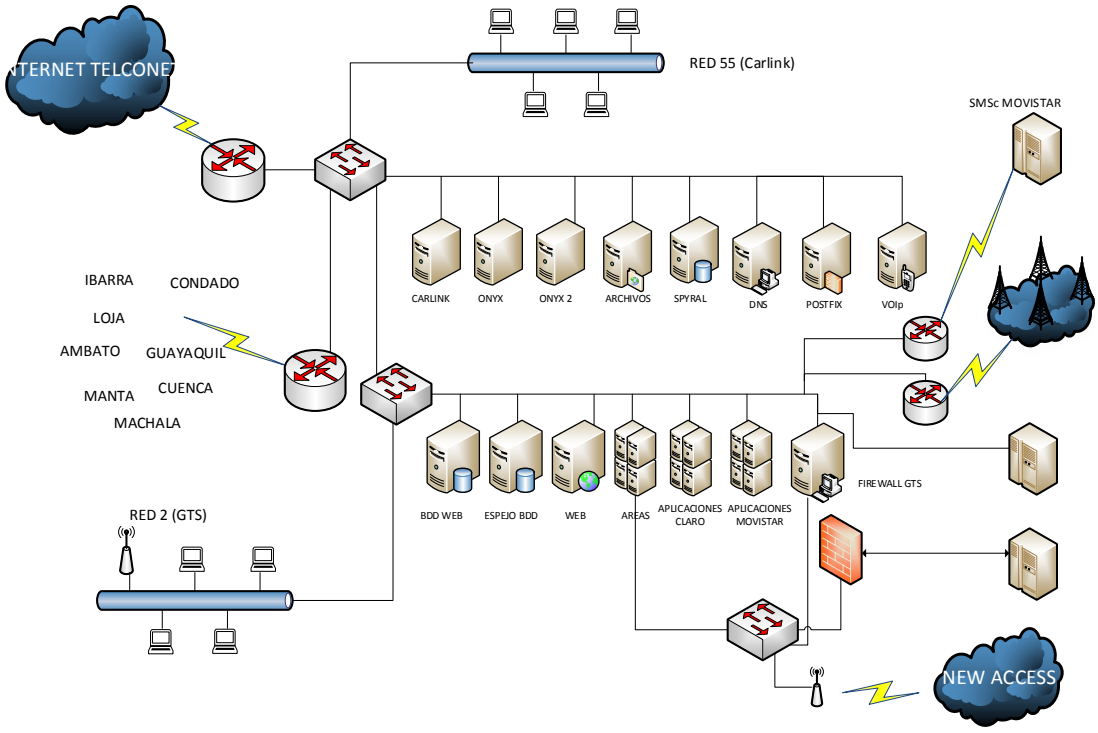

Figura 10. Diagrama de Red

CAPÍTULO 3.- EVALUACIÓN DE LOS RIESGOS

3.1. IDENTIFICACIÓN DE LOS ACTIVOS RELEVANTES DE TI

3.1.1. INFRAESTRUCTURA DE HARDWARE

3.1.1.1. Descripción de los centros de datos

- **Centro de datos UIO 1 contiene:**

Rack 1 ubicado en la parte posterior izquierda.

Rack 2 ubicado en la parte posterior derecha.

Rack 5 ubicado sobre una mesa ubicada en la parte delantera izquierda.

Rack 6 colocado sobre una mesa ubicada en la parte delantera derecha.

- **Centro de datos UIO 2 contiene:**

Rack 3 ubicado en la parte posterior izquierda.

Rack 4 ubicado en la parte posterior derecha.

Y a su vez cada uno de los Rack tienen varios niveles en los cuales se encuentran los diferentes servidores, cada nivel está denominado por una letra mayúscula.

3.1.1.2. Servidores de Correo

Tabla 1.

Servidores de Correo

Nombre	Sistema Operativo	Modelo	Procesador	Memoria	Disco	Ubicación
Srvmaildomprinc	Linux Fedora 15, Postfix	HP ML150	Intel(R) Xeon(R) CPU E5405 @ 2.00GHz, 4 cores	4Gb	250	Rack 6A
srvmaildomsec1	Linux Fedora 15, Postfix	Clon	Intel(R) Core(TM)2 CPU E7400 @ 2.80GHz, 2 cores	2Gb	800	Rack 5A
srvmaildomsec2	Linux Fedora 15, Postfix	Clon	Intel(R) Core(TM) i3-2100 CPU @ 3.10GHz, 4 cores	4Gb	400	Rack 5B

3.1.1.3. Servidores de Aplicación

Tabla 2.

Servidores de Aplicación

Nombre	Sistema Operativo	Modelo	Procesador	Memoria	Disco	Ubicación
srvcrm1	Linux Fedora 13, Glassfish V2R2	HP DL160G6	Intel(R) Xeon(R) CPU E5504 @ 2.00GHz, 4 cores	8Gb	250	Rack 1F
*srvcrm2	Linux Fedora 13, Glassfish V2R2	HP DL160G6	Intel(R) Xeon(R) CPU E5620 @ 2.40GHz, 8 cores	36Gb	500	Rack 1D
srvextranet1	Windows 2003, IIS Framework 2.0, Apache	HP DL360G5	Intel(R) Xeon(R) CPU 5140 @ 2.33GHz, 2 cores	4Gb	73	Rack 1K
srvextranet2	Windows 2008, IIS Framework 2.0, Apache	HP DL160G6	Intel(R) Xeon(R) CPU E5620 @ 2.40GHz, 8 cores	8Gb	500	Rack 1E
Srvrrhh	Windows 2008, Active Directory, Remote Desktop	HP DL160G6	Intel(R) Xeon(R) CPU E5620 @ 2.40GHz, 8 cores	4Gb	500	Rack 1M
Srvsky	Windows XP, skyapp	Clon	Intel(R) Core(TM)2 CPU E7400 @ 2.80GHz, 2 cores	2Gb	250	Rack 5C
Srvactfij	Windows XP, skyapp	Clon	Intel(R) Core(TM)2 CPU E7400 @ 2.80GHz, 2 cores	2Gb	250	Rack 3ª

3.1.1.4. Servidores de Base de Datos

Tabla 3.

Servidores de Bases de Datos

Nombre	Sistema Operativo	Modelo	Procesador	Memoria	Disco	Ubicación
Srvreports	Linux Fedora 17, MySQL 5.5.27	HP DL160G6	Intel(R) Xeon(R) CPU E5620 @ 2.40GHz, 8 cores	8Gb	500	Rack 1B
Srvareas	Linux Fedora 11, MySQL 5.1.47	HP DL160G6	Intel(R) Xeon(R) CPU E5504 @ 2.00GHz, 4 cores	6Gb	250	Rack 1E
srvsmsoper1	Linux Fedora 17, MySQL 5.5.27	HP DL160G6	Intel(R) Xeon(R) CPU E5620 @ 2.40GHz, 8 cores	8Gb	500	Rack 1G
srvsmsoper2	Linux Fedora 15, MySQL 5.5.14	HP DL160G6	Intel(R) Xeon(R) CPU E5620 @ 2.40GHz, 8 cores	8Gb	500	Rack 1L
*srvcrm2	Linux Fedora 13, MySQL 5.5.23	HP DL160G6	Intel(R) Xeon(R) CPU E5620 @ 2.40GHz, 8 cores	36Gb	500	Rack 1D
Srvmirror	Windows 2003 Server, SQLServer 2005	HP DL380G5	Intel(R) Xeon(R) CPU 5320 @ 1.90GHz, 4 cores	4Gb	292	Rack 1H
Srvbddextranet	Windows 2003 Server, SQLServer 2005	HP DL380G5	Intel(R) Xeon(R) CPU 5160 @ 3.00GHz, 4 cores	4Gb	892	Rack 1I
Srvfincon	Windows 2000 Server, SQLServer 2000	HP DL385G5	AMD Opteron (tm) CPU 254 @ 2.8Ghz	2Gb	108	Rack 1J
*srvcall1	Linux Core 2.6.18, Elastix, MySQL 5.0.77		Intel(R) Atom(TM) CPU D410 @ 1.66GHz	1Gb	300	Rack 3B
*srvcall2	Linux Core 2.6.18, Zycoo, MySQL 5.0.77		Intel(R) CPU N270 @ 1.60GHz	2Gb	300	Rack 4ª

3.1.1.5. Otros Servidores

Tabla 4.

Servidores Otros Servidores

Nombre	Sistema Operativo	Modelo	Procesador	Memoria	Disco	Ubicación
Srvdom	Windows 2000 Server, Active Directory	Compaq G2	Intel(R) Pemtium(R) III CPU Family @ 1.26GHz	1.2Gb	72	Rack 1N
Srvfiles	Windows 2000 AD Server	Compaq G2	Intel(R) Pemtium(R) III CPU Family @ 1.26GHz	0.6Gb	1000	Rack 1º

3.1.1.6. Equipos de Comunicaciones

Tabla 5.

Equipos de Comunicaciones

Nombre	Descripción	Destinado a	Ubicación
	Router x		Rack 2C
	Switch		Rack 2C
Alcatel1	Central Telefónica Alcatel E1	Brindar el servicio de comunicaciones	Rack 2C
*srvcall1	Linux Core 2.6.18, Elastix, MySQL 5.0.77	Intel(R) Atom(TM) CPU D410 @ 1.66GHz	Rack 2A
*srvcall2	Linux Core 2.6.18, Zycoo, MySQL 5.0.77	Intel(R) CPU N270 @ 1.60GHz	Rack 2A

3.1.1.7. Enlaces de Comunicaciones

Tabla 6.

Enlaces de Comunicaciones

Nombre	Proveedor	Caracteristicas Técnicas	Desde	Hasta
Enlace1 – Interno	Telconet	3Mb compartición 1:1	Quito	Guayaquil
Enlace2 – Interno	Telconet	512Mb compartición 1:1	Quito	Cuenca
Enlace3 – Interno	Telconet	512Mb compartición 1:1	Quito	Ambato
Enlace4 – Interno	Telconet	512Mb compartición 1:1	Quito	Ibarra
Enlace5 – Interno	Telconet	512Mb compartición 1:1	Quito	Loja
Enlace6 – Interno	Telconet	512Mb compartición 1:1	Quito	Coca
Enlace7 – Interno	Telconet	512Mb compartición 1:1	Quito	Manta
Enlace8 – Interno	New Access	512Mb compartición 1:1	Quito	Machala
Enlace9 – Interno	Telconet	512Mb compartición 1:1	Quito	Condado
Enlace10 – Interno	Telconet	512Mb compartición 1:1	Quito	Quicentro Sur
Enlace11 – Extranet 1	New Access	3.5Mb compartición 1:1	Quito	Internet
Enlace12– Internet	Telconet	2Mb compartición 1:1	Quito	Internet
Enlace13 – Internet	Telconet	2Mb compartición 1:1	Guayaquil	Internet
Enlace14 - Extranet 2	New Access	1Mb compartición 1:1	Guayaquil	Internet
Enlace14 – Mail Dominio 1	New Access	1Mb compartición 1:1	Quito	Internet
Enlace14 – Mail Dominio 2	New Access	1Mb compartición 1:1	Quito	Internet
Enlace14 – Mail Dominio 3	New Access	256Kb compartición 1:1	Quito	Internet

3.1.2. INFRAESTRUCTURA DE SOTWARE

Sistema Administrativo Financiero: El back office de la compañía esta soportado por un ERP que apoya la gestión interna de las Áreas Administrativo Financiera y Comercial. Corresponde a una solución Cliente-Servidor y utiliza como motor de base de datos SQLServer 2000. El sistema brinda los siguientes servicios:

Inventarios: Mantiene los procesos relacionados con la administración y control del inventario mediante Ordenes y Movimientos de Ingresos, Egresos y Transferencias entre Bodegas, así como también se encarga de los procesos de Costeo y Tomas Físicas, integrándose con el sistema de contabilidad para generar los registros correspondientes de forma automática.

Ensamblaje: Se encarga del control de ensamblaje de componentes electrónicos por unidades y lotes de producción, integrándose con el sistema de inventarios para generar las transacciones de ingresos y egresos correspondientes.

Cuentas por Cobrar: Se encarga del registro y administración de las obligaciones por cobrar de la cartera de clientes derivada del proceso de facturación, administra los estados de cuenta, antigüedad. Se integra con recaudaciones y genera automáticamente la información contable y tributaria relacionada.

Cuentas por Pagar: Se encarga del registro y administración de las obligaciones por pagar de la cartera de proveedores derivada de los procesos de compras e importaciones, administra los estados de cuenta y calendarios de pago. Se integra con pagos y genera automáticamente la información contable y tributaria relacionada.

Tesorería: Se encarga de la administración de las cajas recaudadoras y pagadoras, el estado de las cuentas bancarias, el registro de los pagos y recaudaciones de las obligaciones por cobrar y pagar.

Contabilidad: Se integra con todos los módulos del ERP para permitir controlar los registros contables resultantes de los módulos auxiliares y el registro de todas las transacciones contables adicionales, así como el registro del presupuesto contable. Se encarga además de la generación de los estados financieros normales y comparativos con el presupuesto y/o los diferentes ejercicios y periodos contables.

Sistema Administración Tributaria: Soporta las actividades del Área Administrativo Financiera en lo relacionado a la elaboración de los Anexos Transaccionales y Formularios Electrónicos para la declaración de impuestos, en función de los registros generados por los módulos Administrativo Financieros y utiliza como motor de base de datos SQLServer 2000. El sistema brinda los siguientes servicios:

- **Mantenimiento de Compras e Importaciones**: Prepara la información de compras, importaciones y notas de crédito de proveedores para la elaboración de los Anexos Transaccionales.

- **Mantenimiento de Ventas y Exportaciones**: Prepara la información de ventas, exportaciones y notas de crédito de clientes para la elaboración de los Anexos Transaccionales.

- **Generación del ATS**: Genera la información del Anexo Transaccional en base a la información procesada de Clientes y Proveedores.

Activos Fijos: Soporta las actividades del Área Administrativo Financiera en lo relacionado al registro de las altas y bajas de activos fijos, genera la información relacionada con la depreciación y el etiquetado de los

activos fijos. Corresponde a un sistema basado en una aplicación que corre en un host utilizando como medio de almacenamiento archivos tipo Dbase II.

Sistema de Gestión Humana: Soporta las actividades del Departamento de Talento Humano. Corresponde a una solución Cliente-Servidor, utiliza como motor de base de datos MySql 5.0 y requiere del Remote Desktop de Windows 2008 para su funcionamiento, mantiene los siguientes servicios:

- **Gestión del Recurso Humano**: Se encarga del registro todo tipo de Acciones de Personal de los Socios de Negocio para los Ingresos, Salidas, Cambios de Posición, Cambios de Sueldo, Anticipos, Préstamos, etc.

- **Selección de Personal**: Se encarga de administrar la información necesaria para la gestión de los prospectos con el fin de realizar la selección de personal de acuerdo a las competencias y los cargos.

- **Generación de Nómina**: Se encarga del Cálculo y Generación de la nómina, anticipos de personal, liquidaciones, descuentos, anticipos, préstamos, etc.

Sistema de Evaluaciones: Soporta las actividades del Departamento de Talento Humano y en lo relacionado a la definición de objetivos de personal y evaluación mensual de los resultados en función de los objetivos. Corresponde a una aplicación Cliente Servidor que requiere una base de datos SqlServer 2005.

Sistema de Administración de Clientes: Este sistema es un CRM gerencial y operativo que administra la relación con los clientes, antes, durante y después del proceso de venta, soportando las actividades de las áreas Comercial, Operaciones y Gerencia General. Está basado en tecnología web de tres capas, utiliza un servidor de aplicaciones Glasfish

v2r2, accediendo a los servidores de base de datos MySQL 5.0., SQLServer 2000 y SQLServer 2005. Está constituido por los siguientes módulos:

- **Clientes:** Centraliza la información de clientes brindando un punto de acceso desde donde se puede administrar todos los procesos relacionados, manteniendo además integración con la información de clientes generada por los sistemas Administrativo Financiero y de Operaciones.

- **Campañas**.- Permite generar campañas de mailing a los clientes en función de necesidades específicas o procesos periódicos de Cobranzas, chequeos, renovaciones.

- **Solicitudes y Seguimiento.-** Administra las solicitudes de los usuarios y permite dar seguimiento al cumplimiento de los compromisos realizados con el cliente.

- **Proformas.-** Administra y da seguimiento a las proformas enviadas a los clientes y/o prospectos

- **Citas / Turnos.-** Administra todo tipo de citas realizadas con los clientes dentro y fuera de la compañía, administrando los horarios y rutas del personal, así como la capacidad del taller.

- **Ortes.**- Permite registrar la información de los vehículos de los clientes que llegan al taller para realizar los servicios de instalación y chequeo.

- **Ordenes de Trabajo.**- Permite registrar y controlar los procesos de chequeo, instalación, renovación y retiro de sistemas de rastreo, así como el funcionamiento de todos los servicios que lo conforman.

- **Ordenes de Monitoreo.**- Permite activar los sistemas de localización y los servicios relacionados en los servidores de localización y el extranet.

- **Contratos.**- Administra los contratos derivados de los procesos de instalación y renovación de los dispositivos. Controla y almacena las imágenes de los documentos requeridos durante el proceso de contratación y genera la información necesaria para la gestión de chequeos y renovaciones.

Sistemas: Administra la información de las importaciones de sistemas de localización.

Robos: Administra la información de robos de Vehículos así como el proceso de recuperación.

Facturación: Genera la facturación originada por las órdenes de trabajo y los contratos, alimentando automáticamente la información contable y de cartera de clientes al sistema contable.

Comisiones: Administra las solicitudes de comisiones de acuerdo con los convenios establecidos con los diferentes canales, controlando el proceso de cálculo, aprobación y pago.

Presupuesto de Ventas: Brinda las herramientas para el cálculo de estimaciones y el registro del presupuesto de ventas de acuerdo a las líneas de negocio y canales.

Reports: Mantiene las consultas, reportes e informes necesarios para apoyar las tareas operativas de las áreas financiero contable, mercadeo, comercial y operaciones.

Business: Brinda a los niveles gerenciales los cuadros de mando de BI conteniendo los indicadores resultantes de la gestión de la compañía en lo referente a las áreas financiero contable, mercadeo, comercial y operaciones.

Accounting Interfase: Este sistema administra la integración contable entre sistemas externos y contabilidad. Está basado en tecnología web de tres capas, utiliza un servidor de aplicaciones Glasfish, accediendo a la información de servidores MySql 5.0, SQLServer 2000 y SQLServer 2008.

Sistema de Administración de Seguridades: Este sistema administra las seguridades de los sistemas Administrativo Financieros y de Administración de Clientes. Las seguridades se controlan a nivel de Perfiles, Usuarios, Opciones y Procesos. Controla además la ejecución de los procesos Batch, mantiene los registros de errores y auditoría. Está basado en tecnología web de tres capas, utiliza un servidor de aplicaciones Glasfish, accediendo a la información de servidores MySql 5.0 y SQLServer 2000.

Call Center Asterix: Permite a las áreas de Cobranzas y Renovaciones ejecutar campañas telefónicas mediante la información generada desde el Sistema de Clientes. Está basado en tecnología web,utiliza un servidor de aplicaciones Apache y el motor de base de datos MySql de los servidores Elastix.

Postfix: Es un servicio para Linux para gestionar el correo. Utilizado por todas las áreas de la organización.

CIFS: Es un servicio de Windows para la compartición y administración de archivos.

Sistema de control de mensajes: Permite gestionar los servicios y administrar los mensajes de los sistemas de rastreo satelital. Es una

aplicación cliente servidor, se ejecuta en cada estación de trabajo utiliza los servicios de la base de datos SQLServer 2005 y mantiene comunicación directa con los dispositivos de localización. Para los dispositivos Sms utiliza la red sms enviando mensajes tcp y para los dispositivos Gprs utilizandoel protocolo de comunicación udp. Utilizado como soporte a las actividades operativas del área de Operaciones.

Sistema de análisis de mensajes: Permite consultar y obtener reportes para análisis de la mensajería de los sistemas de localización. Utilizado como soporte a las actividades de análisis del área de Operaciones.

Sistema Web portal Tracklink: Mediante la Extranet de la compañía permite a sus clientes acceder a los servicios de rastreo satelital de sus vehículos. Mantiene módulos adicionales para controlar el Mantenimiento de Vehículos, Zonas, Rutas, Puntos de Interés.

Sistema Web portal Vestigo: Mediante la Extranet de la compañía permite a sus clientes acceder a los servicios de localización personal.

Administración de Usuarios de Dominio: Para el efecto se utilizan servidores de dominio mediante ActiveDirectory.

Backups y Recuperación: Se realiza mediante los servicios de Backup automáticos brindados por MySQL y SQLServer en cada caso. Se realizan respaldos manuales de los documentos almacenados en los servidores de archivos. Para los servicios críticos se mantiene un servidor de aplicaciones alternativo que podrá ser levantado en caso que sea requerido.

3.1.3. MAPEO DE LOS SERVICIOS, APLICACIONES Y SERVIDORES

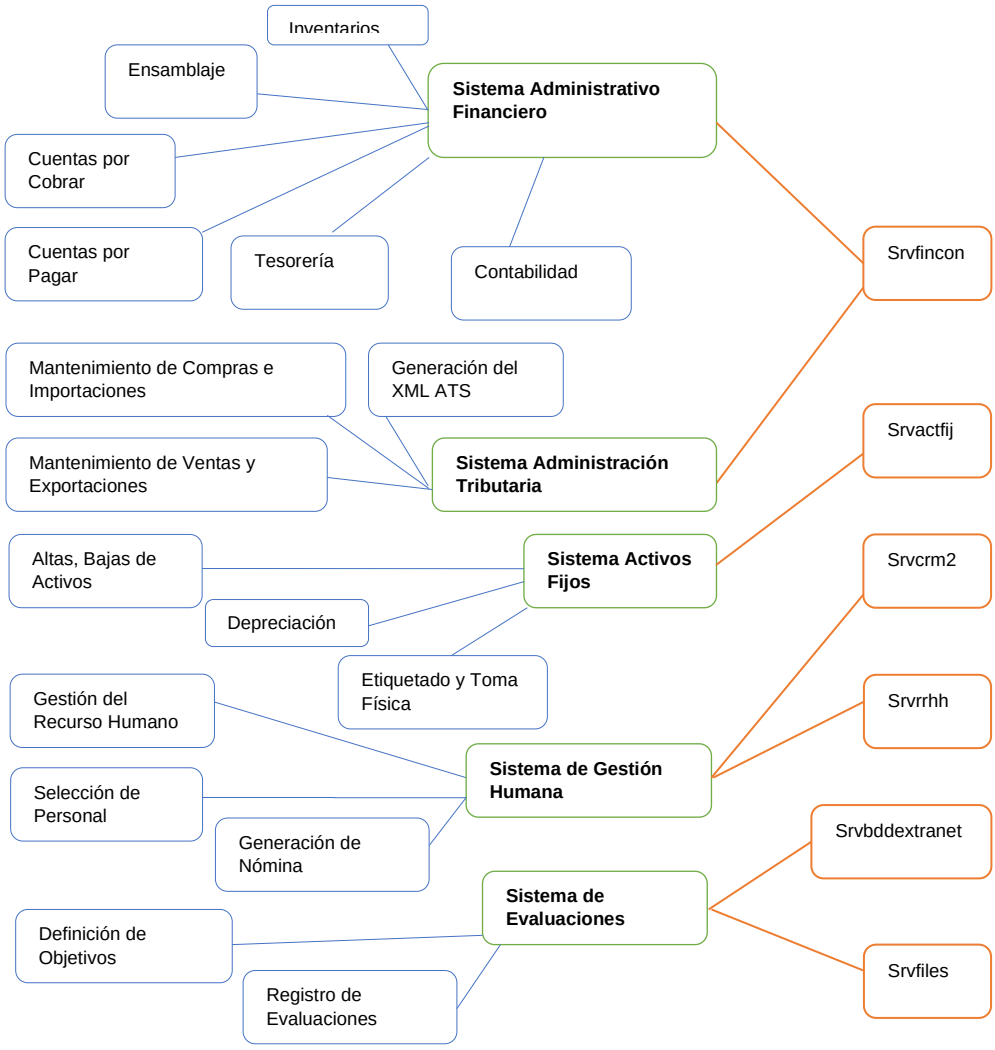

Figura 11. Mapeo de los Servicios Aplicaciones y de los Servidores

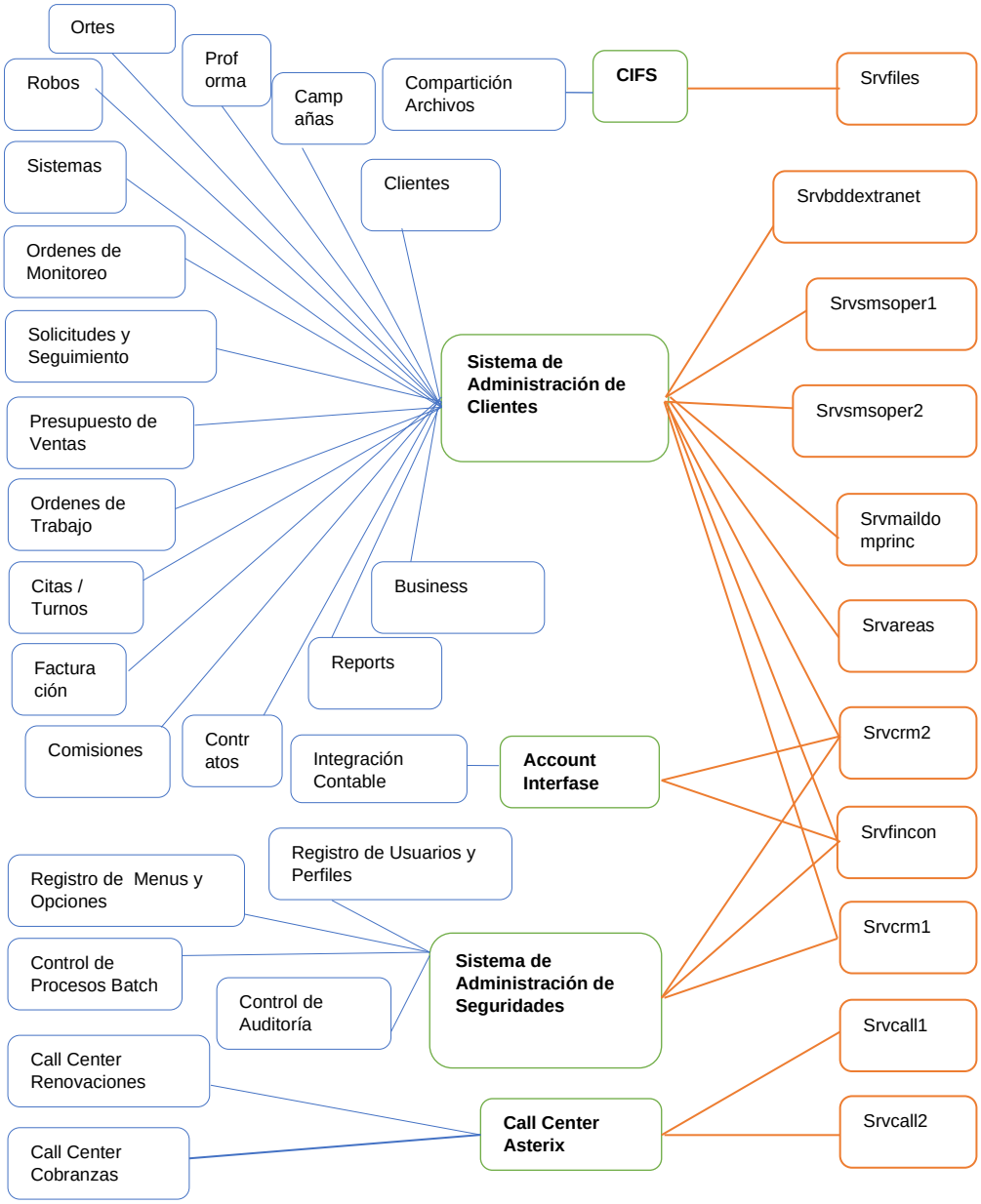

Figura 12. Mapeo de los Servicios Aplicaciones y de los Servidores

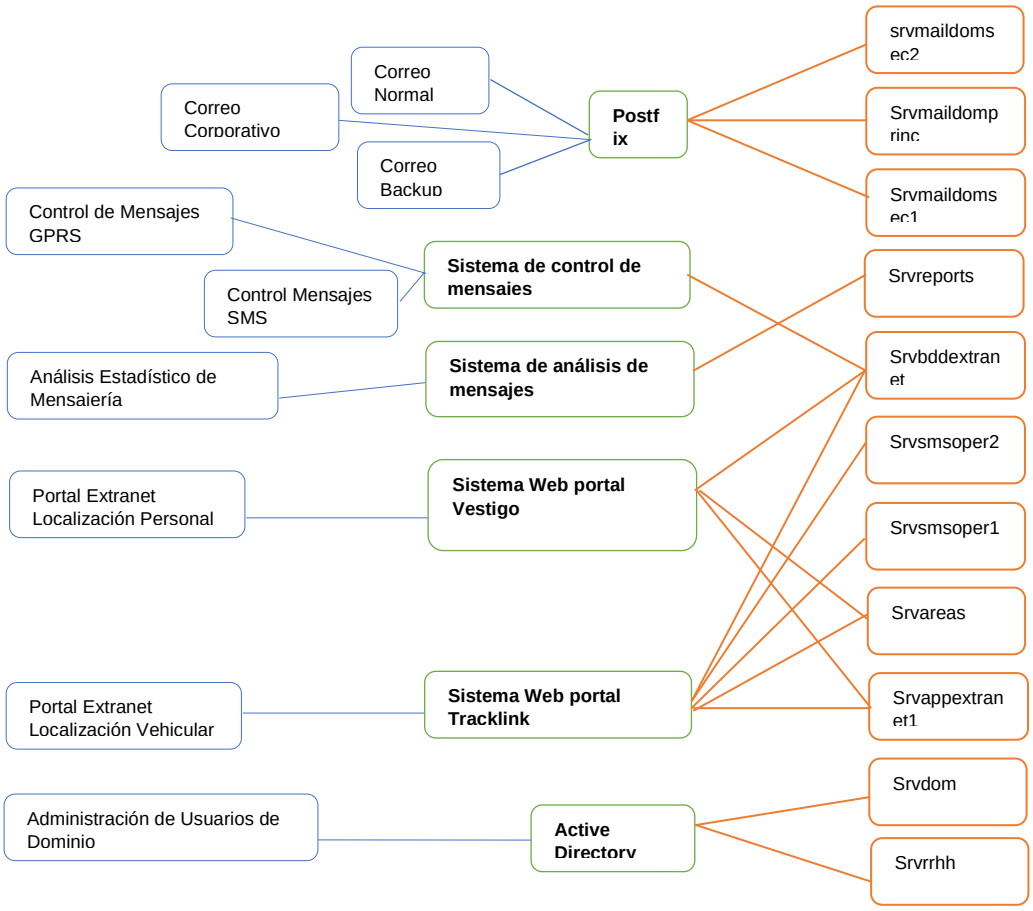

Figura 13. Mapeo de los Servicios Aplicaciones y de los Servidores

3.1.4. MAPEO DE LOS SERVICIOS, APLICACIONES Y BASES DE DATOS

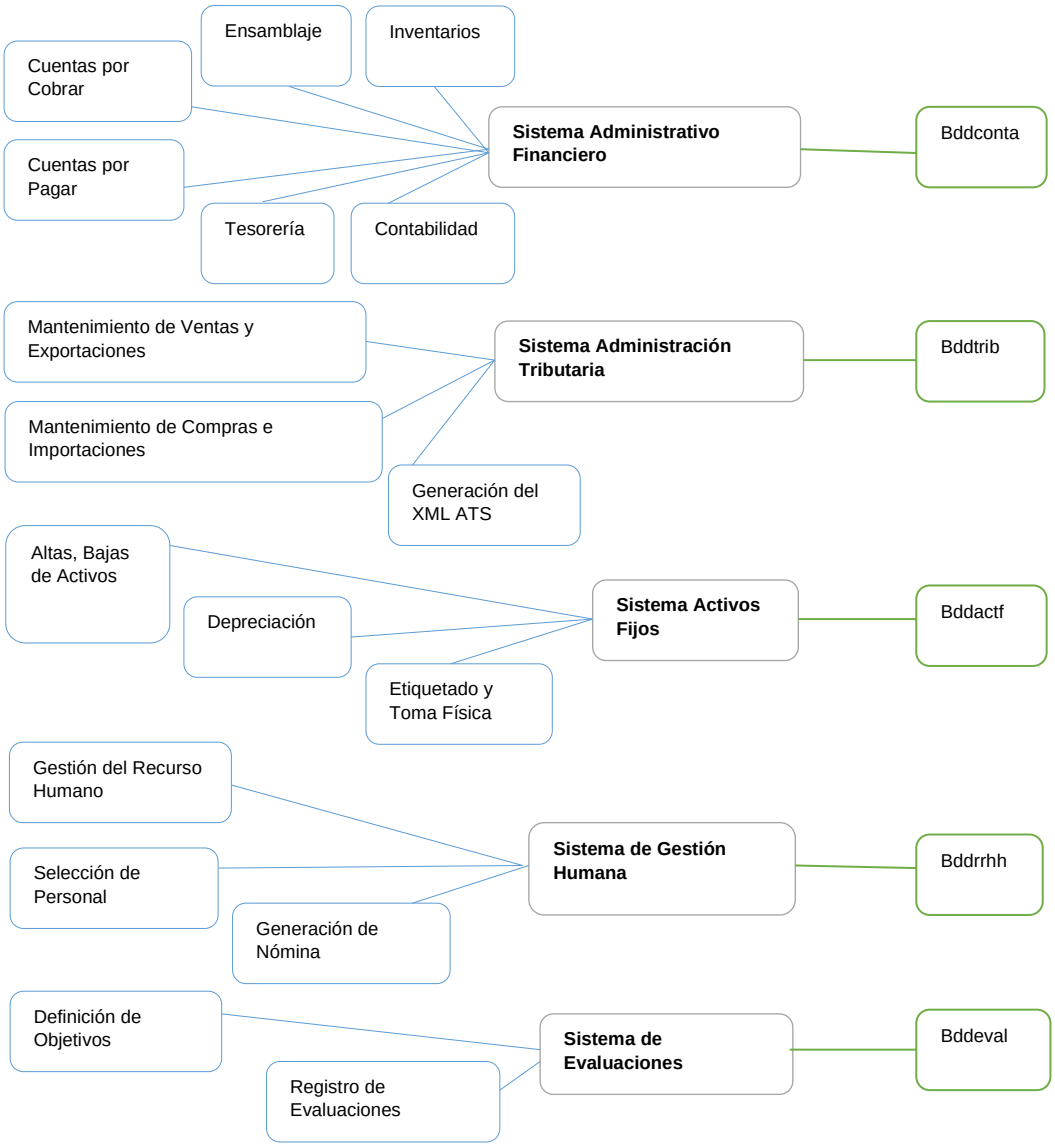

Figura 14. Mapeo de los Servicios Aplicaciones y Bases de Datos

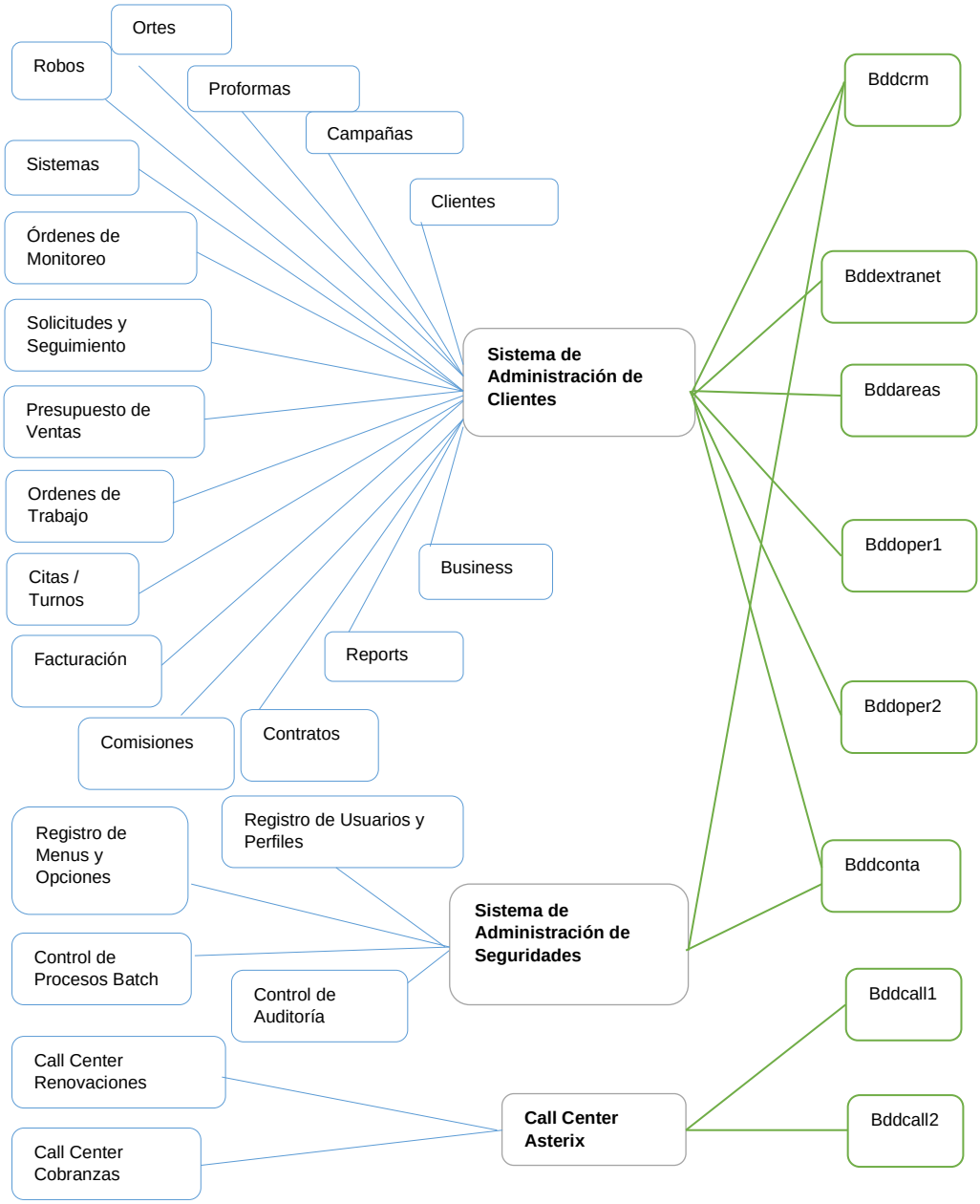

Figura 15. Mapeo de los Servicios Aplicaciones y Bases de Datos

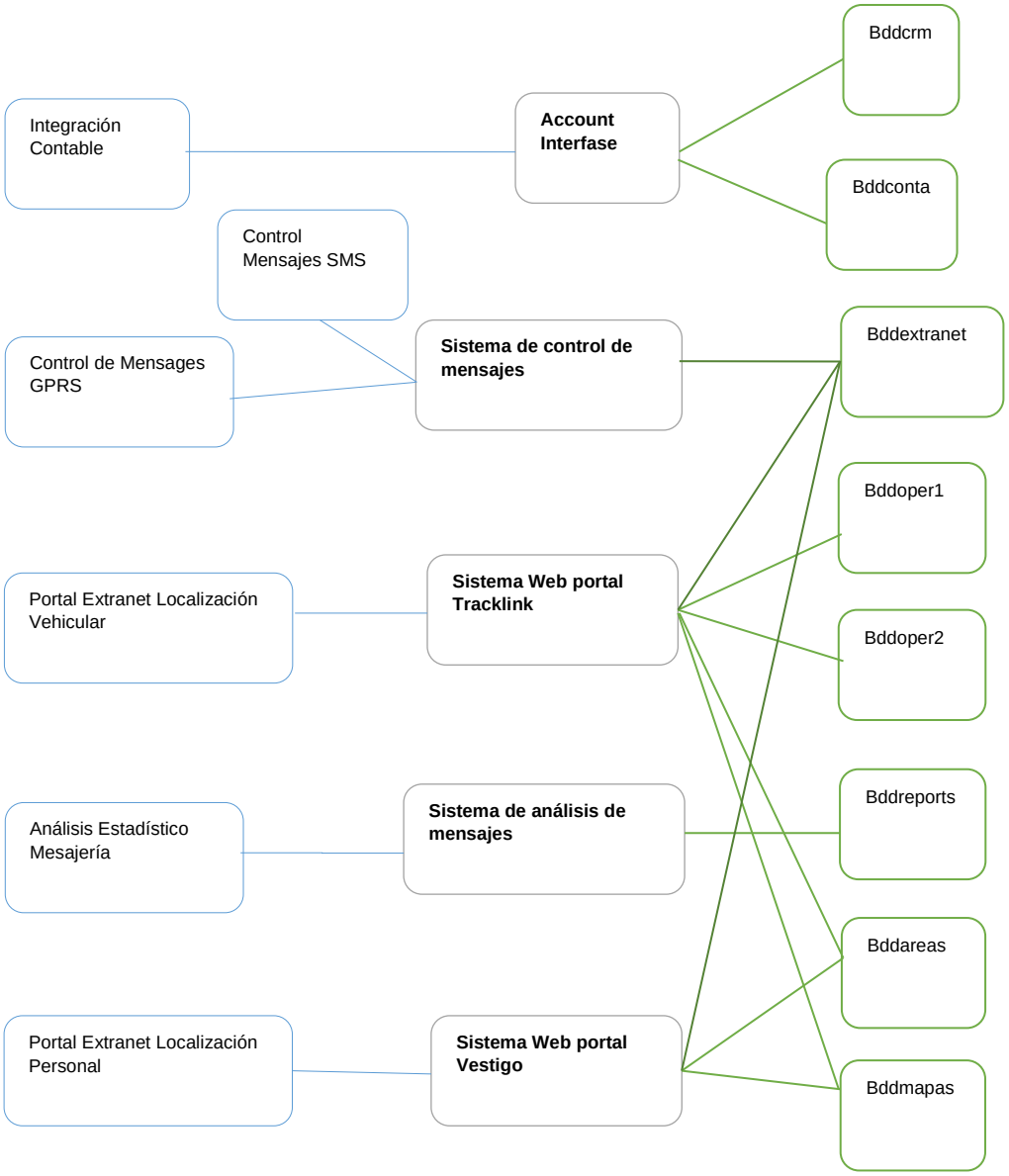

Figura 16. Mapeo de los Servicios Aplicaciones y Bases de Datos

3.1.5. DIAGRAMAS DE PROCESOS

Se han identificado los siguientes procesos macro como los más críticos para la operación de la compañía:

A continuación se muestra el proceso de instalación de sistemas nuevos:

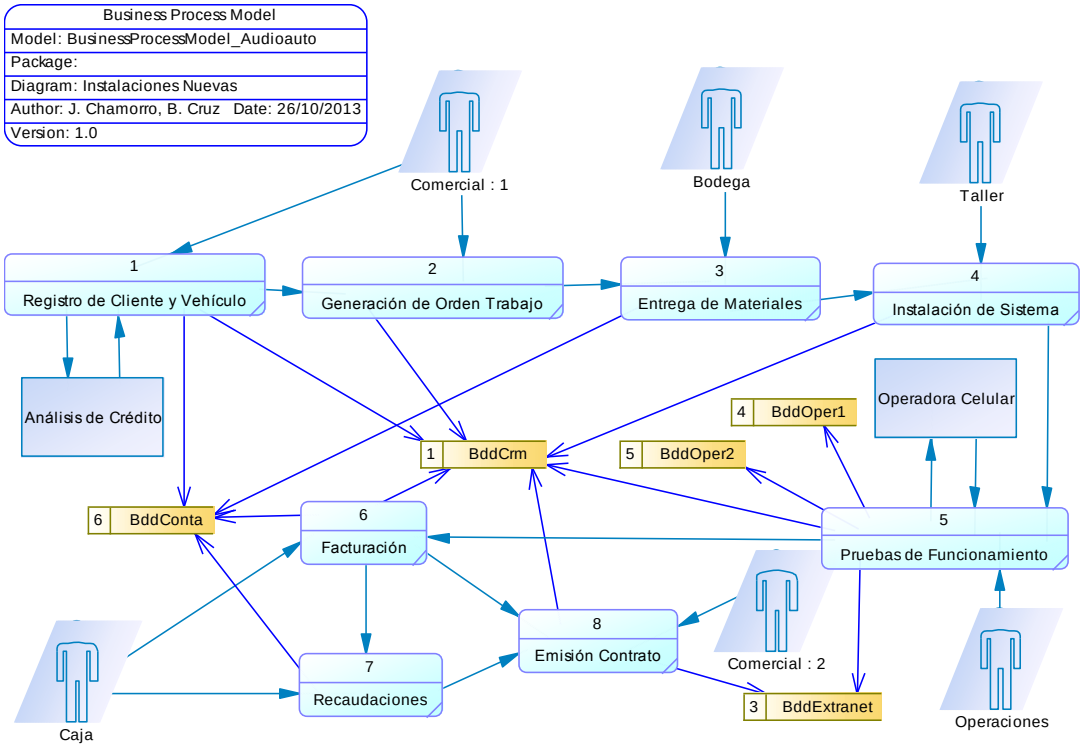

Figura 17. Instalaciones Nuevas

A continuación se muestra el proceso de renovación de clientes normales:

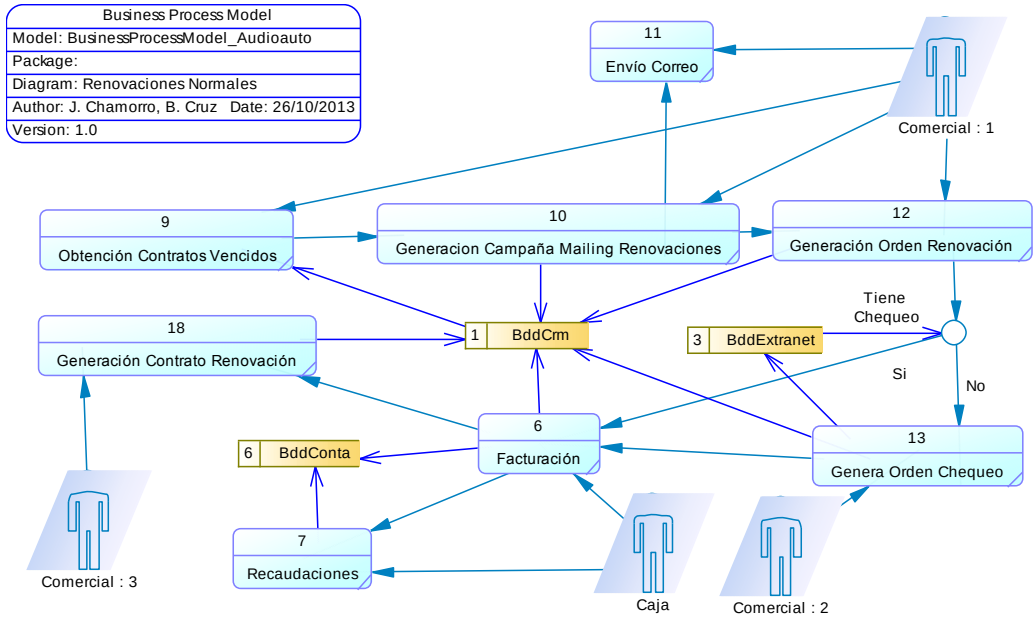

Figura 18. Renovaciones Normales

A continuación se muestra el proceso de renovación de clientes corporativos mediante pago de Fee mensual:

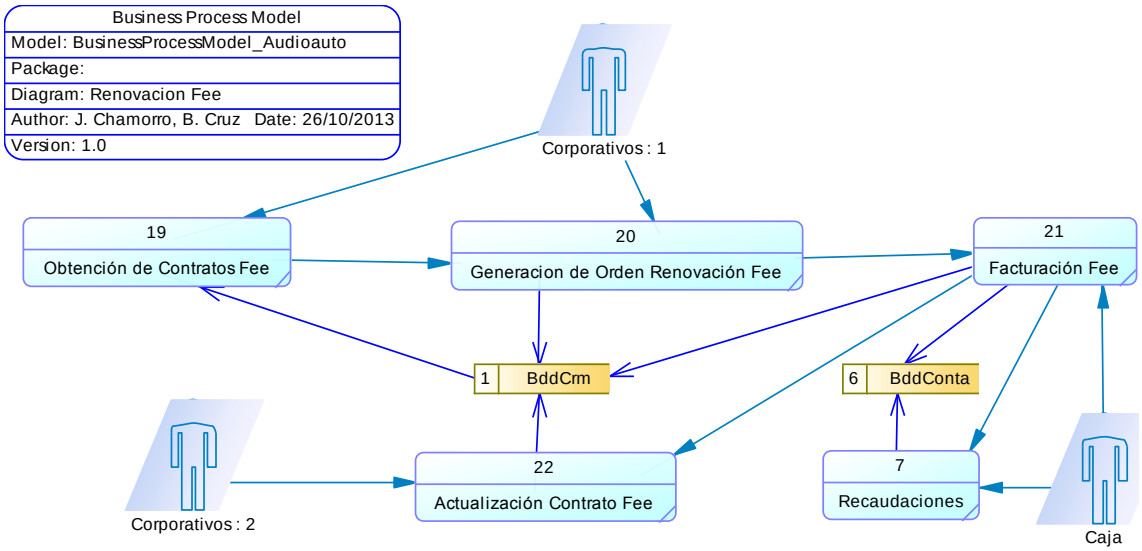

Figura 19. Renovaciones Fee

A continuación se muestra el proceso de chequeo periódico de sistemas de localización:

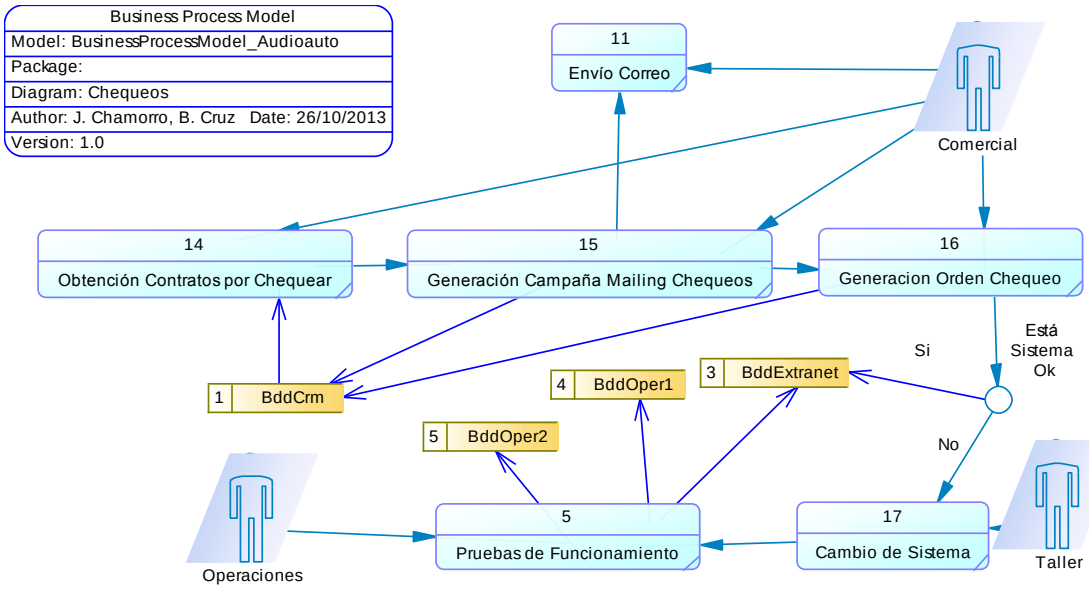

Figura 20. Chequeos

A continuación se muestra el proceso para el pago de comisiones externas:

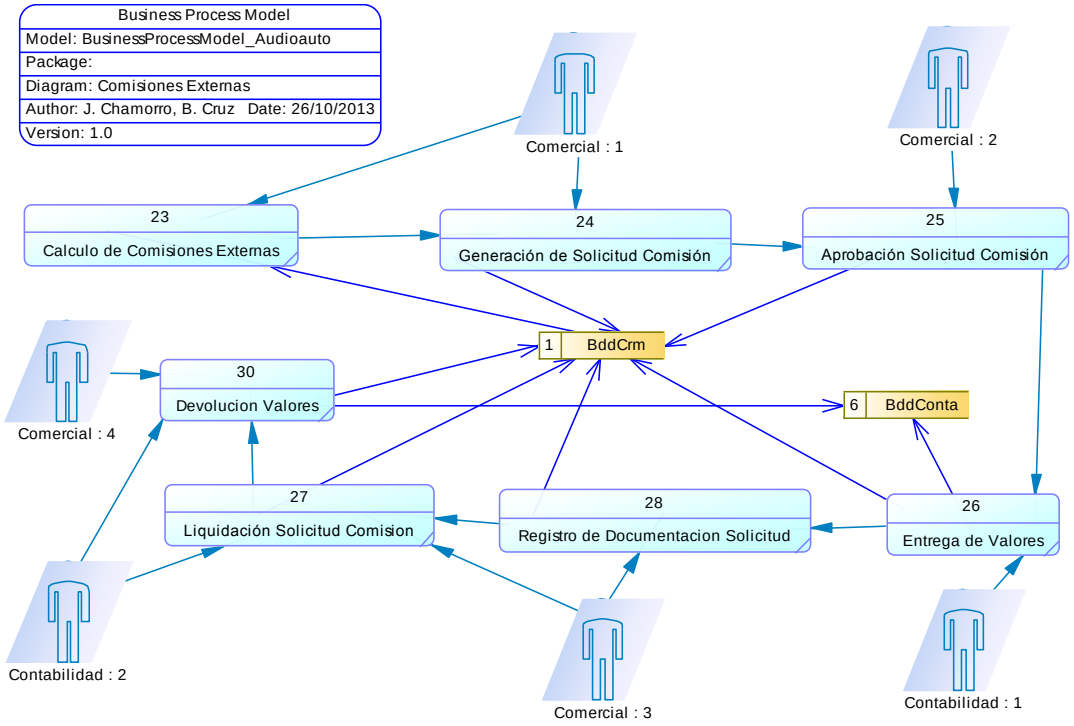

Figura 21. Comisiones Externas

A continuación se muestra el proceso para el pago de comisiones internas:

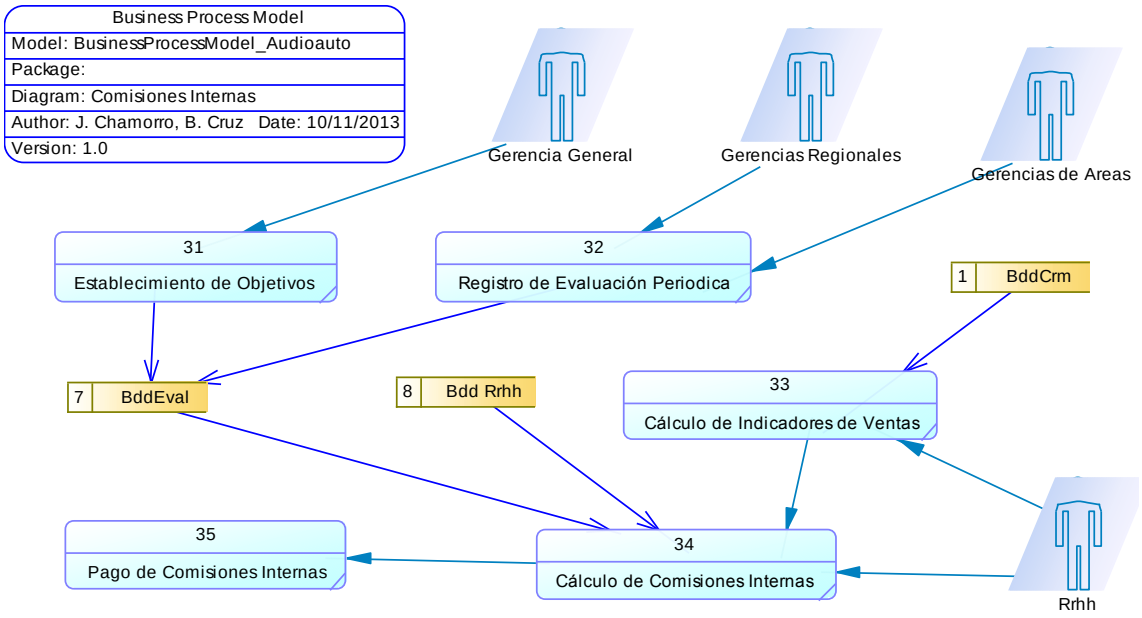

Figura 22. Comisiones Internas

A continuación se muestra el proceso de importación de sistemas de localización:

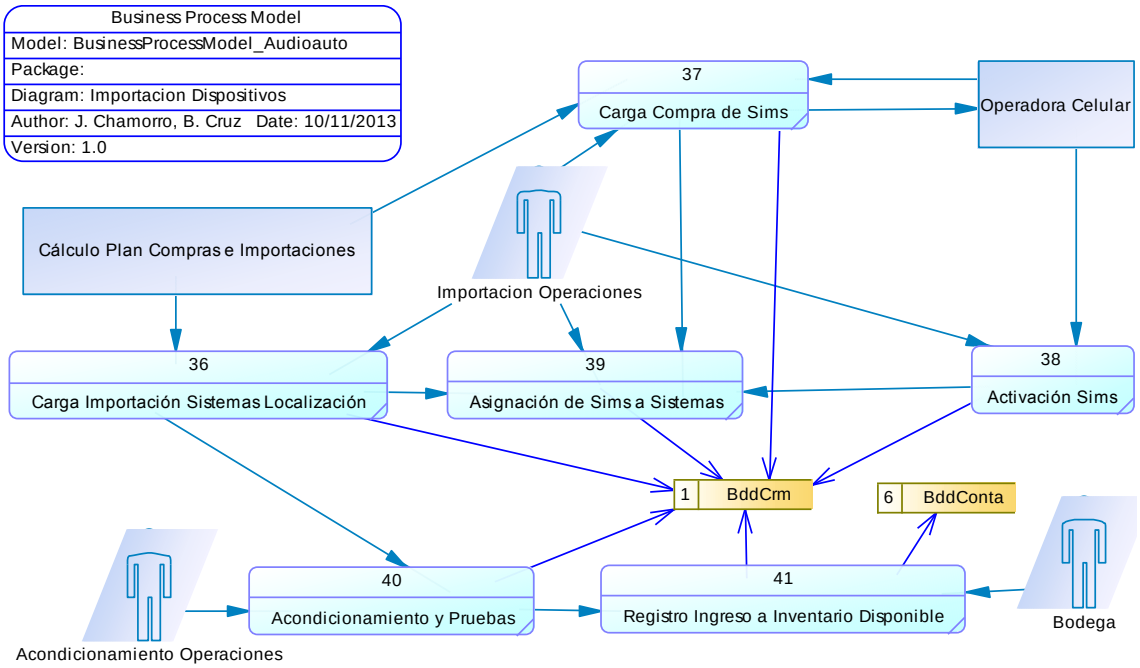

Figura 23. Importación Dispositivos

A continuación se muestra el proceso de compra de materiales, suministros y servicios:

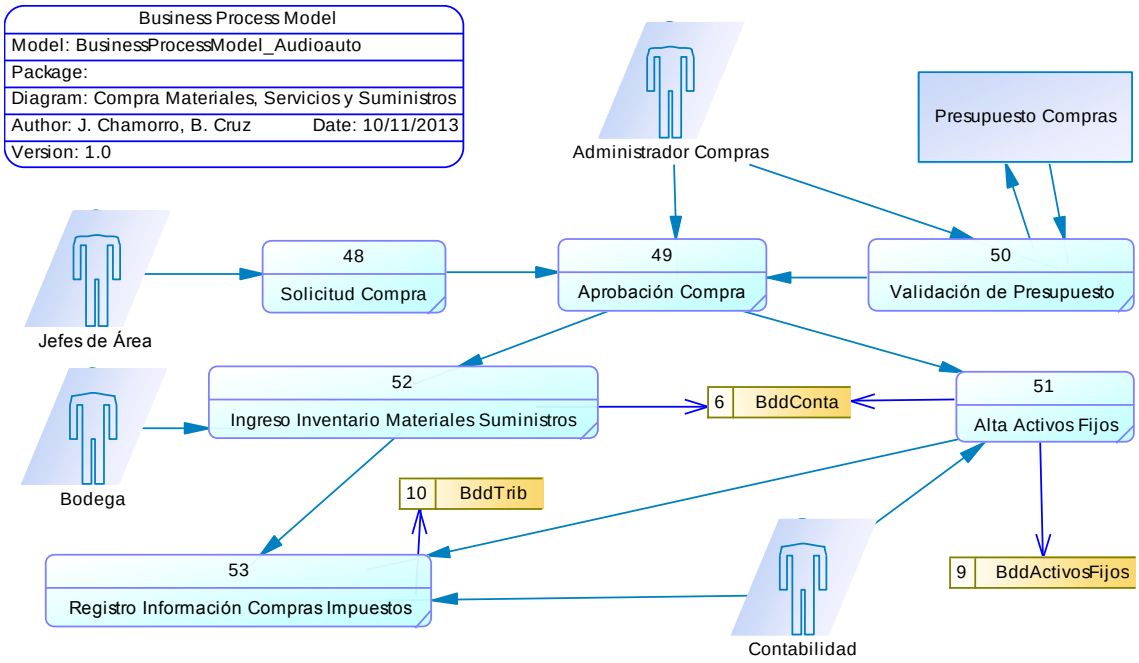

Figura 24. Compra Materiales, Servicios y Suministros

A continuación se muestra el proceso de ensamblaje y acondicionamiento de kits de instalación:

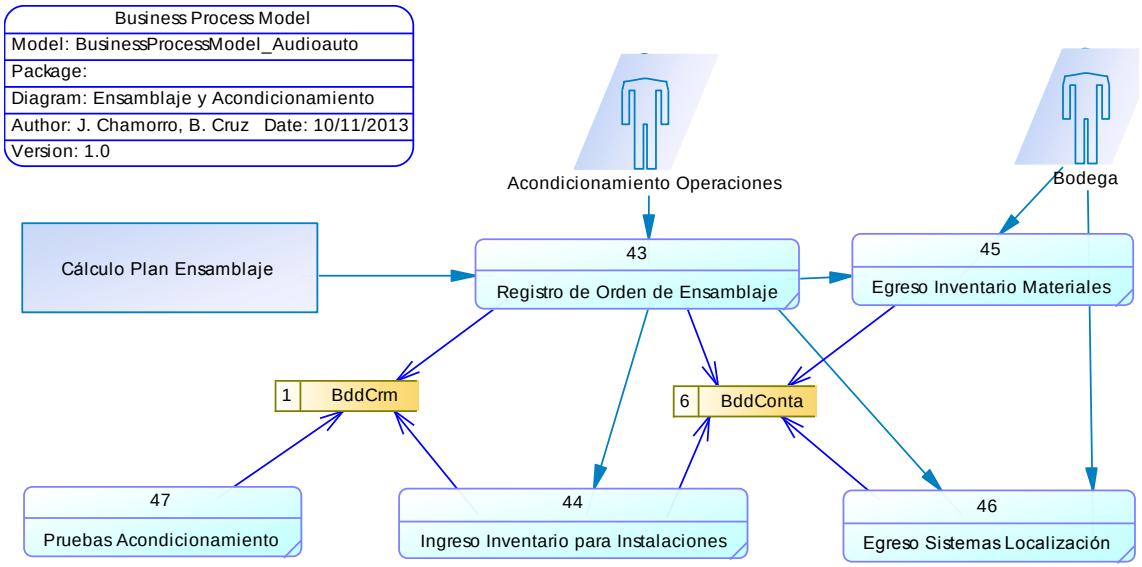

Figura 25. Ensamblaje y Acondicionamiento

A continuación se muestra el proceso de gestión de cobranza mediante el Call Center:

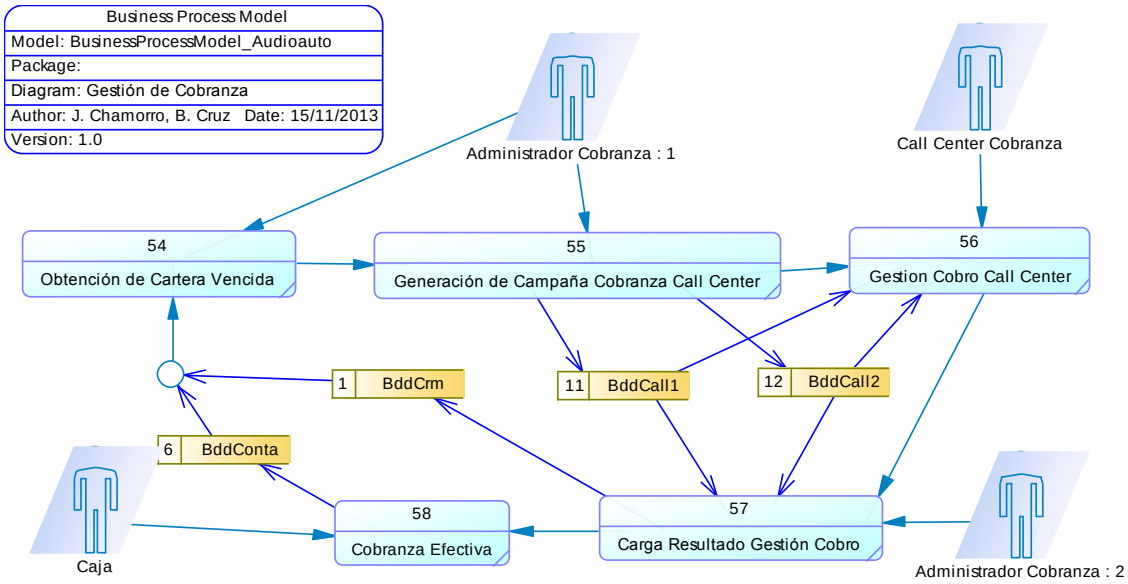

Figura 26. Gestión de Cobranza

A continuación se muestra el proceso de interacción del Cliente en la Extranet o mediante Call Center de Monitoreo para reporte de novedades y acceso a servicios relacionados con la localización vehicular:

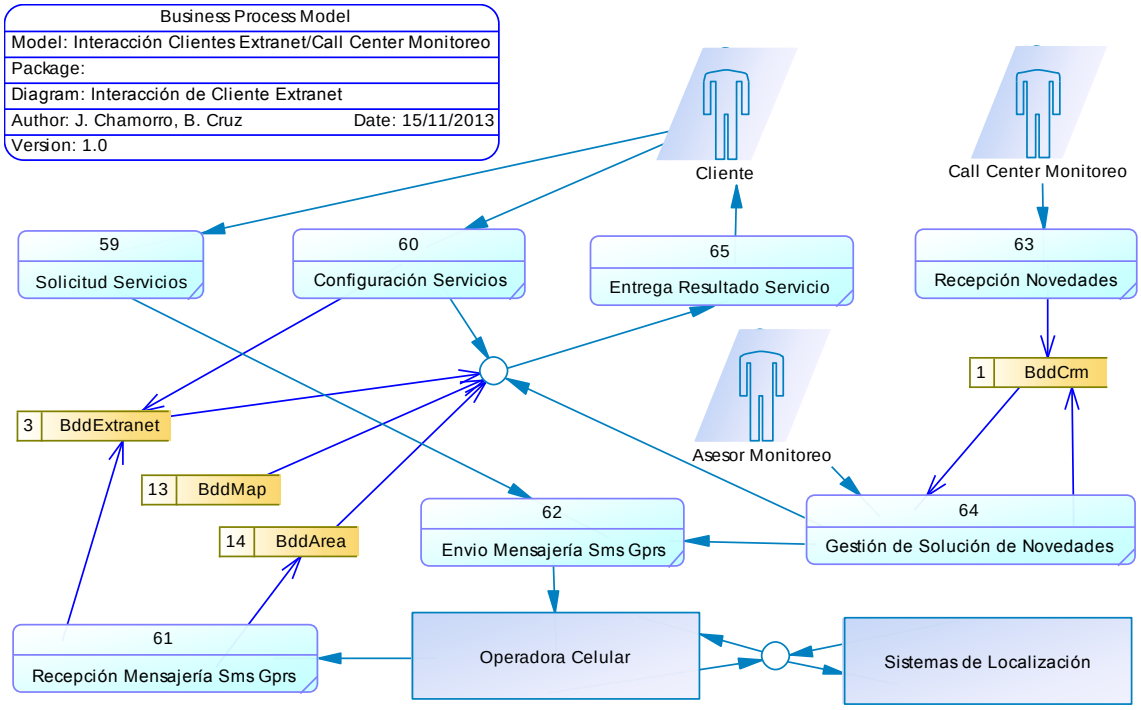

Figura 27. Interacción de Clientes Extranet

3.1.6. CARACTERIZACIÓN DE LOS ACTIVOS

Para la caracterización de la información, servicios, aplicaciones, equipos que constituyen los activos esenciales tomamos como referencia la siguiente clasificación nos sugiere Magerit:

- Información
  - [adm] datos de interés para la administración pública
  - [vr] datos vitales
  - [per] datos de carácter personal
    - [A] nivel alto
    - [M] nivel medio
    - [B] nivel bajo
  - [clasif] datos clasificados
    - [C] nivel confidencial
    - [R] difusión limitada
    - [UC] sin clasificar
    - [pub] de carácter público

- Servicios
  - [anon] anónimo (sin requerir identificación del usuario)
  - [pub] al público en general (sin relación contractual)
  - [ext] a usuarios externos (bajo una relación contractual)
  - [int] interno (a usuarios de la propia organización)

- Aplicaciones
  - [prp] desarrollo propio (in house)
  - [sub] desarrollo a medida (subcontratado)
  - [std] estándar (off the shelf)
    - [browser] navegador web
    - [www] servidor de presentación
    - [app] servidor de aplicaciones

    - [email_client] cliente de correo electrónico
    - [email_server] servidor de correo electrónico
    - [file] servidor de ficheros
    - [dbms] sistema de gestión de bases de datos
    - [tm] monitor transaccional
    - [office] ofimática
    - [av] anti virus
    - [os] sistema operativo
    - [hypervisor] gestor de máquinas virtuales
    - [ts] servidor de terminales
    - [backup] sistema de backup
    - [dom] administración del dominio

- Equipos Informáticos
    - [host] grandes equipos
    - [mid] equipos medios
    - [pc] informática personal
    - [mobile] informática móvil
    - [pda] agendas electrónicas
    - [vhost] equipo virtual
    - [backup] equipamiento de respaldo
    - [peripheral] periféricos
        - [print] medios de impresión
        - [scan] escáneres
        - [crypto] dispositivos criptográficos
    - [bp] dispositivo de frontera
    - [network] soporte de la red
    - [modem] módems
    - [hub] concentradores
    - [switch] conmutadores
    - [router] encaminadores
    - [bridge] pasarelas

- [firewall] cortafuegos
- [wap] punto de acceso inalámbrico
- [pabx] centralita telefónica [ipphone] teléfono IP

A continuación se muestra una tabla que contiene la clasificación de la información relacionada con los servicios que la requieren, las aplicaciones que brindan los servicios y el equipo físico utilizado tanto el principal como el backup en caso de existir:

Tabla 7.

Clasificación de Inventarios, Transacciones y Activos, relacionada con los servicios, las aplicaciones y el equipo físicos

INFORMACION	TIPO	NIVEL	SOPORTE FUNCIONAL	TIPO	SOPORTE TECNICO	TIPO	SERVICIO	TIPO	APLICACIÓN	TIPO	SERVIDOR
Inventarios	[clasif]	[R]	Usuario admin inventario	[ui]	Prov Sist AdmFin	[prov]	Inventarios	[int]	Sistema Administrativo Financiero	[app]	srvfincon
Ensamblaje	[clasif]	[R]					Ensamblaje	[int]			
Cartera Clientes	[clasif]	[R]	Usuario admin cobranza	[ui]			Cuentas por Cobrar	[int]			
Cartera Proveedores	[clasif]	[R]	Usuario admin compras	[ui]			Cuentas por Pagar	[int]			
Movimiento Financiero	[clasif]	[R]	Usuario admin Conta	[ui]			Tesorería	[int]	BddConta (SqlServer 2000)	[dbms]	
Transaciones Contables	[clasif]	[R]					Contabilidad	[int]			
Transacciones de Compra	[adm]	[R]	Usuario admin Conta	[ui]	Prov Sist AdmFin	[prov]	Mantenimiento de Compras e Importaciones	[int] [ext]	Sistema Admin Tributaria	[app] [app]	Srvfincon
Transaciones de Venta	[adm]	[R]					Mantenimiento de Ventas y Exportaciones	[int] [ext]		[dbms]	
							Generación del XML ATS	[int] [ext]	BddTrib (SqlServer 2000)	[dbms]	
Activos Fijos	[clasif]	[pub]	Usuario admin Conta	[ui]	Usuario Admin Sistemas	[adm]	Altas, Bajas de Activos	[int]	Sistema Activos Fijos	[app]	Srvactf
							Depreciación	[int]			
							Etiquetado y Toma Física	[int]	BddAcf (Dbase II)	[file]	

Tabla 8.

Clasificación de Nómina y Bitácoras, relacionada con los servicios, las aplicaciones y el equipo físicos

INFORMACION	TIPO	NIVEL	SOPORTE FUNCIONAL	TIPO	SOPORTE TECNICO	TIPO	SERVICIO	TIPO	APLICACIÓN	TIPO	SERVIDOR
Información de Personal	[per]	[A]	Usuario admin Rrhh	[ui]	Prov Sist Rrhh	[prov]	Gestión del Recurso Humano	[int]	Sistema de Gestión Humana	[app]	srvcrm2
Información de Selección	[clasif]	[R]					Selección de Personal	[int]	BddRrhh MySQL (5.5.23)	[dbms]	srvcrm1
Nominas	[per]	[A]					Generación de Nómina	[i[]	Remote Desktop	[ts]	Srvrrhh
Objetivos Individuales	[clasif]	[pub]	Usuario admin Rrhh	[ui]	Prov Sist Eval	[prov]	Definición de Objetivos	[int]	Sistema de Evaluaciones	[sub]	Srvbddextranet
Evaluaciones	[clasif]	[R]					Registro de Evaluaciones	[int]	BddEval (SQLServer 2005)	[file]	Srvfiles
Bitácora Llamadas	[clasif]	[R]	Usuario Admin Sistemas	[adm]	Usuario Admin Sistemas	[adm]	Call Center Renovaciones	[int]	Call Center Asterix BddCall1 (Mysql 5.0.77)	[app] [dbms]	srvcall1
Bitácora Llamadas	[clasif]	[R]	Usuario Admin Sistemas	[adm]	Usuario Admin Sistemas	[adm]	Call Center Cobranzas	[int]	Call Center Asterix BddCall2 (Mysql5.0.77)	[app] [dbms]	srvcall2

Tabla 9.

Clasificación de Clientes, Facturación y Ventas, relacionada con los servicios, las aplicaciones y el equipo físicos

INFORMACION	TIPO	NIVEL	SOPORTE FUNCIONAL	TIPO	SOPORTE TECNICO	TIPO	SERVICIO	TIPO	APLICACIÓN	TIPO	SERVIDOR
Clientes	[clasif]	[R]					Clientes	[int]	Sis. Clientes	[app]	srvcrm1
Campañas	[clasif]	[R]					Campañas	[int]	Glassfish v2	[app]	
Solicitudes y Seg.	[clasif]	[R]	Usuario admin Crm	[ui]			Solicitudes y Segto.	[int]	BddCrm	[dbms]	srvcrm2
Proformas	[clasif]	[R]					Proformas	[int]	(Mysql 5.5.23)		
Citas / Turnos	[clasif]	[R]					Citas / Turnos	[int]	BddConta	[dbms]	srvfincon
Ortes	[clasif]	[R]					Ortes	[int]	(Sql 2000)		
Ordenes de Trabajo	[clasif]	[R]	Usuario				Ordenes de Trabajo	[int]	BddCrm	[dbms]	srvsmsoper1
Ordenes de Monitoreo	[clasif]	[R]	Adm Operac		Prov.	[prov]	Ordenes de Monitoreo	[int]	(Mysql 5.1.27)		
Contratos	[clasif]	[C]		[ui]			Contratos	[int]	BddCrm	[dbms]	srvsmsoper2
Sistemas	[clasif]	[C]					Sistemas	[int]	(Mysql 5.5.14)		
Robos	[clasif]	[C]					Robos	[int]	Postfix	[email server]	Srvmaildomprinc
Comisiones	[clasif]	[R]					Comisiones	[int]			
Facturación	[clasif]	[R]	U. adm Conta	[ui]			Facturación	[int]	BddExtranet (SQLS2005)	[dbms]	Srvbddextranet
Presupuesto de Ventas	[clasif]	[pub]					Presupuesto de Ventas	[int]			
Ventas	[adm]						Reports	[int]	BddAreas	[dbms]	Srvareas
Indicadores	[clasif]	[C]					Business	[int]	(Mysql 5.1.47)		

Tabla 10.

Clasificación de Anexos Contables, Perfiles de Usuarios y Registros de Auditoria, relacionada con los servicios, las aplicaciones y el equipo físicos

INFORMACION	TIPO	NIVEL	SOPORTE FUNCIONAL	TIPO	SOPORTE TECNICO	TIPO	SERVICIO	TIPO	APLICACIÓN	TIPO	SERVIDOR
Anexos Contables Externos	[clasif]	[R]	Usuario admin Conta	[ui]	Prov Sist AdmFin	[prov]	Integración Contable	[int]	Accounting Interfase BddCrm (Mysql 5.5.23) Glassfish v2 BddConta (SqlServer 2000)	[app] [dbms] [app] [dbms]	srvcrm2 Srvfincon
Usuarios y Perfiles	[clasif]	[C]					Registro de Usuarios y Perfiles	[int]	Sistema Adm. Y Seg.	[sub]	srvcrm1
Menus y Opciones	[clasif]	[R]	Usuario Admin Sistemas	[adm]	Prov Sist AdmFin	[prov]	Registro de Menus y Opciones	[int]	Glassfish v2	[app]	srvcrm2
Ejecución Procesos	[clasif]	[R]					Control de Procesos Batch	[int]	BddCrm (Mysql 5.5.23)	[dbms]	Srvfincon
Registros de Auditoría	[clasif]	[C]					Control de Auditoría	[int]	BddConta (SqlServer 2000)	[dbms]	
Correo Normal	[clasif]	[R]	Usuario Admin Sistemas	[adm]	Usuario Admin Sistemas	[adm]	Correo Normal	[int]	Postfix	[email server] [email server]	Srvmaildomprinc srvmaildomsec1

Tabla 11.

Clasificación de Correos, Mensajes y Estadísticas, relacionada con los servicios, las aplicaciones y el equipo físicos

INFORMACION	TIPO	NIVEL	SOPORTE FUNCIONAL	TIPO	SOPORTE TECNICO	TIPO	SERVICIO	TIPO	APLICACIÓN	TIPO	SERVIDOR
Correo Corporativo	[clasif]	[R]	Usuario Admin Sistemas	[adm]	Usuario Admin Sistemas	[adm]	Correo Corporativo	[int]	Postfix	[email server]	srvmaildomsec1
Correo Backup	[clasif]	[R]	Usuario Admin Sistemas	[adm]	Usuario Admin Sistemas	[adm]	Correo Backup	[int]	Postfix	[email server]	srvmaildomsec2
Archivos Trabajo	[clasif]	[UC]	Usuario Admin Sistemas	[adm]	Usuario Admin Sistemas	[adm]	Compartición de Archivos	[int]	CIFS	[file]	srvfiles
Mensajes Localización Sms Gprs	[vr]	[R]	Usuario Admin Sistemas	[adm]	Prov Sis	[prov]	Control Mensajes SMS	[int]	Sistema Control Mensajes	[app]	Srvbddextranet
	[vr]	[R]			Gps		Control de Mensages GPRS	[int]	BddExtranet (SQLServer 2005)	[dbms]	Srvmirror
Estadisticas Mensajes	[clasif]	[R]	Usuario Admin Sistemas	[adm]	Usuario Admin Sistemas	[adm]	Análisis Estadístico de Mesajería	[int]	Sistema Análisis Mensajes	[app]	Srvreports
									BddReports (MySQL 5.5.27)	[dbms]	

Tabla 12.

Clasificación de Información de Cliente - Vehículos, relacionada con los servicios, las aplicaciones y el equipo físicos

INFORMACION	TIPO	NIVEL	SOPORTE FUNCIONAL	TIPO	SOPORTE TECNICO	TIPO	SERVICIO	TIPO	APLICACIÓN	TIPO	SERVIDOR
Información Cliente Vehiculos	[vr]		Usuario Admin Web	[adm]	Prov Sis	[prov]	Portal Extranet Localizacion Vehicular	[ext]	Sistema Web portal Tracklink	[sub]	srvappextranet1
									Internet Information Server	[app]	
									Apache Tomcat	[app]	
									BddMapas (Postgress)	[dbms]	srvappextranet2
					Gps				BdExtranet (SQLServer 2005)	[dbms]	Srvbddextranet
											srvmirror
									BddCrm (Mysql 5.5.27)	[dbms]	srvsmsoper1
									BddCrm (Mysql 5.5.14)	[dbms]	srvsmsoper2
									Bddareas (Mysql 5.5.47)	[dbms]	Srvareas

Tabla 13.

Clasificación de Información de Personal y Usuarios de Dominio, relacionada con los servicios, las aplicaciones y el equipo físicos

INFORMACION	TIPO	NIVEL	SOPORTE FUNCIONAL	TIPO	SOPORTE TECNICO	TIPO	SERVICIO	TIPO	APLICACIÓN	TIPO	SERVIDOR
Información cliente Personal	[vr]		Usuario Admin Web	[adm]	Prov Sis Gps	[prov]	Portal Extranet Localizacion Personal	[ext]	Sistema Web portal Vestigo Internet Information Server BddMapas (Postgress) Apache Tomcat BdExtranet (SQLServer 2005) Bddareas (Mysql 5.5.47)	[app] [app] [dbms] [app] [dbms] [dbms]	srvappextranet1 srvappextranet2 Srvbddextranet srvmirror srvareas
Usuarios del Dominio	[clasif]	[C]	Usuario Admin Sistemas	[adm]	Usuario Admin Sistemas	[adm]	Administración de Usuarios de Dominio	[int]	Active Directory	[dom]	Srvdom srvrrhh

3.1.7. VALORACIÓN DE LOS ACTIVOS

Para la valoración de los activos esenciales tomamos en cuenta las dimensiones: Confidencialidad, Integridad, Disponibilidad, Autenticidad y Trazabilidad. A estas dimensiones les hemos aplicado un criterio de valoración cualitativa en una escala de: extremo [EX], muy alto [MA], alto [AL], medio [ME], bajo [BA], despreciable [DE] de en función de las escalas estándar sugeridas en libro del Catálogo de Elementos de Magerit que se presentan a continuación:

Información de Carácter Personal: Se relaciona fuertemente con la Confidencialidad y Autenticidad.

Tabla 14.

Información de Carácter Personal y su relación con la Confidencialidad y Autenticidad

[AL].pi1	Probablemente afecte gravemente a un grupo de individuos.
[AL].pi2	Probablemente quebrante seriamente la ley o algún reglamento de protección de información personal.
[AL].pi1	Probablemente afecte gravemente a un individuo
[AL].pi2	Probablemente quebrante seriamente leyes o regulaciones
[ME].pi1	Probablemente afecte a un grupo de individuos
[ME].pi2	Probablemente quebrante leyes o regulaciones
[ME].pi1	Probablemente afecte a un individuo
[ME].pi2	Probablemente suponga el incumplimiento de una ley o regulación
[ME].pi1	Pudiera causar molestias a un individuo
[ME].pi2	Pudiera quebrantar de forma leve leyes o regulaciones
[BA].pi1	Pudiera causar molestias a un individuo

Obligaciones legales: Se relaciona fuertemente con la Integridad.

Tabla 15.

Obligaciones legales se relaciona fuertemente con la Integridad

[MA].lro	Probablemente cause un incumplimiento excepcionalmente grave de una ley o regulación
[AL].lro	Probablemente cause un incumplimiento grave de una ley o regulación
[AL].lro	Probablemente sea causa de incumplimiento de una ley o regulación
[ME].lro	Probablemente sea causa de incumplimiento leve o técnico de una ley o regulación
[BA].lro	Pudiera causar el incumplimiento leve o técnico de una ley o regulación

Seguridad: Se relaciona fuertemente con la Integridad, Autenticidad y Trazabilidad.

Tabla 16.

Seguridad se relaciona fuertemente con la Integridad, Autenticidad y Trazabilidad

[EX].si	Probablemente sea causa de un incidente excepcionalmente serio de seguridad o dificulte la investigación de incidentes excepcionalmente serios
[MA].si	Probablemente sea causa de un serio incidente de seguridad o dificulte la investigación de incidentes serios
[AL].si	Probablemente sea causa de un grave incidente de seguridad o dificulte la investigación de incidentes graves
[ME].si	Probablemente sea causa de una merma en la seguridad o dificulte la investigación de un incidente
[BA].si	Pudiera causar una merma en la seguridad o dificultar la investigación de un incidente

Intereses comerciales o económicos: Se relaciona fuertemente con la Confidencialidad.

Tabla 17.

Intereses comerciales o económicos se relaciones fuertemente con la Confidencialidad

[MA].cei.a	De enorme interés para la competencia
[MA].cei.b	De muy elevado valor comercial
[MA].cei.c	Causa de pérdidas económicas excepcionalmente elevadas
[MA].cei.d	Causa de muy significativas ganancias o ventajas para individuos u organizaciones
[MA].cei.e	Constituye un incumplimiento excepcionalmente grave de las obligaciones contractuales relativas a la seguridad de la información proporcionada por terceros
[AL].cei.a	De alto interés para la competencia
[AL].cei.b	De elevado valor comercial
[AL].cei.c	Causa de graves pérdidas económicas
[AL].cei.d	Proporciona ganancias o ventajas desmedidas a individuos u organizaciones

Interrupción del servicio: Se relaciona fuertemente con la Disponibilidad.

Tabla 18.

Interrupción del servicio se relaciona fuertemente con la Disponibilidad

[MA].da	Probablemente cause una interrupción excepcionalmente seria de las actividades propias de la Organización con un serio impacto en otras organizaciones
[MA].da2	Probablemente tenga un serio impacto en otras organizaciones
[AL].da1	Probablemente cause una interrupción seria de las actividades propias de la Organización con un impacto significativo en otras organizaciones
[AL].da2	Probablemente tenga un gran impacto en otras organizaciones
[AL].da1	Probablemente cause la interrupción de actividades propias de la Organización con impacto en otras organizaciones
[AL].da2	Probablemente cause un cierto impacto en otras organizaciones
[ME].da	Probablemente cause la interrupción de actividades propias de la Organización
[BA].da	Pudiera causar la interrupción de actividades propias de la Organización

Operaciones: Se relaciona fuertemente con la Disponibilidad e Integridad.

Tabla 19.

Disponibilidad se relaciona fuertemente con la Disponibilidad e Integridad

[EX].olm	Probablemente cause un daño excepcionalmente serio a la eficacia o seguridad de la misión operativa o logística
[MA].olm	Probablemente cause un daño serio a la eficacia o seguridad de la misión operativa o logística
[AL].olm	Probablemente perjudique la eficacia o seguridad de la misión operativa o logística
[AL].olm	Probablemente merme la eficacia o seguridad de la misión operativa o logística más allá del ámbito local

Administración y gestión: Se relaciona fuertemente con la Disponibilidad e Integridad.

Tabla 20.

Administración y gestión se relaciona fuertemente con la Disponibilidad e Integridad

[MA].adm	Probablemente impediría seriamente la operación efectiva de la Organización, pudiendo llegar a su cierre
[AL].adm	Probablemente impediría la operación efectiva de la Organización
[AL].adm	Probablemente impediría la operación efectiva de más de una parte de la Organización
[ME].adm	Probablemente impediría la operación efectiva de una parte de la Organización
[BA].adm	Pudiera impedir la operación efectiva de una parte de la Organización

Pérdida de confianza (reputación): Se relaciona fuertemente con la Disponibilidad e Integridad.

Tabla 21.

Pérdida de Confianza se relaciona fuertemente con la Disponibilidad e Integridad

[MA].lg.a	Probablemente causaría una publicidad negativa generalizada por afectar de forma excepcionalmente grave a las relaciones a las relaciones con otras organizaciones
[MA].lg.b	Probablemente causaría una publicidad negativa generalizada por afectar de forma excepcionalmente grave a las relaciones a las relaciones con el público en general
[AL].lg.a	Probablemente causaría una publicidad negativa generalizada por afectar gravemente a las relaciones con otras organizaciones
[AL].lg.b	Probablemente causaría una publicidad negativa generalizada por afectar gravemente a las relaciones con el público en general
[AL].lg.a	Probablemente sea causa una cierta publicidad negativa por afectar negativamente a las relaciones con otras organizaciones
[AL].lg.b	Probablemente sea causa una cierta publicidad negativa por afectar negativamente a las relaciones con el público
[ME].lg	Probablemente afecte negativamente a las relaciones internas de la Organización
[ME].lg	Probablemente cause una pérdida menor de la confianza dentro de la Organización
[BA].lg	Pudiera causar una pérdida menor de la confianza dentro de la Organización

Persecución de delitos: Se relaciona fuertemente con la Integridad, Autenticidad y Trazabilidad.

Tabla 22.

Persecución de delitos se relaciona fuertemente con la Integridad, Autenticidad y Trazabilidad

[MA].crm	Impida la investigación de delitos graves o facilite su comisión
[ME].crm	Dificulte la investigación o facilite la comisión de delitos

Tiempo de recuperación del servicio: Se relaciona fuertemente con la Disponibilidad.

Tabla 23.

Tiempo de recuperación del servicio se relaciona fuertemente con la Disponibilidad

[EX].rto	RTO <30 minutos
[AL].rto	30 minutos <RTO < 4 horas
[ME].rto	4 horas < RTO < 1 día
[BA].rto	1 día < RTO < 5 días
[DE].rto	5 días < RTO

En función de estas escalas procedemos a valorar cada uno de los activos de información:

Tabla 24.

Valoración de los Activos: Compras - Ventas - Activos Fijos

INFORMACION	TIPO	NIVEL	SERVICIO	TIPO	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	AUTENTICIDAD	TRAZABILIDAD
Inventarios	[clasif]	[R]	Inventarios	[int]	[BA]	[AL]	[ME]	[AL]	[BA]
Ensamblaje	[clasif]	[R]	Ensamblaje	[int]	[BA]	[ME]	[ME]	[AL]	[BA]
Cartera Clientes	[clasif]	[R]	Cuentas por Cobrar	[int]	[ME]	[AL]	[ME]	[AL]	[ME]
Cartera Proveedores	[clasif]	[R]	Cuentas por Pagar	[int]	[ME]	[ME]	[ME]	[AL]	[ME]
Movimiento Financiero	[clasif]	[R]	Tesorería	[int]	[MA]	[AL]	[ME]	[AL]	[AL]
Transacciones Contables	[clasif]	[R]	Contabilidad	[int]	[ME]	[EX]	[ME]	[AL]	[AL]
Transacciones de Compra	[adm]		Mantenimiento de Compras e Importaciones Generación del XML ATS	[int] [ext]	[DE]	[AL]	[ME]	[AL]	[ME]
Transacciones de Venta	[adm]		Mantenimiento de Ventas y Exportaciones Generación del XML ATS	[int] [ext]	[DE]	[AL]	[ME]	[AL]	[ME]
Activos Fijos	[clasif]	[R]	Altas, Bajas de Activos Depreciación Etiquetado y Toma Física	[int]	[DE]	[ME]	[BA]	[AL]	[BA]
Información de Personal	[per]	[A]	Gestión del Recurso Humano	[int]	[AL]	[ME]	[BA]	[AL]	[AL]
Información de Selección	[clasif]	[R]	Selección de Personal	[int]	[ME]	[ME]	[BA]	[AL]	[AL]

Tabla 25.

Valoración de los Activos: Clientes - Anexos Contables - Perfiles de Usuarios - Bitácoras

INFORMACION	TIPO	NIVEL	SERVICIO	TIPO	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	AUTENTICIDAD	TRAZABILIDAD
Nóminas	[per]	[A]	Generación de Nómina	[int]	[AL]	[AL]	[ME]	[AL]	[AL]
Objetivos Individuales	[clasif]	[pub]	Definición de Objetivos	[int]	[BA]	[AL]	[ME]	[ME]	[BA]
Evaluaciones	[clasif]	[R]	Registro de Evaluaciones	[int]	[BA]	[AL]	[ME]	[ME]	[BA]
Clientes	[clasif]	[R]	Clientes	[int]	[EX]	[EX]	[EX]	[EX]	[EX]
Campañas	[clasif]	[R]	Campañas	[int]	[BA]	[BA]	[BA]	[ME]	[ME]
Solicitudes y Seguimiento	[clasif]	[R]	Solicitudes y Seguimiento	[int]	[BA]	[ME]	[NE]	[ME]	[ME]
Proformas	[clasif]	[R]	Proformas	[int]	[BA]	[ME]	[BA]	[BA]	[BA]
Citas / Turnos	[clasif]	[R]	Citas / Turnos	[int]	[BA]	[ME]	[AL]	[BA]	[ME]
Ortes	[clasif]	[R]	Ortes	[int]	[BA]	[ME]	[AL]	[ME]	[ME]
Ordenes de Trabajo	[clasif]	[R]	Ordenes de Trabajo	[int]	[BA]	[AL]	[AL]	[AL]	[AL]
Ordenes de Monitoreo	[clasif]	[R]	Ordenes de Monitoreo	[int]	[BA]	[AL]	[AL]	[AL]	[AL]
Contratos	[clasif]	[C]	Contratos	[int]	[BA]	[AL]	[ME]	[AL]	[AL]
Sistemas	[clasif]	[C]	Sistemas	[int]	[AL]	[EX]	[MA]	[MA]	[MA]
Robos	[clasif]	[C]	Robos	[int]	[EX]	[EX]	[AL]	[AL]	[AL]
Comisiones	[clasif]	[R]	Comisiones	[int]	[ME]	[ME]	[ME]	[AL]	[ME]
Facturación	[clasif]	[R]	Facturación	[int]	[BA]	[AL]	[AL]	[AL]	[AL]
Presupuesto de Ventas	[clasif]	[pub]	Presupuesto de Ventas	[int]	[BA]	[ME]	[BA]	[ME]	[ME]
Ventas	[adm]		Reports	[int]	[BA]	[AL]	[ME]	[ME]	[ME]
Indicadores	[clasif]	[C]	Business	[int]	[AL]	[AL]	[AL]	[AL]	[AL]
Anexos Contables Externos	[clasif]	[R]	Integración Contable	[int]	[BA]	[AL]	[ME]	[ME]	[ME]
Usuarios y Perfiles	[clasif]	[C]	Registro de Usuarios y Perfiles	[int]	[EX]	[EX]	[ME]	[MA]	[MA]
Menus y Opciones	[clasif]	[R]	Registro de Menus y Opciones	[int]	[EX]	[EX]	[ME]	[MA]	[MA]
Ejecución Procesos	[clasif]	[R]	Control de Procesos Batch	[int]	[EX]	[EX]	[ME]	[MA]	[MA]
Registros de Auditoría	[clasif]	[C]	Control de Auditoría	[int]	[EX]	[EX]	[ME]	[MA]	[MA]
Bitácora Llamadas	[clasif]	[R]	Call Center Renovaciones	[int]	[DE]	[BA]	[BA]	[BA]	[BA]
Bitácora Llamadas	[clasif]	[R]	Call Center Cobranzas	[int]	[DE]	[BA]	[BA]	[BA]	[BA]

Tabla 26.

Valoración de los Activos: Correos - Estadísticas - Información de Clientes

INFORMACION	TIPO	NIVEL	SERVICIO	TIPO	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	AUTENTICIDAD	TRAZABILIDAD
Correo Normal	[clasif]	[R]	Correo Normal	[int]	[AL]	[AL]	[AL]	[AL]	[AL]
Correo Corporativo	[clasif]	[R]	Correo Corporativo	[int]	[AL]	[AL]	[AL]	[AL]	[AL]
Correo Backup	[clasif]	[R]	Correo Backup	[int]	[AL]	[AL]	[ME]	[AL]	[AL]
Archivos Trabajo	[clasif]	[UC]	Compartición de Archivos	[int]	[ME]	[AL]	[ME]	[ME]	[ME]
Mensajes Localización SmsGprs	[vr]	[R]	Control Mensajes SMS	[int]	[EX]	[AL]	[EX]	[MA]	[MA]
	[vr]	[R]	Control de Mensages GPRS	[int]	[EX]	[AL]	[EX]	[MA]	[MA]
Estadísticas Mensajes	[clasif]	[R]	Análisis Estadístico de Mesajería	[int]	[AL]	[AL]	[ME]	[ME]	[ME]
Información Cliente Vehículos	[vr]		Portal Extranet Localizacion Vehicular	[ext]	[EX]	[AL]	[AL]	[EX]	[MA]
Información Cliente Personal	[vr]		Portal Extranet Localizacion Persona	ext]	[EX]	[AL]	[AL]	[EX]	[MA]
Usuarios del Dominio	[clasif]	[C]	Administración de Usuarios de Dominio	[int]	[EX]	[EX]	[AL]	[AL]	[AL]

3.1.8. CARACTERIZACIÓN Y VALORACIÓN DE LAS AMENAZAS

Para la caracterización de las amenazas tomamos como referencia la siguiente clasificación nos sugiere Magerit para:

Tipo de Activo

- [HW] Equipos informáticos (hardware).
- [D] Datos o información.
- [S] Servicios.
- [SW] Aplicaciones (software).
- [D.log] Registros de actividad.

Valoración de las amenazas.

- [MA] Muy alta, casi seguro, fácil.
- [A] Alta, muy alto, medio.
- [M] Media, posible, difícil.
- [B] Baja, poco probable, muy difícil.
- [MB] Muy baja, muy raro, extremadamente difícil.

3.1.8.1. DESASTRES DE ORIGEN NATURAL

Tabla 27.

Amenazas por Desastres Naturales

AMENAZA	ACTIVO	TIPO DE ACTIVO	EFECTO DE LA AMENAZA	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	AUTENTICIDAD	TRAZABILIDAD
Fuego	Centro de datos UIO 1 Y 2.	[HW]	Posibilidad de que el fuego acabe con los recursos del Sistema.			[B]		
Daños por agua	Centro de datos UIO 1 Y 2.	[HW]	Posibilidad de que el agua acabe con los recursos del Sistema.			[B]		
Desastres naturales	Centro de datos UIO 1 Y 2.	[HW]	Posibilidad de que los desastres naturales (excluyendo los incendios e inundaciones) acaben con los recursos del Sistema.			[B]		

3.1.8.2. DESASTRES DE ORIGEN INDUSTRIAL

Tabla 28.

Amenazas por Desastres Industriales

AMENAZA	ACTIVO	TIPO DE ACTIVO	EFECTO DE LA AMENAZA	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	AUTENTICIDAD	TRAZABILIDAD
Fuego	Centro de datos UIO 1 y 2.	[HW]	Posibilidad de que el fuego acabe con los recursos del Sistema ya sea de manera accidental o deliberada.			[B]		
Daños por agua	Centro de datos UIO 1 y 2.	[HW]	Posibilidad de que el agua acabe con los recursos del Sistema ya sea de manera accidental o deliberada.			[B]		
Desastres industriales	Centro de datos UIO 1 y 2.	[HW]	Posibilidad de que otros desastres debidos a la actividad humana: Explosiones, derrumbes, sobrecarga eléctrica, fluctuaciones eléctricas, accidentes de tráfico, acabe con los recursos del sistema.			[B]		
Contaminación mecánica	Centro de datos UIO 1 y 2.	[HW]	Posibilidad que por las vibraciones, polvo, suciedad, se acabe con los recursos del sistema.			[M]		
Avería de origen físico o lógico	Centro de datos UIO 1 y 2.	[HW]	Fallos en los equipos. Puede ser debido a un defecto de origen o sobrevenida durante el funcionamiento del sistema, esto puede acabar con los recursos del sistema.			[M]		
Corte del suministro eléctrico	Centro de datos UIO 1 y 2.	[HW]	El cese de energía, indisponibilidad del servicio.			[M]		
Condiciones inadecuadas de temperatura o humedad	Centro de datos UIO 1 y 2.	[HW]	Deficiencias en la aclimatación de los locales, excediendo los márgenes de trabajo de los equipos: excesivo calor, excesivo frío, exceso de humedad pueden acabar con los recursos del sistema.			[M]		
Fallo de servicios de comunicaciones	Centro de datos UIO2.	[COM]	Pérdida de los Medios de telecomunicación.			[A]		
Degradación de los soportes de almacenamiento de la información	Centro de datos UIO 1.	[HW]	No se puede restaurar la Bases de Datos.			[B]		

3.1.8.3. ERRORES Y FALLOS NO INTENCIONADOS.

Tabla 29.

Amenazas por Errores y Fallos no intencionados de Usuarios, Administración y Monitoreo

	AMENAZA	ACTIVO	TIPO DE ACTIVO	EFECTO DE LA AMENAZA	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	AUTENTICIDAD	TRAZABILIDAD
Errores de los usuarios	Nombres y apellidos incompletos, ruc incorrecto. Colocar al cliente en un canal incorrecto. Vehículo equivocado. Descripción incorrecta o incompleta el estado del vehículo. Detalle incorrecto de los documentos o herramientas que deja el cliente en el vehículo. Escoger mal el tipo de movimiento, artículo o línea de negocio. No seleccionar quien cancela. Generar mal los valores de quien cancela. Seleccionar servicios incorrectos. Colocar mal la fecha de vigencia del contrato. Seleccionar mal los servicios. Colocar mal el número de factura. Distribuir mal los valores a ser recaudados con el nombre equivocado.	Clientes Ortes Órdenes de trabajo. Órdenes de monitoreo. Contratos. Facturación.	[D]	Inconsistencia de la información.	A	MA	M		
Errores del admin.	Colocar un usuario dentro de un perfil equivocado. Dar autorizaciones de acceso a usuarios incorrectos.	Sistema de administración y seguridades.	[SW]	Aplicaciones no confiables por parte de quienes administran.	M	A	MA		
Errores de monitorización (log)	Nombres y apellidos incompletos. Ruc incorrecto. Colocar al cliente en un canal incorrecto. Vehículo equivocado. Colocar mal la fecha de vigencia del contrato. Seleccionar mal los servicios.	Clientes Contratos.	[D.log]	El inadecuado registro de actividades: falta de registros, registros incompletos, registros incorrectamente fechados, etc., ocasionan tener desconocimiento de las transacciones realizadas en los servidores			MA		MA

Tabla 30.

Amenazas por Errores y Fallos no intencionados de Configuración y Difusión de Software Dañino

AMENAZA	ACTIVO	TIPO DE ACTIVO	EFECTO DE LA AMENAZA	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	AUTENTICIDAD	TRAZABILIDAD
Errores de configuración	Error en la plantilla de los contratos. Contratos Plantilla contable con errores. Transacciones contables.	[D.conf]	La configuración mal realizada hace que las aplicaciones funcionan de manera errónea provocando pérdida de los datos relevantes del negocio.		MA			
Difusión de software dañino	Enviar virus, espías (spyware), gusanos, troyanos, bombas lógicas, etc., a las aplicaciones sin intención.	[SW]	Las aplicaciones no podrían funcionar correctamente y de esta manera queda ineficiente la atención al cliente.	MA	MA	MA		

Sistema Administrativo Financiero.

Sistema Administración Tributaria.

Sistema de activos fijos.

Sistema de gestión humana

Sistema de evaluaciones

Sistema de administración de clientes.

Accouting Interfase

Sistema de administración de seguridades.

Posfix.

CIFS.

Sistema de control de mensajes.

Sistema de análisis de mensajes.

Tabla 31.

Amenazas por Errores y Fallos no intencionados en la Información

AMENAZA	ACTIVO	TIPO DE ACTIVO	EFECTO DE LA AMENAZA	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	AUTENTICIDAD	TRAZABILIDAD
Errores de secuencia	Enviar mails sin tomar en cuenta el orden de prioridad.	Correo corporativo	[S]	Alteración accidental del orden de los mensajes transmitidos.		M		
Alteración accidental de la información	Alterar accidentalmente la información y esto se puede identificar con mayor facilidad sobre los datos en general.	BddConta (SqlServer 2000) BddTrib (SqlServer 2000) BddAcf (Dbase II) BddRrhh MySQL (5.5.23) Remote Desktop BddEval (SQLServer 2005) BddCall1 (Mysql 5.0.77) BddCall2 (Mysql5.0.77) BddCrm (Mysql 5.5.23) BddCrm (Mysql 5.1.27) BddCrm (Mysql 5.5.14) BddExtranet(SQLServer 2005)	[SW]	Información incorrecta.		A		
Destrucción de información	Eliminar accidentalmente la información, con ánimo de obtener un beneficio personal o causar daño.	BddConta (SqlServer 2000) BddTrib (SqlServer 2000) BddAcf (Dbase II) BddRrhh MySQL (5.5.23) Remote Desktop BddEval (SQLServer 2005) BddCall1 (Mysql 5.0.77) BddCall2 (Mysql5.0.77) BddCrm (Mysql 5.5.23) BddCrm (Mysql 5.1.27) BddCrm (Mysql 5.5.14) BddExtranet(SQLServer 2005)	[SW]	Bases de datos sin información o incompletas.			M	
Fugas de información	Falsificación de datos del cliente.	Cartera clientes	[D]	Conversaciones acerca de la información de la compañía.			B	
	Falsificación de datos del personal.	Información del personal.						
	Falsificación de usuarios y claves.	Usuarios y perfiles						
	Acceso al sistema a personas que no son parte del personal de la empresa.	Menús y opciones						

Tabla 32.

Amenazas por Errores y Fallos no intencionados en el Software y Equipos

AMENAZA		ACTIVO	TIPO DE ACTIVO	EFECTO DE LA AMENAZA	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	AUTENTICIDAD	TRAZABILIDAD
Vulnerabilidades de los programas (software)	Defectos en el código al momento de programar.	Sistema de administración de los clientes.	[SW]	Datos erróneos que no pueden ser por mal uso de las aplicaciones de los usuarios.	MB	A	B		
		Sistema de administración de los clientes.							
Errores de mantenimiento / actualización de programas (software)	Falla del funcionamiento de las aplicaciones debido a que las mismas tenían defectos.	Sistema de administración de seguridades.	[SW]	Programas con mal funcionamiento.		[A]	[B]		
		Posfix							
		CIFS							
		Sistema de administración tributaria.							
Caída del sistema por agotamiento de recursos	Saturación del sistema informático.	Clientes	[S]	Carencia de recursos suficientes provoca la caída del sistema cuando la carga de trabajo es desmesurada.			[B]		
		Solicitudes y seguimiento							
		Proformas							
		Citas o Turnos							
		Órdenes de trabajo							
		Órdenes de monitoreo.							
		Contratos.							
		Facturación.							
		Comisiones.							
		Ventas.							
Pérdida de equipos	No hay acceso a internet.	Rack 1I	[HW]	Carencia de un medio para prestar los servicios.			[B]		

3.1.8.4. ATAQUES INTENCIONADOS

Tabla 33.

Ataques Intencionados: Manipulación de la Configuración - Suplantación de Identidad - Abuso de Privilegios

AMENAZA		ACTIVO	TIPO DE ACTIVO	EFECTO DE LA AMENAZA	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	AUTENTICIDAD	TRAZABILIDAD
Manipulación de la configuración	Errores al colocar privilegios de acceso.	Registro de menús y opciones.	[D.log]	Configuración incorrecta por parte del administrador.		B			
Suplantación de la identidad del usuario	Los usuarios no autorizados podrían modificar la información a su conveniencia.	Clientes Solicitudes y seguimiento Proformas Citas o Turnos Órdenes de trabajo Órdenes de monitoreo. Contratos. Facturación. Comisiones. Ventas.	[D]	Información errónea.	A	MB		B	
Abuso de privilegios de acceso	Los usuarios podrían crear, modificar y eliminar la información dependiendo de los privilegios que tengan.	Clientes Solicitudes y seguimiento Proformas Citas o Turnos Órdenes de trabajo Órdenes de monitoreo. Contratos. Facturación. Comisiones. Ventas.	[D]	Al tener la información errónea podrían llegar a surgir problemas de integridad.	MA	A	B		

Tabla 34.

Ataques Intencionados: Uso No Previsto - Alteración de Secuencia - Acceso no autorizado

AMENAZA		ACTIVO	TIPO DE ACTIVO	EFECTO DE LA AMENAZA	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	AUTENTICIDAD	TRAZABILIDAD
Uso no previsto	Usar los recursos del sistema para juegos, consultas personales, programas personales, etc. Y esto a su vez podrían ser causantes de un servicio incompetente.	Clientes Solicitudes y seguimiento Proformas Citas o Turnos Órdenes de trabajo Órdenes de monitoreo. Contratos. Facturación. Comisiones. Ventas.	[S]	Utilización de los recursos del sistema para fines no previstos, es decir, típicamente de interés personal.	A	B	MA		
Alteración de secuencia	Enviar mails incorrectos con la intención de causar problemas.	Correo corporativo	[S]	Alteración intencional del orden de los mensajes transmitidos.		B			
Acceso no autorizado	Acceder al sistema sin tener autorización se puede manipular la información dejando datos incorrectos.	Clientes Solicitudes y seguimiento Proformas Citas o Turnos Órdenes de trabajo Órdenes de monitoreo. Contratos. Facturación. Comisiones. Ventas.	[D]	Al haber un fallo del sistema de identificación y autorización los usuarios consiguen acceder a los recursos del sistema sin tener autorización.	MA	A			

Tabla 35.

Ataques Intencionados: Repudio - Modificación de la Información

AMENAZA	ACTIVO	TIPO DE ACTIVO	EFECTO DE LA AMENAZA	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	AUTENTICIDAD	TRAZABILIDAD
Repudio	Clientes Solicitudes y seguimiento Proformas Citas o Turnos Órdenes de trabajo Órdenes de monitoreo. Contratos. Facturación. Comisiones. Ventas.	[S]	Negación de acciones realizadas.		MA			
A l negar que se ha enviado, recibido o entregado mensajes podría afectar de gran manera a la información o servicios ya que esos mensajes podrían ser importantes o urgentes y se llegaría incluso a perder clientes debido a la ineficiencia de los usuarios.								
No dar de baja artículos o dar de baja más de los artículos que en realidad son.	Inventarios							
Modificación deliberada de la información	Cartera clientes Cartera proveedores Transacciones contables Contratos Facturación Comisiones Registros de auditoría Información del cliente vehículos	[D]	Modificar intencionalmente la información por obtener algún beneficio o simplemente por perjudicar ya sea a una persona o a la empresa.		MA			
Canal incorrecto, datos personales erróneos, vehículos equivocados, Datos personales erróneos. Descuadre al cierre de mes o del año. Servicios y fecha incorrecta. Facturas físicas diferentes a las del sistema. Comisiones a personas incorrectas. Se tendría una inconsistencia sobre los registros. Información incorrecta en la página del cliente.								

Tabla 36.

Ataques Intencionados: Destrucción de la Información - Divulgación de la Información

AMENAZA		ACTIVO	TIPO DE ACTIVO	EFECTO DE LA AMENAZA	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	AUTENTICIDAD	TRAZABILIDAD
Destrucción de información	Eliminar intencionalmente la información, con ánimo de obtener un beneficio personal o causar daño.	BddConta (SqlServer 2000) BddTrib (SqlServer 2000) BddAcf (Dbase II) BddRrhh MySQL (5.5.23) Remote Desktop BddEval (SQLServer 2005) BddCall1 (Mysql 5.0.77) BddCall2 (Mysql5.0.77) BddCrm (Mysql 5.5.23) BddCrm (Mysql 5.1.27) BddCrm (Mysql 5.5.14) BddExtranet(SQLServer 2005)	[SW]	Bases de datos sin información.			B		
Divulgación de la información	Falsificación de datos del cliente.	Cartera clientes	[D]	Revelar la información a personas ajenas a la compañía.	MA				
	Falsificación de datos del personal.	Información del personal.							
	Falsificación de usuarios y claves.	Usuarios y perfiles							
	Acceso al sistema a personas que no son parte del personal de la empresa.	Menús y opciones							

Tabla 37.

Ataques Intencionados: Manipulación de Programas

AMENAZA	ACTIVO	TIPO DE ACTIVO	EFECTO DE LA AMENAZA	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	AUTENTICIDAD	TRAZABILIDAD
Manipulación de programas	Al modificar el código de los programas se podría capturar los datos y enviar a otra base para uso personal indebido.	Sistema administrativo financiero.	[SW]	Al realizar una alteración intencionada del funcionamiento de los programas, las aplicaciones funcionarían de manera incorrecta.	M	A	MB	
	Dejar con un mal funcionamiento las aplicaciones.	Sistema administración tributaria. Sistema activos fijos. Sistema de gestión humana. Sistema de evaluaciones Sistema de administración de clientes. Accouting interfase. Sistema de administración de seguridades. Call center asterix. Posfix. CIFS Sistema de control de mensajes Sistema de análisis de mensajes Sistema web portal Tracklink. Sistema web portal véstigo. Active directory.						

3.1.9. CARACTERIZACIÓN Y VALORACIÓN DE LAS SALVAGUARDAS

3.1.9.1. PROTECCIONES GENERALES U HORIZONTALES

Tabla 38.

Protección a los activos: Clientes - Facturación - Base de Datos

ACTIVOS	AMENAZAS	SALVAGUARDA	ACIONES A TOMAR	IMPLEMENTADO
Clientes				
Solicitudes y seguimiento Proformas Citas o Turnos				SI
Órdenes de trabajo			Antiviurs, Anti-spyware, firewall.	
Órdenes de monitoreo.			Uso de claves seguras, con combinación de números, letras y caracteres especiales.	NO
Contratos.	Suplantación de la identidad del usuario	H.IA Identificación y autenticación	Control de las últimas claves utilizadas, no se deben repetir las claves.	NO
Facturación.			Implementar como Política el No ingresar usuarios y claves en links extraños que lleguen por correo electrónico.	NO
Comisiones.			No compartir información financiera	
			Asegurarse que en las que se ingresa los datos tengan el prefijo https://.	NO
Ventas.			No proporcionar información financiera o personal en encuestas telefónicas.	NO
BddConta (SqlServer 2000) BddTrib (SqlServer 2000) BddAcf (Dbase II) BddRrhh MySQL (5.5.23) Remote Desktop BddEval (SQLServer 2005) BddCall1 (Mysql 5.0.77)		H.IA Identificación y autenticación H.AC Control de acceso lógico H.tools.DLP DLP: Herramienta de monitorización de contenidos	Uso de claves seguras, con combinación de números, letras y caracteres especiales.	NO
BddCall2 (Mysql5.0.77)	Destrucción de información		Contar un adecuado almacenamiento de datos, para evitar el extravío, sustracción o deterioro.	NO
BddCrm (Mysql 5.5.23)		D Protección de la información	Contar con sitios alternos de operación, donde haya la información y aplicaciones críticas de la información.	NO
BddCrm (Mysql 5.1.27)			Crear copias de seguridad periódicamente.	SI
BddCrm (Mysql 5.5.14)		D.I Aseguramiento de la integridad	Tener un repositorio de datos, para el backup periódico de los archivos del usuario.	SI
BddExtranet(SQLServer 2005)			Establecer una política de respaldos.	NO

Tabla 39.

Protección a los activos: Clientes - Facturación – Ventas

ACTIVOS	AMENAZAS	SALVAGUARDA	ACIONES A TOMAR	IMPLEMENTADO
Cartera clientes			Concientizar a los empleados de la empresa	SI
Información del personal.			Establecer una Política de seguridad	NO
Usuarios y perfiles	Fugas de información	H.IA Identificación y autenticación	Clasificar la información en públicos, confidenciales y privados, para la información confidencias utilizar un sw calificado para proteger su confidencialidad	NO
Menús y opciones			Proteger los mensajes de correo electrónico	NO
Clientes				
Solicitudes y seguimiento		H.IA Identificación y autenticación		
Proformas				
Citas o Turnos				
Órdenes de trabajo	Acceso no autorizado		Uso de claves seguras, con combinación de números, letras y caracteres especiales.	NO
Órdenes de monitoreo.		S.SC Se aplican perfiles de seguridad		
Contratos.				
Facturación.				
Comisiones.				
Ventas.			Control de las últimas claves utilizadas.	NO
Clientes				
Solicitudes y seguimiento		H.AC Control de acceso lógico.		
Proformas				
Citas o Turnos		H.ST Segregación de tareas	Concientizar a los empleados de la empresa.	SI
Órdenes de trabajo				
Órdenes de monitoreo.				
Contratos.	Abuso de privilegios de acceso		Establecer una Política de seguridad.	NO
Facturación.		SW.SC Se aplican perfiles de seguridad	Establecer una revisión periódica de los derechos y permisos efectivos de los usuarios.	NO
Comisiones.			Implementar un sistema de control de tráfico que monitoree el comportamiento de los usuarios y aplicaciones que están en uso por parte de estos.	NO
Ventas.			Implementar cifrado de datos que sean considerados como confidenciales o altamente críticos.	NO

Tabla 40.

Protección a los activos: Clientes - Facturación - Ventas - Transacciones Contables

ACTIVOS	AMENAZAS	SALVAGUARDA	ACIONES A TOMAR	IMPLEMENTADO
Inventarios Cartera clientes. Cartera proveedores. Transacciones contables. Contratos. Facturación.	Modificación deliberada de la información	H.AC Control de acceso lógico H.tools.DLP DLP: Herramienta de monitorización de contenidos D Protección de la información		NO
Comisiones. Registro de auditoría.		D.I Aseguramiento de la integridad	Implementar un sistema de monitoreo en línea que dispare alarmas al ejecutar un cambio de un usuario no autorizado	
Información del cliente vehículos Clientes Solicitudes y seguimiento Proformas Citas o Turnos Órdenes de trabajo Órdenes de monitoreo. Contratos. Facturación. Comisiones. Ventas. Cartera clientes	Uso no previsto	SW.SC Se aplican perfiles de seguridad H.AC Control de acceso lógico SW.SC Se aplican perfiles de seguridad SW.op Explotación / Producción SW.CM Cambios (actualizaciones y mantenimiento) SW.end Terminación	Revisión periódica de derechos y permisos efectivos de los usuarios. Implementar un mecanismo de control centralizado para monitorear el uso de los equipos de los usuarios y garantizar que no se usen estos equipos para fines no previstos.	NO SI
Información del personal. Usuarios y perfiles	Divulgación de información	H.AC Control de acceso lógico H.tools.DLP DLP: Herramienta de monitorización de contenidos	Clasificar la información en públicos, confidenciales y privados, para la información confidencias utilizar un sw calificado para proteger su confidencialidad.	NO
Menús y opciones		D Protección de la información	Concientizar a los empleados de la empresa.	SI

Tabla 41.

Protección a los activos: Bases de Datos - Ordenes de Trabajo

ACTIVOS	AMENAZAS	SALVAGUARDA	ACIONES A TOMAR	IMPLEMENTADO
BddConta (SqlServer 2000)				
BddTrib (SqlServer 2000)				
BddAcf (Dbase II)				
BddRrhh MySQL (5.5.23) Remote Desktop			Definir accesos Críticos, determinados por su importancia o impacto operativo	SI
BddEval (SQLServer 2005)				
BddCall1 (Mysql 5.0.77)				
BddCall2 (Mysql5.0.77)				
BddCrm (Mysql 5.5.23)				
BddCrm (Mysql 5.1.27)				
BddCrm (Mysql 5.5.14)			Definir controles asociados al perfil de funciones	NO
BddExtranet(SQLServer 2005)	Alteración accidental de la información	H.ST Segregación de tareas	Establecer controles Manuales.	NO
Clientes				
Ortes				
Órdenes de trabajo				SI
Órdenes de monitoreo.				
Contratos.				
Facturación.	Errores de los usuarios	H.IR Gestión de incidencias	Implementación de un Sistema de Mesa de Ayuda (glpisoftware).	
Clientes				
		H.IR Gestión de incidencias H.tools.TM Herramienta de monitorización de tráfico H.tools.LA Herramienta para análisis de logs		NO
	Errores de monitorización (log)	H.AU Registro y auditoría	Implementar un sistema de monitorización de aplicaciones.	
Contratos.				

Tabla 42.

Protección a los activos: Sistemas de Administración

ACTIVOS	AMENAZAS	SALVAGUARDA	ACIONES A TOMAR	IMPLEMENTADO
Sistema Administrativo Financiero. Sistema Administración Tributaria. Sistema de activos fijos. Sistema de gestión humana Sistema de evaluaciones Sistema de administración de clientes. Accouting Interfase Sistema de administración de seguridades. Posfix. CIFS. Sistema de control de mensajes. Sistema de análisis de mensajes.	Difusión de software dañino	H.IR Gestión de incidencias	Implementación de Antivirus	SI
Clientes Solicitudes y seguimiento Proformas Citas o Turnos Órdenes de trabajo Órdenes de monitoreo. Contratos. Facturación. Comisiones. Ventas.	Caída del sistema por agotamiento de recursos	H.IR Gestión de incidencias S.A Aseguramiento de la disponibilidad	Establecer como Política el Monitoreo de Red el estado y el uso de los recursos como consumo de memoria, ancho de banda, estadísticas históricas de funcionamiento, estado de ups de emergencia(Cacti+Nagios= Pandora FMS)	NO

Tabla 43.

Protección a los activos: Centro de Datos

ACTIVOS	AMENAZAS	SALVAGUARDA	ACIONES A TOMAR	IMPLEMENTADO
Centro de datos UIO 1 y 2.	Fuego	H.tools Herramientas de seguridad S.A Aseguramiento de la disponibilidad Protección de las instalaciones L.design Diseño L.depth Defensa en profundidad L.AC Control de los accesos físicos L.A Aseguramiento de la disponibilidad L.end Terminación BC Continuidad del negocio BC.BIA Análisis de impacto (BIA)	Establecer como Política de Seguridad, la revisión periódica de las instalaciones eléctricas del edificio.	SI
		BC.DRP Plan de recuperación de desastres (DRP)	Extintor de incendio.	SI
Centro de datos UIO 1 y 2.	Daños por agua	H.tools Herramientas de seguridad S.A Aseguramiento de la disponibilidad Protección de las instalaciones L.design Diseño L.depth Defensa en profundidad L.AC Control de los accesos físicos L.A Aseguramiento de la disponibilidad L.end Terminación Plan de recuperación ante desastres. BC Continuidad del negocio BC.BIA Análisis de impacto (BIA)	Establecer como Política de Seguridad, la revisión periódica de las instalaciones de agua.	NO
			Revisión periódica del techo del DataCenter.	SI
		BC.DRP Plan de recuperación de desastres (DRP)	Revisión periódica de fugas en el aire acondicionado.	SI

Tabla 44.

Protección a los activos: Centro de Datos - Sistema de Administración de los Clientes

ACTIVOS	AMENAZAS	SALVAGUARDA	ACIONES A TOMAR	IMPLEMENTADO
Centro de datos UIO 1 y 2.	Desastres naturales	H.tools Herramientas de seguridad S.A Aseguramiento de la disponibilidad Protección de las instalaciones L.design Diseño L.depth Defensa en profundidad L.AC Control de los accesos físicos L.A Aseguramiento de la disponibilidad L.end Terminación BC Continuidad del negocio BC.BIA Análisis de impacto (BIA) BC.DRP Plan de recuperación de desastres (DRP) H.tools Herramientas de seguridad S.A Aseguramiento de la disponibilidad AUX Elementos auxiliares AUX.A Aseguramiento de la disponibilidad Protección de las instalaciones L.design Diseño L.depth Defensa en profundidad L.AC Control de los accesos físicos L.A Aseguramiento de la disponibilidad L.end Terminación BC Continuidad del negocio BC.BIA Análisis de impacto (BIA) BC.DRP Plan de recuperación de desastres (DRP)	Plan de contingencia y mitigación de riesgos contra desastres naturales.	NO
Centro de datos UIO 1 y 2.	Desastres industriales		Realizar un plan en el que se mantenimiento periódico a las instalaciones.	SI
Sistema de administración de los clientes.	Vulnerabilidades de los programas (software)	H.tools.AV Herramienta contra código dañino H.tools.VA Herramienta de análisis de vulnerabilidades H.VM Gestión de vulnerabilidades NEW Adquisición / desarrollo NEW.S Servicios: Adquisición o desarrollo NEW.SW Aplicaciones: Adquisición o desarrollo NEW.HW Equipos: Adquisición o desarrollo NEW.MP Soportes de I.	Establecer como Política la creación de Documentación sobre aplicaciones desarrolladas internamente	NO

Tabla 45.

Protección a los activos: Centro de Datos - Sistema de Administración de los Clientes - Rack 1I

ACTIVOS	AMENAZAS	SALVAGUARDA	ACIONES A TOMAR	IMPLEMENTADO
Sistema de administración de los clientes.	Errores de mantenimiento / actualización de programas (software)	H.tools.AV Herramienta contra código dañino S.start Aceptación y puesta en operación NEW Adquisición / desarrollo NEW.S Servicios: Adquisición o desarrollo NEW.SW Aplicaciones: Adquisición o desarrollo NEW.HW Equipos: Adquisición o desarrollo NEW.COM Comunicaciones: Adquisición o contratación NEW.MP Soportes de Información: Adquisición	Establecer una Política de control de cambios.	NO
Sistema de adm. de seguridades. Posfix - CIFS Sistema de adm. tributaria.		NEW.C Productos certificados o acreditados	Creación de un ambiente de pruebas.	NO
Contratos	Errores de configuración	H.tools.CC Herramienta de chequeo de configuración	Efectuar una auditoria de configuración, para comprobar si son susceptibles a manipulación	NO
Transacciones contables			Establecer adecuados mecanismos de control de acceso físico.	NO
Rack 1I	Pérdida de equipos	H.tools.SFV Verificación de las funciones de seguridad	Hacer un monitoreo automatizado de los accesos.	NO
			Lugares a los que pueden tener acceso a los visitantes y personas ajenas a la institución.	NO
			Implementar un sistema de monitoreo de actividades del personal interno como de las personas ajenas a la institución.	NO
			Asignar tarjetas de acceso a los visitantes diferentes al personal interno, para que puedan ser identificados fácilmente.	NO
Centro de datos UIO 1 y 2.	Contaminación mecánica	S.A Aseguramiento de la disponibilidad Protección de las instalaciones L.design Diseño L.depth Defensa en profundidad L.AC Control de los accesos físicos L.A Aseguramiento de la disponibilidad	Mantenimiento periódico de los equipos.	SI
		L.end Terminación	Adquisición de accesorios de protección.	NO

Tabla 46.

Protección a los activos: Centro de Datos

ACTIVOS	AMENAZAS	SALVAGUARDA	ACIONES A TOMAR	IMPLEMENTADO
		S.A Aseguramiento de la disponibilidad AUX.AC Climatización Protección de las instalaciones L.design Diseño L.depth Defensa en profundidad L.AC Control de los accesos físicos	Mantenimiento periódico de los equipos.	SI
Centro de datos UIO 1 y 2.	Avería de origen físico o lógico	L.A Aseguramiento de la disponibilidad	Adquisición de accesorios de protección.	NO
		L.end Terminación S.A Aseguramiento de la disponibilidad AUX.wires Protección del cableado AUX.start Instalación	Respaldar la información periódicamente.	NO
		AUX.power Suministro eléctrico Protección de las Instalaciones L.design Diseño L.depth Defensa en profundidad L.AC Control de los accesos físicos	Instalar Generadores de Energía alternos.	SI
Centro de datos UIO 1 y 2.	Corte del suministro eléctrico	L.A Aseguramiento de la disponibilidad L.end Terminación S.A Aseguramiento de la disponibilidad Protección de las instalaciones L.design Diseño L.depth Defensa en profundidad L.AC Control de los accesos físicos	Instalar un Medidor de temperatura y Humedad.	NO
Centro de datos UIO 1 y 2.	Condiciones inadecuadas de temperatura o humedad	L.A Aseguramiento de la disponibilidad L.end Terminación S.A Aseguramiento de la disponibilidad	Revisión Periódica de las Instalaciones.	SI
Centro de datos UIO 1 y 2.	Fallo de servicios de comunicaciones	HW Protección de los equipos informáticos HW.start Puesta en producción HW.SC Se aplican perfiles de seguridad HW.A Aseguramiento de la disponibilidad HW.op Operación HW.CM Cambios (actualizaciones y mantenimiento) HW.end Terminación HW.PCD Informática móvil HW.print Reproducción de documentos HW.pabx Protección de la centralita telefónica (PABX)	Mantenimiento periódico de la arquitectura de comunicación.	NO
		L.end Terminación	Instalación de la herramienta para monitoreo de enlaces. (Cacti+Nagios= Pandora FMS)	NO

Tabla 47.

Protección a los activos: Sistemas de Información

ACTIVOS	AMENAZAS	SALVAGUARDA	ACIONES A TOMAR	IMPLEMENTADO
Centro de datos UIO 1 y 2. Sistema administrativo financiero. Sistema administración tributaria. Sistema activos fijos. Sistema de gestión humana. Sistema de evaluaciones Sistema de administración de clientes. Accouting interfase. Sistema de administración de seguridades. Call center asterix. Posfix. CIFS Sistema de control de mensajes Sistema de análisis de mensajes Sistema web portal Tracklink. Sistema web portal véstigo. Active directory.	Degradación de los soportes de almacenamiento de la información	D.A Copias de seguridad de los datos (backup) S.A Aseguramiento de la disponibilidad	Realizar pruebas de recuperación de datos periódicamente.	NO
	Manipulación de programas	H.IR Gestión de incidencias	Implementar un sistema de Mesa de Ayuda (GLPI).	SI
Clientes Solicitudes y seguimiento Proformas Citas o Turnos Órdenes de trabajo Órdenes de monitoreo. Contratos. Facturación. Comisiones. Ventas.	Repudio	H.IR Gestión de incidencias	Implementar un sistema de recepción de comentarios, sugerencias y quejas de los clientes (GLPI).	SI
Correo corporativo	Alteración de secuencia	H.ST Segregación de tareas	Implementar un plan en el que se pueda establecer la prioridad y de acuerdo a eso ir respondiendo.	NO
Registro de menús y opciones.	Manipulación de la configuración	H.tools.CC Herramienta de chequeo de configuración	Efectuar una auditoria de configuración, para comprobar si son susceptibles a manipulación	NO
Sistema de administración y seguridades.	Errores del administrador.	H.IR Gestión de incidencias	Establecer una política de seguridad de contraseñas diferentes para los diferentes servidores. Segmentar la red, usando listas de control de acceso.	NO

3.1.10. ESTIMACION DEL ESTADO DEL RIESGO

Siguiendo la metodología MAGERIT 3.0, debemos establecer la influencia que tienen las amenazas en los activos de acuerdo a la **"Degradación"** que le provocarían y a la **"Probabilidad"** de que la amenaza se materialice.

Como resultado se tiene una estimación fundada de lo que puede ocurrir es decir el IMPACTO y de lo que probablemente ocurra es decir el RIESGO.

Con la información del porcentaje de degradación y la probabilidad de ocurrencia tenemos los elementos necesarios para establecer el **"Impacto Potencial"** que es la medida del daño que le puede causar al activo la materialización de la amenaza, sin tomar en cuenta las salvaguardas existentes.

Se conoce como **"Impacto Acumulado"** al impacto potencial calculado sobre cada activo tomando en cuenta su propio valor más el valor de todos los activos que dependen de él y las amenazas a las que está expuesto, en cambio el **"Impacto Repercutido"** es el impacto potencial calculado tomando en cuenta su propio valor y las amenazas de a las que están expuestos los activos de los que depende.

La medida del probable daño al sistema tomando en cuenta el Impacto Potencial y la probabilidad de ocurrencia se la denomina como **"Riesgo Potencial"**, si se toma en cuenta el Impacto Acumulado obtenemos el **"Riesgo Acumulado"** y aplicando el Impacto Repercutido tenemos el **"Riesgo Repercutido"**.

Para impedir o reducir la probabilidad de que una amenaza se materialice se han definido un conjunto de salvaguardas, a la medida del daño que se le puede causar a un activo tomando en cuenta las salvaguardas implementadas se le denomina **“Impacto Residual”**.

La eficacia de las salvaguardas implementadas, logra disminuir la degradación del activo, quedando una degradación que no consiguen contrarrestar las salvaguardas aplicadas, a esto le conoce como **“Degradación Residual”**.

Al riesgo que está sometido el sistema una vez establecidas las salvaguardas se le denomina **“Riesgo Residual”** y lo calculamos tomando en cuenta el Impacto Residual y la probabilidad residual de ocurrencia.

En el siguiente gráfico, se muestra el flujo por el que pasa el Impacto Residual y el Riesgo Residual.

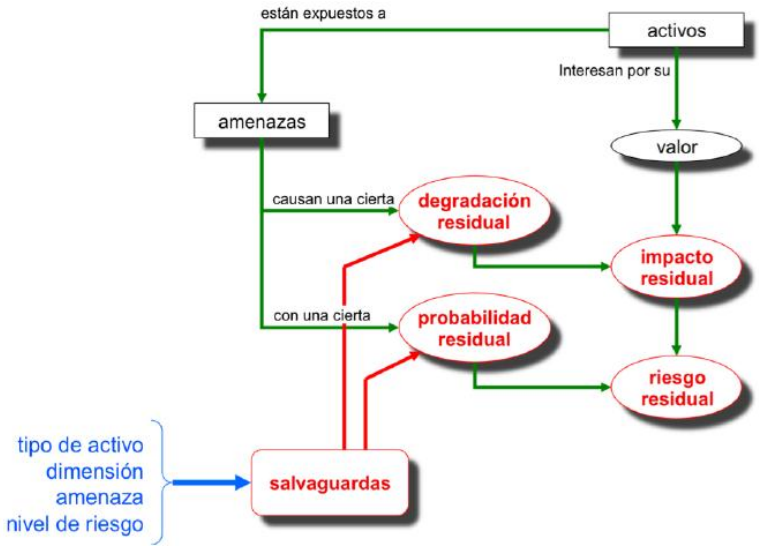

Figura 28. Flujo del Impacto Residual y Riesgo Residual

A continuación establecemos las escalas sugeridas por Magerit 3.0 para lograr la estimación del riesgo:

Para la determinación de la degradación del Activo “D” tomamos en cuenta una escala porcentual 0 a 100%.

Para establecer la Probabilidad de que una amenaza se materialice su Ocurrencia utilizaremos la frecuencia esperada de ocurrencia (ARO – Annual Rate of Occurrence) tomando la siguiente escala nominal:

Tabla 48.

Escala Nominal para Establecer la Probabilidad que una amenaza se materialice

	Probabilidad	Ocurrencia	Equivalencia
MA	muy alta	casi seguro	Fácil
A	Alta	muy alto	Medio
M	Media	posible	Difícil
B	Baja	poco probable	muy difícil
MB	muy baja	muy raro	extremadamente difícil

Para establecer el Impacto tomamos en cuenta la siguiente escala:

Tabla 49.

Escala para Establecer el Impacto

	Impacto	Valor	Observación
EX	Extremo	10	Activos que requieren atención inmediata
MA	Muy Alto	9	
AL	Alto	6 - 8	
ME	Medio	3 - 5	
BA	Bajo	1 – 2	
DE	Despreciable	0	Impacto despreciable

El cálculo del Impacto está determinado por el V (valor del activo) x D (% de degradación) para lo cual establecemos la siguiente tabla:

Tabla 50.

Escala para calcular el Impacto

		Degradación del Activo				
IMPACTO		**20%**	**40%**	**60%**	**80%**	**100%**
Valor del Activo	EX	AL	MA	EX	EX	EX
	MA	ME	AL	MA	MA	MA
	AL	BA	ME	AL	AL	AL
	ME	DE	BA	ME	ME	ME
	BA	DE	DE	BA	BA	BA
	DE	DE	DE	DE	DE	DE

Para establecer el Riesgo tomamos en cuenta la siguiente escala:

Tabla 51.

Escala para Establecer el Riesgo

	Riego	Valor	Observación
MA	Crítico	9 - 10	Riesgo Extremadamente Alto
A	Importante	7 - 8	
M	Apreciable	5 - 6	
B	Bajo	3 - 4	
MB	Despreciable	0 - 2	Riesgo despreciable

El cálculo del Riesgo está determinado por el I (Impacto) × F (frecuencia) para lo cual establecemos la siguiente tabla:

Tabla 52.

Escala para calcular el Riesgo

		Probabilidad de que se materialice una amenaza				
RIESGO		**MB**	**B**	**M**	**A**	**MA**
Impacto	EX	MA	MA	MA	MA	MA
	MA	A	MA	MA	MA	MA
	AL	M	A	A	MA	MA
	ME	B	M	M	A	A
	BA	MB	B	B	M	M
	DE	MB	MB	MB	B	B

3.1.10.1. ESTIMACION DEL ESTADO DE RIESGO POR DESASTRES DE ORIGEN NATURAL

Tabla 53.

Análisis de Estimación del Riesgo por Desastres de Origen Natural

AMENAZA	ACTIVO	VALORACION DEL ACTIVO	TIPO DE ACTIVO	EFECTO DE LA AMENAZA	DIMENSIONES AFECTADAS	DEGRADACION DEL VALOR DEL ACTIVO	PROBABILIDAD DE OCURRENCIA DE LA AMENAZA	IMPACTO POTENCIAL	RIESGO POTENCIAL	SALVAGUARDA IMPLEMENTADA	EFICACIA DE LA SALVAGUARDA	DEGRADACION RESIDUAL	PROBABILIDAD RESIDUAL	IMPACTO RESIDUAL	RIESGO RESIDUAL
Fuego	Centro de datos UIO 1 Y 2.	EX	[HW]	Posibilidad de que el fuego acabe con los recursos del Sistema.	1. [D] disponibilidad	100%	MB	EX	MA	SI	A	20%	MB	MA	A
Daños por agua	Centro de datos UIO 1 Y 2.			Posibilidad de que el agua acabe con los recursos del Sistema.		100%	MB	EX	MA	SI	MB	100%	MB	EX	MA
Desastres naturales	Centro de datos UIO 1 Y 2.			Posibilidad de que los desastres naturales (excluyendo los incendios e inundaciones) acaben con los recursos del Sistema.		100%	MB	EX	MA	NO	DE	100%	MB	EX	MA

3.1.10.1.1. INFORME DEL IMPACTO POTENCIAL Y RESIDUAL POR DESASTRES DE ORIGEN NATURAL

En el grafico se puede ver la diferencia entre el impacto potencial y residual debido a la eficacia de las salvaguardas implementadas en el activo. El impacto tiene mayor diferencia en la amenaza Fuego, debido a que la eficacia de la salvaguarda es alta. En la amenaza Daños por agua, la eficacia de la salvaguarda es MB, por lo que el Impacto Residual sigue siendo alto.

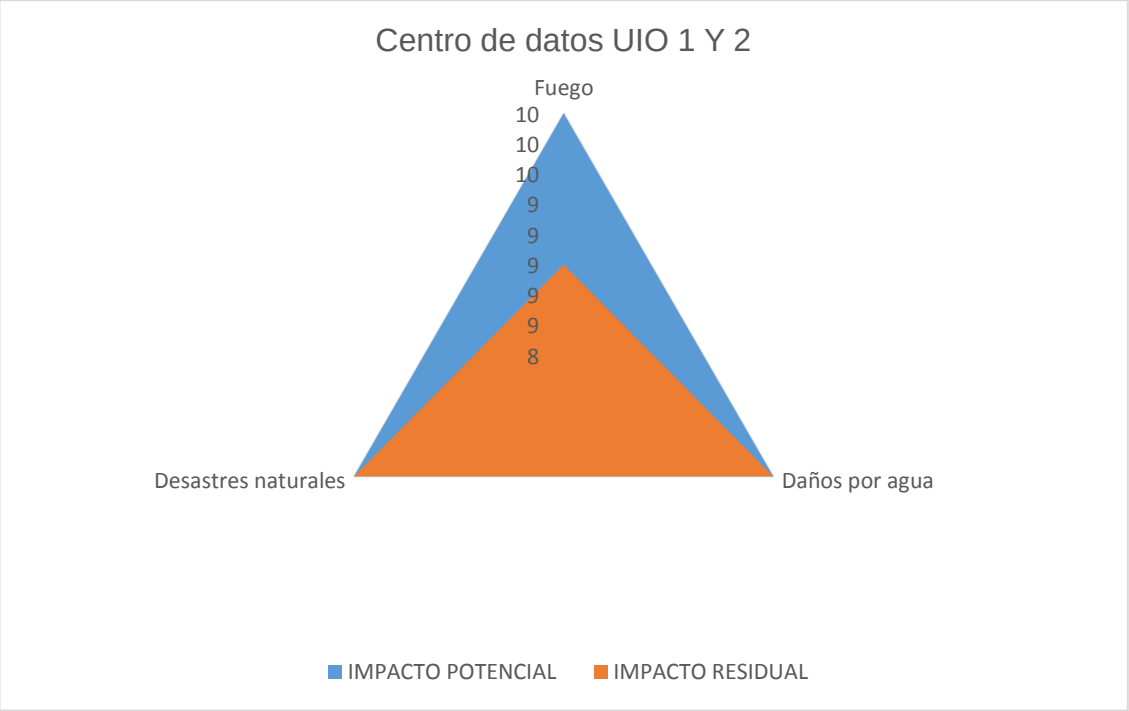

Figura 29. Estimación de Impacto por Desastres Naturales

3.1.10.1.2. INFORME DEL RIESGO POTENCIAL Y RESIDUAL POR DESASTRES DE ORIGEN NATURAL

En el grafico se puede ver la diferencia entre el riesgo potencial y riesgo residual debido a la eficacia de las salvaguardas implementadas en el activo. Hay una diferencia mayor en la amenaza Fuego, ya que la eficacia de la salvaguarda es alta. En la amenaza Daños por agua, la eficacia de la salvaguarda es muy baja, por lo que el Riesgo Residual sigue siendo alto.

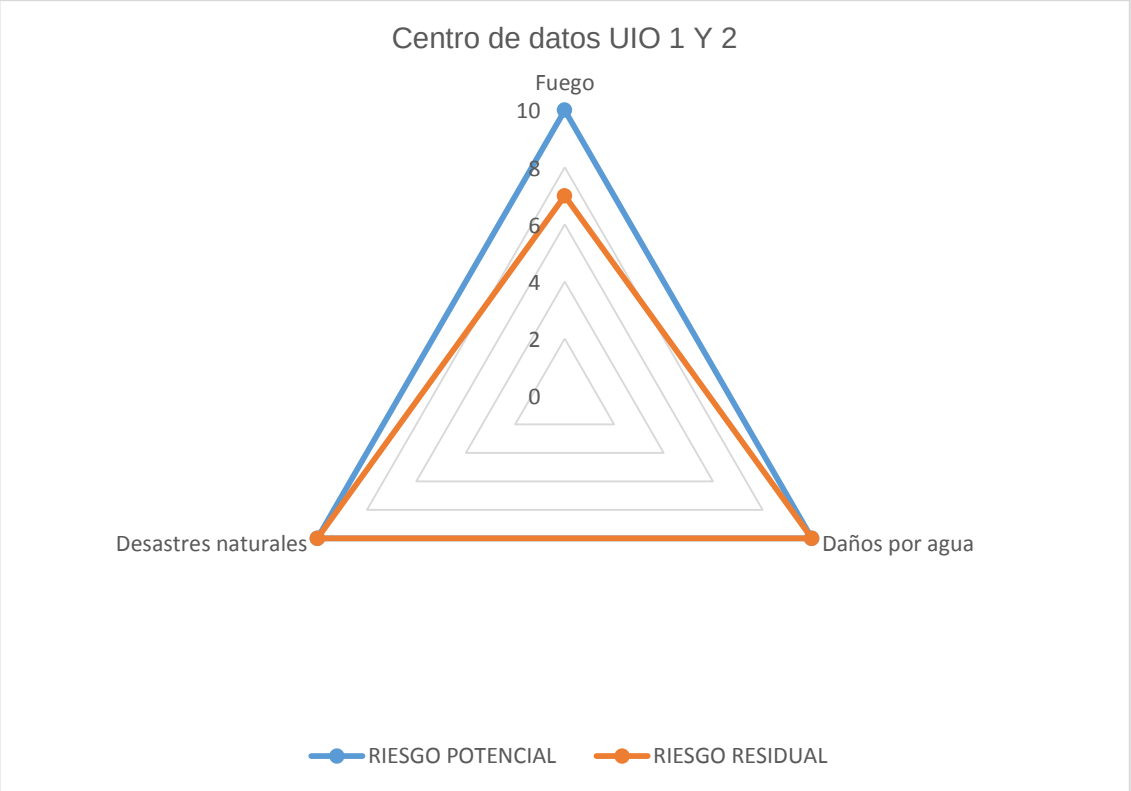

Figura 30. Estimación del Riesgo por Desastres Naturales

3.1.10.2. ESTIMACION DEL ESTADO DE RIESGO POR DESASTRES DE ORIGEN INDUSTRIAL.

Tabla 54.

Análisis de Estimación del Riesgo por Desastres de Origen Industrial

AMENAZA	ACTIVO	VALORACION DEL ACTIVO	TIPO DE ACTIVO	EFECTO DE LA AMENAZA	DIMENSIONES AFECTADAS	DEGRADACION DEL VALOR DEL ACTIVO	PROBABILIDAD DE OCURRENCIA DE LA AMENAZA	IMPACTO POTENCIAL	RIESGO POTENCIAL	SALVAGUARDA IMPLEMENTADA	EFICACIA DE LA SALVAGUARDA	DEGRADACION RESIDUAL	PROBABILIDAD RESIDUAL	IMPACTO RESIDUAL	RIESGO RESIDUAL
Fuego	Centro de datos UIO 1 y 2.	EX	[HW]	Posibilidad de que el fuego acabe con los recursos del Sistema ya sea de manera accidental o deliberada.	1. [D] disponibilidad	100%	MB	EX	MA	SI	M	40%	MB	MA	A
Daños por agua	Centro de datos UIO 1 y 2.	EX	[HW]	Posibilidad de que el agua acabe con los recursos del Sistema ya sea de manera accidental o deliberada.		100%	MB	EX	MA	SI	MB	80%	MB	EX	MA
Desastres industriales	Centro de datos UIO 1 y 2.	EX	[HW]	Posibilidad de que otros desastres debidos a la actividad humana: Explosiones, derrumbes, sobrecarga eléctrica, fluctuaciones eléctricas, accidentes de tráfico, acabe con los recursos del sistema.		100%	MB	EX	MA	SI	B	60%	MB	EX	MA

Tabla 55.

Análisis de Estimación del Riesgo por Desastres de Origen Industrial

AMENAZA	ACTIVO	VALORACION DEL ACTIVO	TIPO DE ACTIVO	EFECTO DE LA AMENAZA	DIMENSIONES AFECTADAS	DEGRADACION DEL VALOR DEL ACTIVO	PROBABILIDAD DE OCURRENCIA DE LA AMENAZA	IMPACTO POTENCIAL	RIESGO POTENCIAL	SALVAGUARDA IMPLEMENTADA	EFICACIA DE LA SALVAGUARDA	DEGRADACION RESIDUAL	PROBABILIDAD RESIDUAL	IMPACTO RESIDUAL	RIESGO RESIDUAL
Contaminación mecánica	Centro de datos UIO 1 y 2.	EX	[HW]	Posibilidad que por las vibraciones, polvo, suciedad, se acabe con los recursos del sistema.	1. [D] disponibilidad	100%	MB	EX	MA	SI	A	20%	MB	AL	M
Avería de origen físico o lógico	Centro de datos UIO 1 y 2.	EX	[HW]	Fallos en los equipos. Puede ser debido a un defecto de origen o sobrevenida durante el funcionamiento del sistema, esto puede acabar con los recursos del sistema.		100%	MB	EX	MA	SI	A	20%	MB	AL	M
Corte del suministro eléctrico	Centro de datos UIO 1 y 2.	EX	[HW]	El cese de energía, indisponibiliza el servicio.		100%	MB	EX	MA	SI	MA	0%	MB	DE	MB

Tabla 56.

Análisis de Estimación del Riesgo por Desastres de Origen Industrial

AMENAZA	ACTIVO	VALORACION DEL ACTIVO	TIPO DE ACTIVO	EFECTO DE LA AMENAZA	DIMENSIONES AFECTADAS	DEGRADACION DEL VALOR DEL ACTIVO	PROBABILIDAD DE OCURRENCIA DE LA AMENAZA	IMPACTO POTENCIAL	RIESGO POTENCIAL	SALVAGUARDA IMPLEMENTADA	EFICACIA DE LA SALVAGUARDA	DEGRADACION RESIDUAL	PROBABILIDAD RESIDUAL	IMPACTO RESIDUAL	RIESGO RESIDUAL
Condiciones inadecuadas de temperatura o humedad	Centro de datos UIO 1 y 2.	EX	[HW]	Deficiencias en la aclimatación de los locales, excediendo los márgenes de trabajo de los equipos: excesivo calor, excesivo frío, exceso de humedad pueden acabar con los recursos del sistema.	1. [D] disponibilidad	60%	MB	MA	MA	SI	M	20%	MB	AL	M
Fallo de servicios de comunicaciones	Centro de datos UIO2.	EX	[COM]	Pérdida de los Medios de telecomunicación.		60%	MB	EX	MA	NO	DE	60%	MB	EX	MA
Degradación de los soportes de almacenamiento de la información	Centro de datos UIO 1.	EX	[HW]	No se puede restaurar la Bases de Datos.		100%	MB	EX	MA	NO	DE	100%	MB	EX	MA

3.1.10.2.1. INFORME DEL IMPACTO POTENCIAL Y RESIDUAL POR DESASTRES DE ORIGEN INDUSTRIAL

En el Grafico se muestra la diferencia entre Impacto Potencial y residual en función de la eficacia de la salvaguarda.

En las Amenazas:

- Fallo de servicios de comunicaciones
- Degradación de los soportes de almacenamiento de la información
- Daños por agua

Que no tienen implementada una salvaguarda, el punto del Impacto Potencial y el Impacto Residual es el mismo

Las amenazas:

- Condiciones inadecuadas de temperatura o humedad
- Contaminación mecánica
- Avería de origen físico o lógico
- Fuego

Que tienen implementadas salvaguardas aunque no eficaces al 100%, el Impacto Residual es menor con respecto al Impacto Potencial.

En el caso de la amenaza:

- Corte de Suministro Eléctrico, tiene una salvaguarda 100% Eficaz por tal razón el Impacto es Despreciable

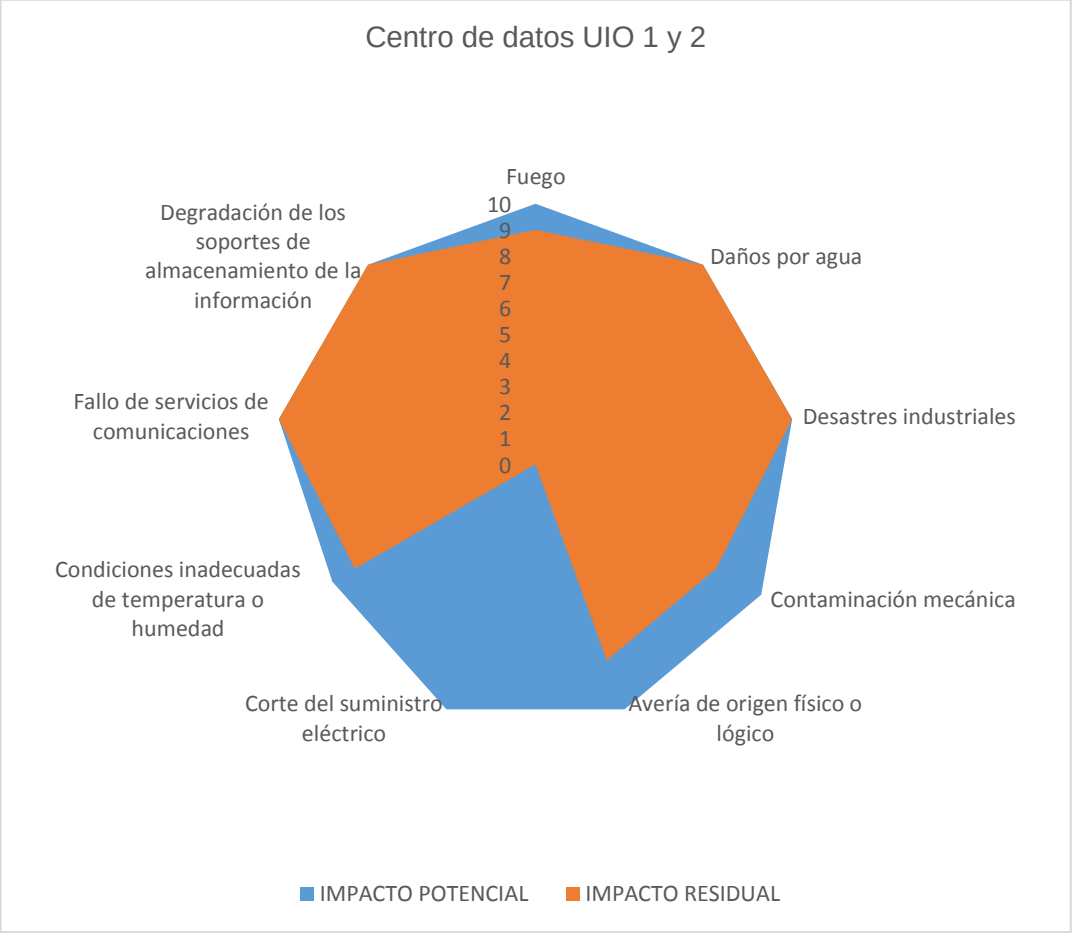

Figura 31. Estimación de Impacto por Desastres de Origen Industrial

3.1.10.2.2. INFORME DEL RIESGO POTENCIAL Y RESIDUAL POR DESASTRES DE ORIGEN INDUSTRIAL

En el Grafico se muestra la diferencia entre Riesgo Potencial y residual en función de la eficacia de la salvaguarda.

En las Amenazas:

- Fallo de servicios de comunicaciones
- Degradación de los soportes de almacenamiento de la información
- Daños por agua

Que no tienen implementada una salvaguarda, el punto del Impacto Potencial y el Impacto Residual es el mismo, por tanto el Riesgo Potencial y Residual esta también el mismo

Las amenazas:

- Condiciones inadecuadas de temperatura o humedad
- Contaminación mecánica
- Avería de origen físico o lógico
- Fuego

Que tienen implementadas salvaguardas aunque no eficaces al 100%, el Impacto Residual es menor con respecto al Impacto Potencial, por tanto el Riesgo Residual también es menor con respecto al Riesgo Potencial.

En el caso de la amenaza

Corte de Suministro Eléctrico, tiene una salvaguarda 100% Eficaz por tal razón el Impacto Residual es Despreciable al igual que el Riesgo Residual, como se puede ver en el gráfico:

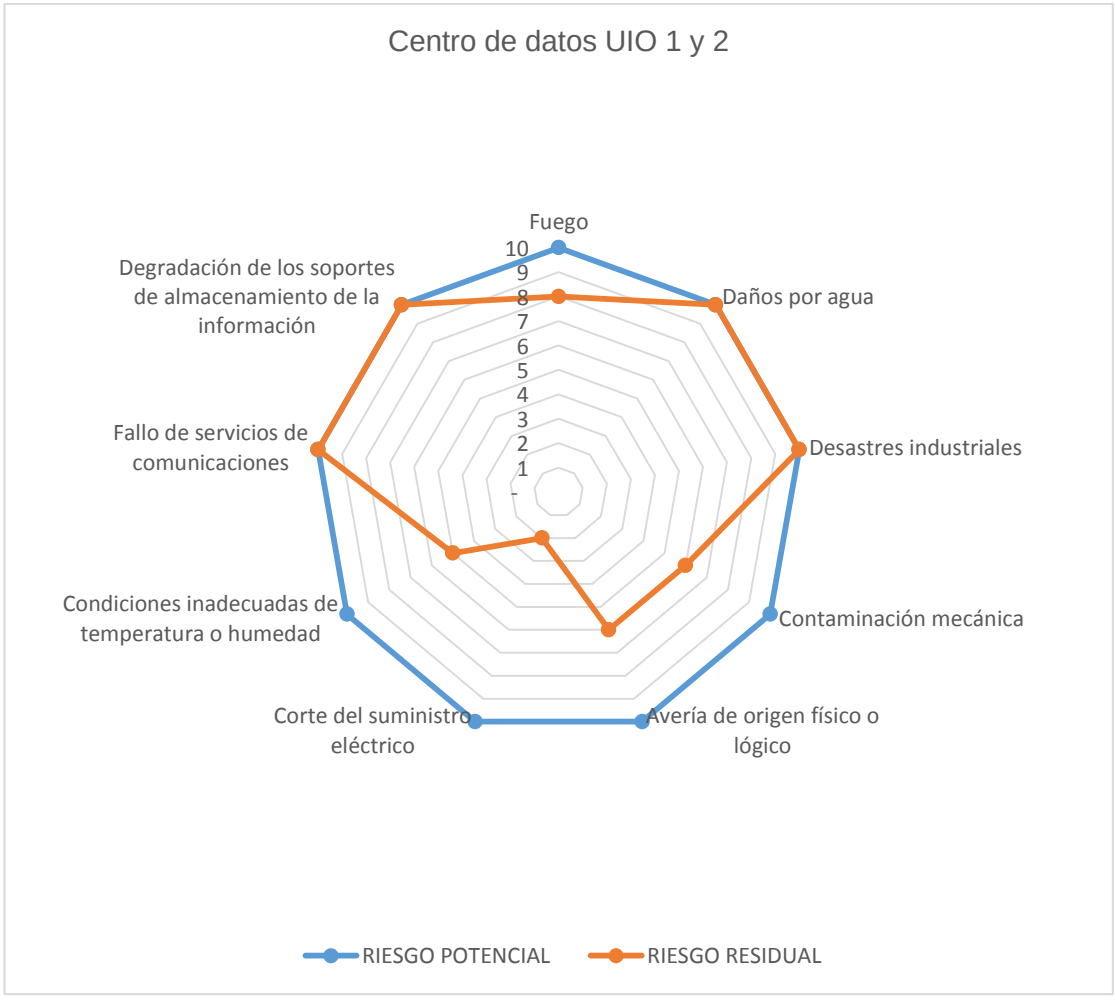

Figura 32. Estimación del Riesgo por Desastres de Origen Industrial

3.1.10.3. ESTIMACION DEL ESTADO DE RIESGO POR ERRORES Y FALLOS NO INTENCIONADOS

Tabla 57.

Análisis de Estimación del Riesgo por Errores y Fallos Intencionados

AMENAZA	ACTIVO	VALORACION DEL ACTIVO	TIPO DE ACTIVO	EFECTO DE LA AMENAZA	DIMENSIONES AFECTADAS	DEGRADACION DEL VALOR DEL ACTIVO	PROBABILIDAD DE OCURRENCIA DE LA AMENAZA	IMPACTO POTENCIAL	RIESGO POTENCIAL	SALVAGUARDA IMPLEMENTADA	EFICACIA DE LA SALVAGUARDA	DEGRADACION RESIDUAL	PROBABILIDAD RESIDUAL	IMPACTO RESIDUAL	RIESGO RESIDUAL
Errores de los usuarios	Clientes	**EX**	[D]	Nombres y apellidos incompletos, ruc incorrecto. Colocar al cliente en un canal incorrecto.	1. [I] integridad 2. [C] confidencialidad 3. [D] disponibilidad	60%	M	EX	MA	SI	MB	40%	M	MA	MA
	Ortes	AL	[D]	Vehículo equivocado. Descripción incorrecta o incompleta el estado del vehículo. Detalle incorrecto de los documentos o herramientas que deja el cliente en el vehículo.	1. [I] integridad 2. [C] confidencialidad 3. [D] disponibilidad	100%	A	AL	MA	SI	MB	80%	A	AL	MA
	Órdenes de trabajo.	AL	[D]	Escoger mal el tipo de movimiento, artículo o línea de negocio. No seleccionar quien cancela. Generar mal los valores de quien cancela.	1. [I] integridad 2. [C] confidencialidad 3. [D] disponibilidad	100%	M	AL	A	SI	MB	80%	M	AL	A

Tabla 58.

Análisis de Estimación del Riesgo por Errores y Fallos no Intencionados

AMENAZA	ACTIVO	VALORACION DEL ACTIVO	TIPO DE ACTIVO	EFECTO DE LA AMENAZA	DIMENSIONES AFECTADAS	DEGRADACION DEL VALOR DEL ACTIVO	PROBABILIDAD DE OCURRENCIA DE LA AMENAZA	IMPACTO POTENCIAL	RIESGO POTENCIAL	SALVAGUARDA IMPLEMENTADA	EFICACIA DE LA SALVAGUARDA	DEGRADACION RESIDUAL	PROBABILIDAD RESIDUAL	IMPACTO RESIDUAL	RIESGO RESIDUAL
Errores de los usuarios	Órdenes de monitoreo.	AL	[D]	Seleccionar servicios incorrectos.	1. [I] integridad 2. [C] confidencialidad 3. [D] disponibilidad	20%	MA	BA	M	SI	MB	1%	MA	DE	B
	Contratos.	AL	[D]	Colocar mal la fecha de vigencia del contrato. Seleccionar mal los servicios.	1. [I] integridad 2. [C] confidencialidad 3. [D] disponibilidad	20%	M	BA	B	SI	MB	1%	M	DE	MB
	Facturación.	AL	[D]	Colocar mal el número de factura. Distribuir mal los valores a ser recaudados con el nombre equivocado.	1. [I] integridad 2. [C] confidencialidad 3. [D] disponibilidad	20%	B	BA	B	SI	MB	1%	B	DE	MB

3.1.10.3.1. INFORME DEL IMPACTO POTENCIAL Y RESIDUAL POR ERRORES DE LOS USUARIOS

En el grafico se puede notar que el Impacto Residual baja a 0 en los activos Ordenes de Monitoreo, Contratos y Facturación, debido a la eficacia de las Salvaguardas.

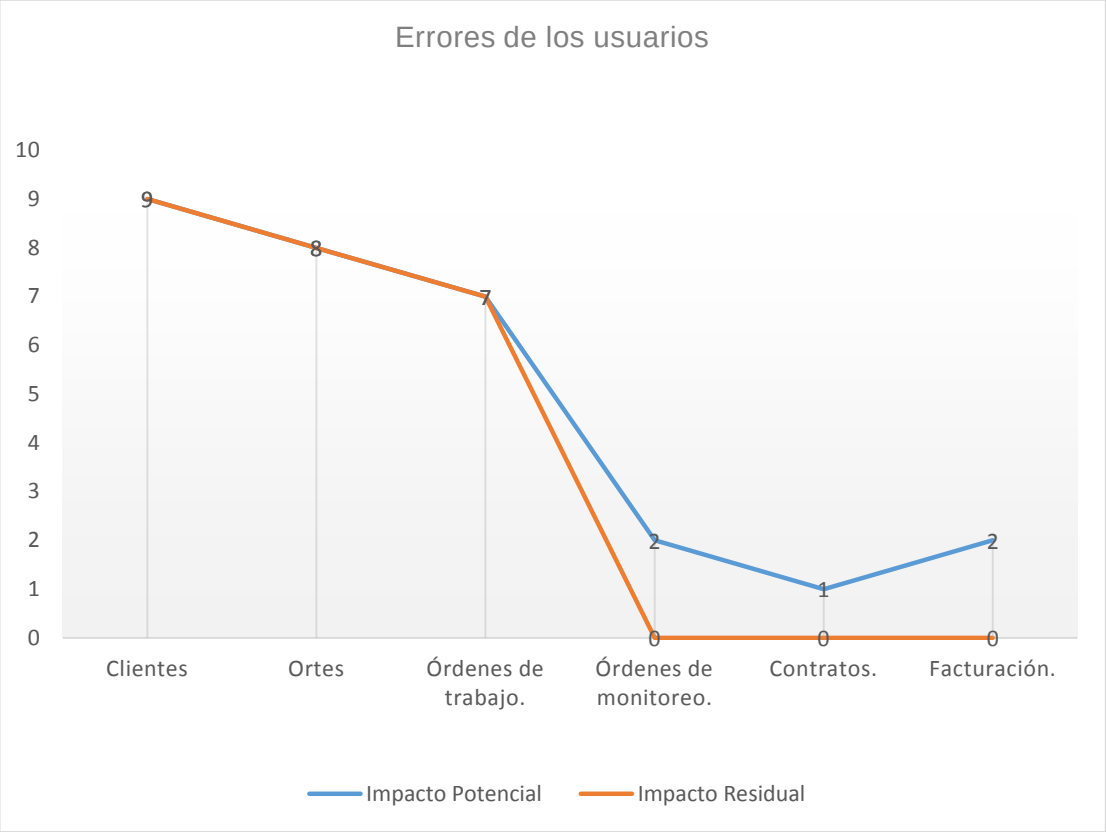

Figura 33. Estimación del Impacto por Errores de los Usuarios

3.1.10.3.2. INFORME DEL RIESGO POTENCIAL Y RESIDUAL POR ERRORES DE LOS USUARIOS

En el grafico se puede notar que el Riesgo Residual baja en los activos Ordenes de Monitoreo, Contratos y Facturación, debido a la eficacia de las Salvaguardas.

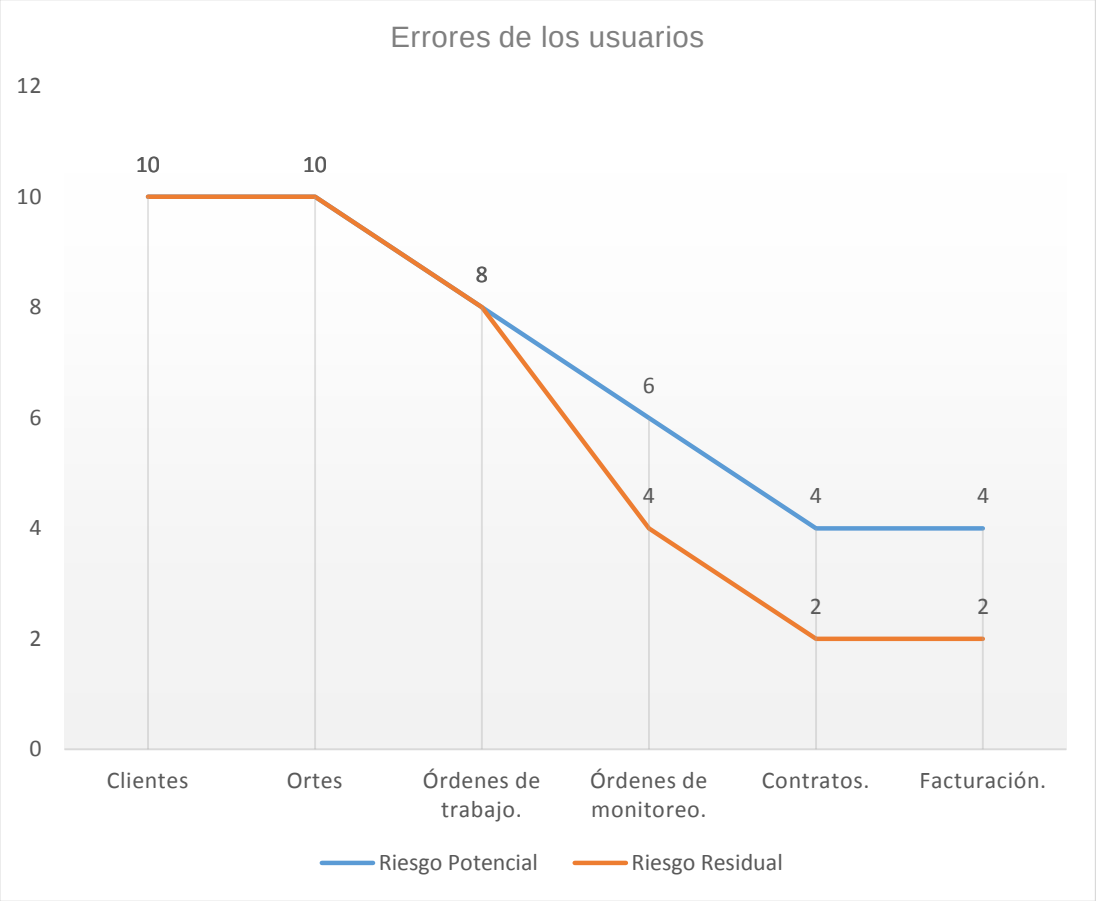

Figura 34. Estimación del Riesgo por Errores de los Usuarios

Tabla 59.

Análisis de Estimación del Riesgo por Errores y Fallos no Intencionados

AMENAZA	ACTIVO	VALORACION DEL ACTIVO	TIPO DE ACTIVO	EFECTO DE LA AMENAZA	DIMENSIONES AFECTADAS	DEGRADACION DEL VALOR DEL ACTIVO	PROBABILIDAD DE OCURRENCIA DE LA AMENAZA	IMPACTO POTENCIAL	RIESGO POTENCIAL	SALVAGUARDA IMPLEMENTADA	EFICACIA DE LA SALVAGUARDA	DEGRADACION RESIDUAL	PROBABILIDAD RESIDUAL	IMPACTO RESIDUAL	RIESGO RESIDUAL
Errores del administrador	Sistema de administración y seguridades.	EX	[SW]	Aplicaciones no confiables por parte de quienes administran. Colocar un usuario dentro de un perfil equivocado. Dar autorizaciones de acceso a usuarios incorrectos.	1. [D] disponibilidad 2. [I] integridad 3. [C] confidencialidad	100%	A	EX	MA	NO	DE	100%	A	EX	MA
Errores de monitorización (log)	Clientes	EX	[D.log]	El inadecuado registro de actividades: falta de registros, registros incompletos, registros incorrectamente fechados, etc., ocasionan tener desconocimiento de las transacciones realizadas en los servidores Nombres y apellidos incompletos. Ruc incorrecto. Colocar al cliente en un canal incorrecto. Vehículo equivocado.	1. [I] integridad 1. [A] autenticidad	60%	A	EX	MA	NO	DE	60%	A	EX	MA

Tabla 60.

Análisis de Estimación del Riesgo por Errores y Fallos no Intencionados

AMENAZA	ACTIVO	VALORACION DEL ACTIVO	TIPO DE ACTIVO	EFECTO DE LA AMENAZA	DIMENSIONES AFECTADAS	DEGRADACION DEL VALOR DEL ACTIVO	DE OCURRENCIA DE LA	IMPACTO POTENCIAL	RIESGO POTENCIAL	SALVAGUARDA IMPLEMENTADA	EFICACIA DE LA SALVAGUARDA	DEGRADACION RESIDUAL	PROBABILIDAD RESIDUAL	IMPACTO RESIDUAL	RIESGO RESIDUAL
Errores de configuración	Contratos	AL	[D.conf]	La configuración mal realizada hace que las aplicaciones funcionan de manera errónea provocando pérdida de los datos relevantes del negocio Error en la plantilla de los contratos.	1. [C] confidencialidad	100%	MA	AL	MA	NO	DE	100%	MA	AL	MA
	Transacciones contables.	EX	[D]	Plantilla contable con errores.	1. [C] confidencialidad	100%	A	EX	MA	NO	DE	100%	A	EX	MA
	Sistema Administrativo Financiero. Sistema Administración Tributaria.			Las aplicaciones no podrían funcionar correctamente y de esta manera queda ineficiente la atención al cliente.											
Difusión de software dañino	Sistema de activos fijos. Sistema de gestión humana Sistema de evaluaciones Sistema de administración de clientes Accouting Interfase Sistema de administración de seguridades Posfix CIFS Sistema de control de mensajes. Sistema de análisis de mensajes	AL	[SW]	Enviar virus, espías (spyware), gusanos, troyanos, bombas lógicas, etc., a las aplicaciones sin intención.	1. [I] integridad 1. [C] confidencialidad 1. [D] disponibilidad	100%	MA	AL	MA	SI	A	20%	B	BA	B

3.1.10.3.3. INFORME DEL IMPACTO POTENCIAL Y RESIDUAL POR ERRORES Y FALLOS NO INTENCIONADOS

Para las amenazas Errores del administrador, Errores de monitorización (log) y Errores de configuración, que afectan a los activos: Sistema de administración y seguridades, Clientes, Contratos y Transacciones contables, no existe una salvaguarda implementada, por lo que en grafico que puede ver que el Punto del Impacto Potencial y el Impacto Residual es el mismo.

Para la amenaza Difusión de software dañino que afecta a los activos:

Sistema Administrativo Financiero, Sistema Administración Tributaria, Sistema de activos fijos, Sistema de gestión humana, Sistema de evaluaciones, Sistema de administración de clientes, Accouting Interfase, Sistema de administración de seguridades, Posfix, CIFS, Sistema de control de mensajes, Sistema de análisis de mensajes, Existe una salvaguarda implementada altamente eficaz.

Por lo que el impacto para estos activos es Despreciable, como se puede ver en el gráfico:

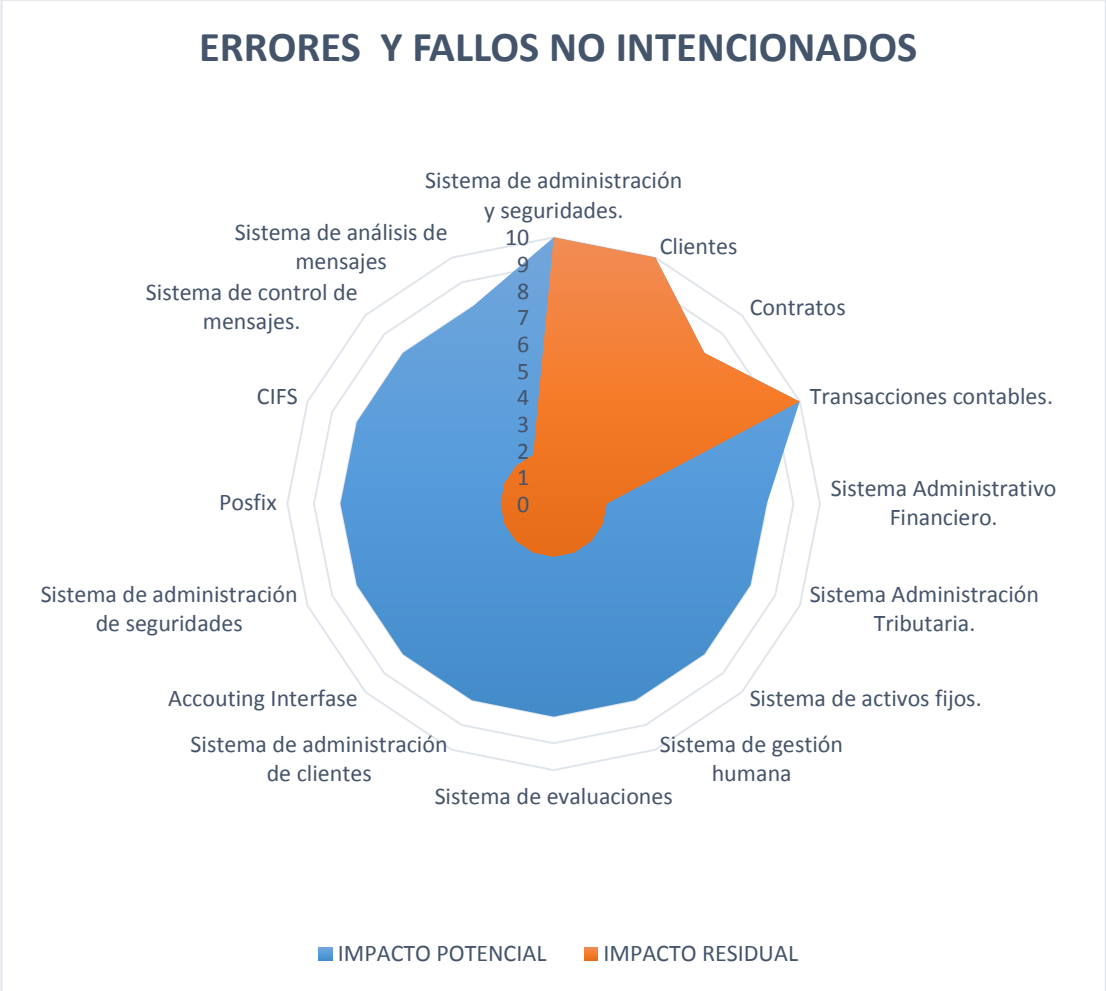

Figura 35. Estimación del Impacto Errores y Fallos No intencionados

3.1.10.3.4. INFORME DEL RIESGO POTENCIAL Y RESIDUAL POR ERRORES Y FALLOS NO INTENCIONADOS

Para las amenazas Errores del administrador, Errores de monitorización (log) y Errores de configuración, que afectan a los activos: Sistema de administración y seguridades, Clientes, Contratos y Transacciones contables, no existe una salvaguarda implementada, por lo que en grafico que puede ver que el Punto del Riesgo Potencial y el Riesgo Residual es el mismo.

Para la amenaza Difusión de software dañino que afecta a los activos:

Sistema Administrativo Financiero, Sistema Administración Tributaria, Sistema de activos fijos, Sistema de gestión humana, Sistema de evaluaciones, Sistema de administración de clientes, Accouting Interfase, Sistema de administración de seguridades, Posfix, CIFS, Sistema de control de mensajes, Sistema de análisis de mensajes, Existe una salvaguarda implementada altamente eficaz.

Por lo que el Riesgo para estos activos es Despreciable, como se puede ver en el gráfico:

Figura 36. Estimación del Riesgo por Errores y Fallos No intencionados

Tabla 61.

Análisis de Estimación del Riesgo por Errores y Fallos no Intencionados

AMENAZA	ACTIVO	VALORACION DEL ACTIVO	TIPO DE ACTIVO	EFECTO DE LA AMENAZA	DIMENSIONES AFECTADAS	DEGRADACION DEL VALOR DEL ACTIVO	PROBABILIDAD DE OCURRENCIA DE LA AMENAZA	IMPACTO POTENCIAL	RIESGO POTENCIAL	SALVAGUARDA IMPLEMENTADA	EFICACIA DE LA SALVAGUARDA	DEGRADACION RESIDUAL	PROBABILIDAD RESIDUAL	IMPACTO RESIDUAL	RIESGO RESIDUAL
Errores de secuencia	Correo corporativo	AL	[SW]	Alteración accidental del orden de los mensajes transmitidos Enviar mails sin tomar en cuenta el orden de prioridad.	1. [I] integridad	60%	A	AL	MA	NO	DE	60%	A	AL	MA
Alteración accidental de la información	BddConta (SqlServer 2000) BddTrib (SqlServer 2000) BddAcf (Dbase II) BddRrhh MySQL (5.5.23) Remote Desktop BddEval (SQLServer 2005) BddCall1 (Mysql 5.0.77) BddCall2 (Mysql5.0.77) BddCrm (Mysql 5.5.23) BddCrm (Mysql 5.1.27) BddCrm (Mysql 5.5.14) BddExtranet(SQLServer 2005)	EX	[SW]	Alterar accidentalmente la información genera Información incorrecta,	1. [I] integridad	100%	M	EX	MA	SI	B	60%	B	EX	MA

Tabla 62.

Análisis de Estimación del Riesgo por Errores y Fallos no Intencionados

AMENAZA	ACTIVO	VALORACION DEL ACTIVO	TIPO DE ACTIVO	EFECTO DE LA AMENAZA	DIMENSIONES AFECTADAS	DEGRADACION DEL VALOR DEL ACTIVO	PROBABILIDAD DE OCURRENCIA DE LA AMENAZA	IMPACTO POTENCIAL	RIESGO POTENCIAL	SALVAGUARDA IMPLEMENTADA	EFICACIA DE LA SALVAGUARDA	DEGRADACION RESIDUAL	PROBABILIDAD RESIDUAL	IMPACTO RESIDUAL	RIESGO RESIDUAL
Destrucción de información	BddConta (SqlServer 2000) BddTrib (SqlServer 2000) BddAcf (Dbase II) BddRrhh MySQL (5.5.23) Remote Desktop BddEval (SQLServer 2005) BddCall1 (Mysql 5.0.77) BddCall2 (Mysql5.0.77) BddCrm (Mysql 5.5.23) BddCrm (Mysql 5.1.27) BddCrm (Mysql 5.5.14) BddExtranet(SQLServer 2005)	EX	[SW]	Bases de datos sin información o incompletas. Eliminar accidentalmente la información, con ánimo de obtener un beneficio personal o causar daño.	1. [I] integridad	100%	A	EX	MA	SI	B	60%	B	EX	MA

Tabla 63.

Análisis de Estimación del Riesgo por Errores y Fallos no Intencionados

AMENAZA	ACTIVO	VALORACION DEL ACTIVO	TIPO DE ACTIVO	EFECTO DE LA AMENAZA	DIMENSIONES AFECTADAS	DEGRADACION DEL VALOR DEL ACTIVO	PROBABILIDAD DE OCURRENCIA DE LA AMENAZA	IMPACTO POTENCIAL	RIESGO POTENCIAL	SALVAGUARDA IMPLEMENTADA	EFICACIA DE LA SALVAGUARDA	DEGRADACION RESIDUAL	PROBABILIDAD RESIDUAL	IMPACTO RESIDUAL	RIESGO RESIDUAL
Fugas de información	Cartera clientes Información del personal. Usuarios y perfiles Menús y opciones	EX	[D]	Conversaciones acerca de la información de la compañía. Falsificación de datos del cliente. Falsificación de datos del personal. Falsificación de usuarios y claves. Acceso al sistema a personas que no son parte del personal de la empresa.	1. [I] integridad	60%	MA	MA	MA	SI	MB	40%	A	MA	MA
Vulnerabilidades de los programas (software)	Sistema de administración de los clientes.	EX	[SW]	Defectos en el código al momento de programar. Programas con mal funcionamiento	1. [I] integridad 2. [D] disponibilidad 3. [C] confidencialidad	100%	MA	EX	MA	NO	DE	100%	MA	EX	MA

Tabla 64.

Análisis de Estimación del Riesgo por Errores y Fallos no Intencionados

AMENAZA	ACTIVO	VALORACION DEL ACTIVO	TIPO DE ACTIVO	EFECTO DE LA AMENAZA	DIMENSIONES AFECTADAS	DEGRADACION DEL VALOR DEL ACTIVO	PROBABILIDAD DE OCURRENCIA DE LA AMENAZA	IMPACTO POTENCIAL	RIESGO POTENCIAL	SALVAGUARDA IMPLEMENTADA	EFICACIA DE LA SALVAGUARDA	DEGRADACION RESIDUAL	PROBABILIDAD RESIDUAL	IMPACTO RESIDUAL	RIESGO RESIDUAL
Errores de mantenimiento / actualización de programas (software)	Sistema de administración de los clientes. Sistema de administración de seguridades. Posfix CIFS Sistema de administración tributaria.	EX	[SW]	Falla del funcionamiento de las aplicaciones debido a que las mismas tenían defectos. Carencia de recursos suficientes provoca la caída del sistema cuando la carga de trabajo es desmesurada	1. [C] confidencialidad 2. [I] integridad	100%	A	EX	MA	NO	DE	100%	A	EX	MA
Caída del sistema por agotamiento de recursos	Clientes Solicitudes y seguimiento Proformas Citas o Turnos Órdenes de trabajo Órdenes de monitoreo. Contratos. Facturación. Comisiones.	EX	[SW]	Saturación del sistema informático. Carencia de un medio para prestar los servicios.	1. [I] integridad	60%	M	EX	MA	NO	DE	60%	M	EX	MA
Pérdida de equipos	Rack 1I	AL	[HW]	Carencia de un medio para prestar los servicios.	1. [I] integridad	100%	M	AL	A	NO	DE	100%	M	AL	A

3.1.10.3.5. INFORME DEL IMPACTO POTENCIAL Y RESIDUAL POR ERRORES Y FALLOS NO INTENCIONADOS.

Los activos que no tienen salvaguardas ante las amenazas:

Errores de secuencia, que afecta al activo: Correo corporativo

Vulnerabilidades de los programas (software), que afecta al activo: Sistema de administración de los clientes.

Errores de mantenimiento / actualización de programas (software), que afecta los activos: Sistema de administración de los clientes, Sistema de administración de seguridades, Posfix, CIFS, Sistema de administración tributaria.

Caída del sistema por agotamiento de recursos, que afecta los activos: Clientes, Solicitudes y seguimiento, Proformas, Citas o Turnos, Órdenes de trabajo, Órdenes de monitoreo, Contratos, Facturación, Comisiones.

Y Pérdida de equipos, que afecta al activo: Rack 1I

El IMPACTO Potencial y Residual es el mismo.

En las amenazas que tienen salvaguardas implementadas, pero su eficacia es muy baja, el Impacto Potencial y Residual sigue siendo el mismo.

Estas amenazas son:

Alteración accidental de la información, que afecta al activo: Bases de Datos SQL y Dbase.

Destrucción de información, que afecta al activo: Bases de Datos SQL y Dbase

Fugas de información, que afecta al activo: Cartera clientes, Información del personal, Usuarios y perfiles, Menús y opciones

En el grafico se muestra El Impacto Potencial y el Impacto Residual son iguales en todos los activos afectados por las amenazas mencionadas anteriormente.

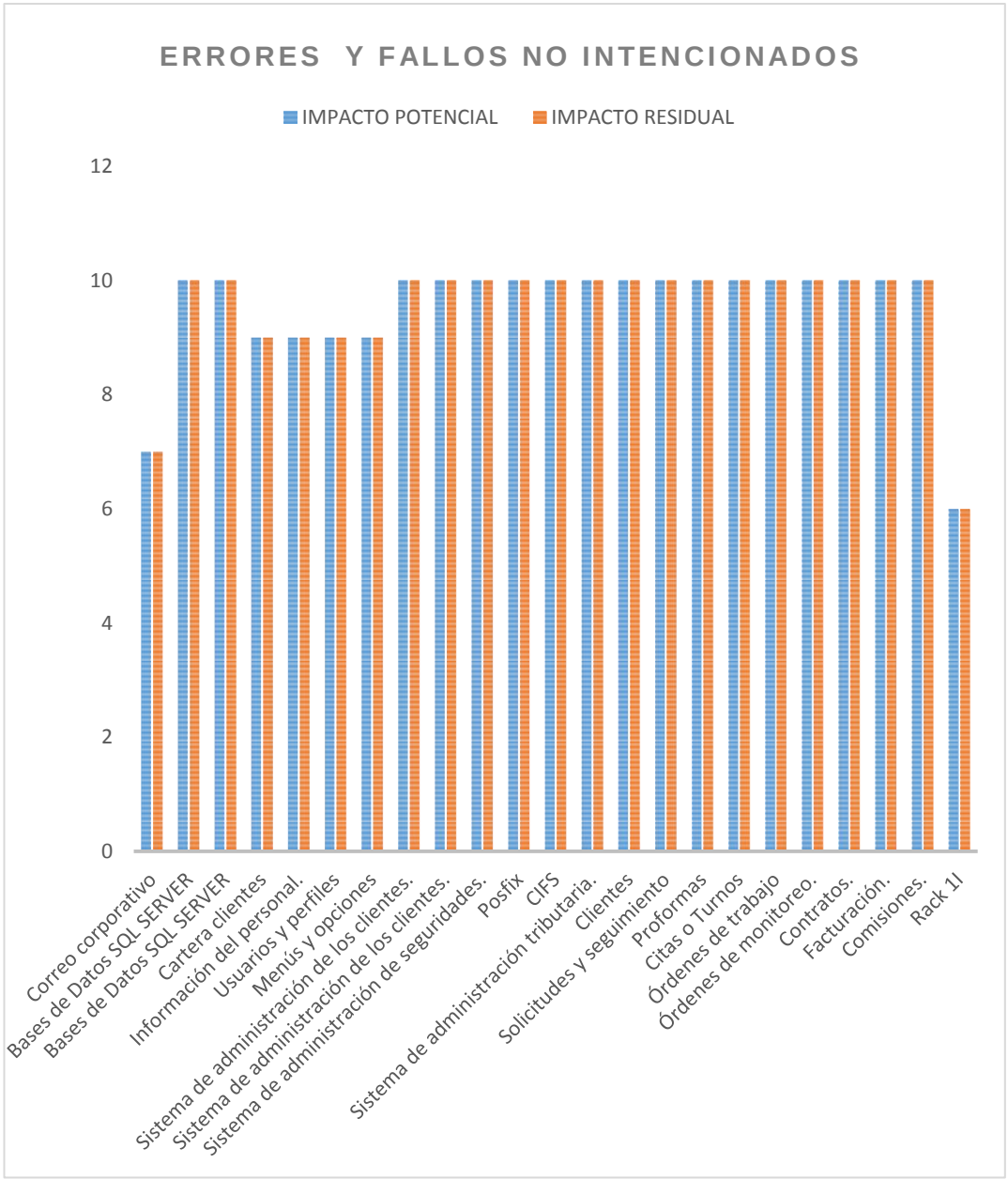

Figura 37. Estimación del Impacto por Errores y Fallos No intencionados

3.1.10.3.6. INFORME DEL IMPACTO POTENCIAL Y RESIDUAL POR ERRORES Y FALLOS NO INTENCIONADOS

Ante las amenazas:

Errores de secuencia, que afecta al activo: Correo corporativo

Vulnerabilidades de los programas (software), que afecta al activo: Sistema de administración de los clientes.

Errores de mantenimiento / actualización de programas (software), que afecta los activos: Sistema de administración de los clientes, Sistema de administración de seguridades, Posfix, CIFS, Sistema de administración tributaria.

Caída del sistema por agotamiento de recursos, que afecta los activos: Clientes, Solicitudes y seguimiento, Proformas, Citas o Turnos, Órdenes de trabajo, Órdenes de monitoreo, Contratos, Facturación, Comisiones.

Y Pérdida de equipos, que afecta al activo: Rack 1I

El RIESGO Potencial y Residual es el mismo, debido a que estos activos no tienen salvaguardas implementadas.

En las amenazas que tienen salvaguardas implementadas, pero su eficacia es muy baja, el Riego Potencial y Residual sigue siendo el mismo.

Estas amenazas son:

Alteración accidental de la información, que afecta al activo: Bases de Datos SQL y Dbase.

Destrucción de información, que afecta al activo: Bases de Datos SQL y Dbase

Fugas de información, que afecta al activo: Cartera clientes, Información del personal, Usuarios y perfiles, Menús y opciones

En el grafico se muestra El Riesgo Potencial y el Riesgo Residual son iguales en todos los activos afectados por las amenazas mencionadas anteriormente.

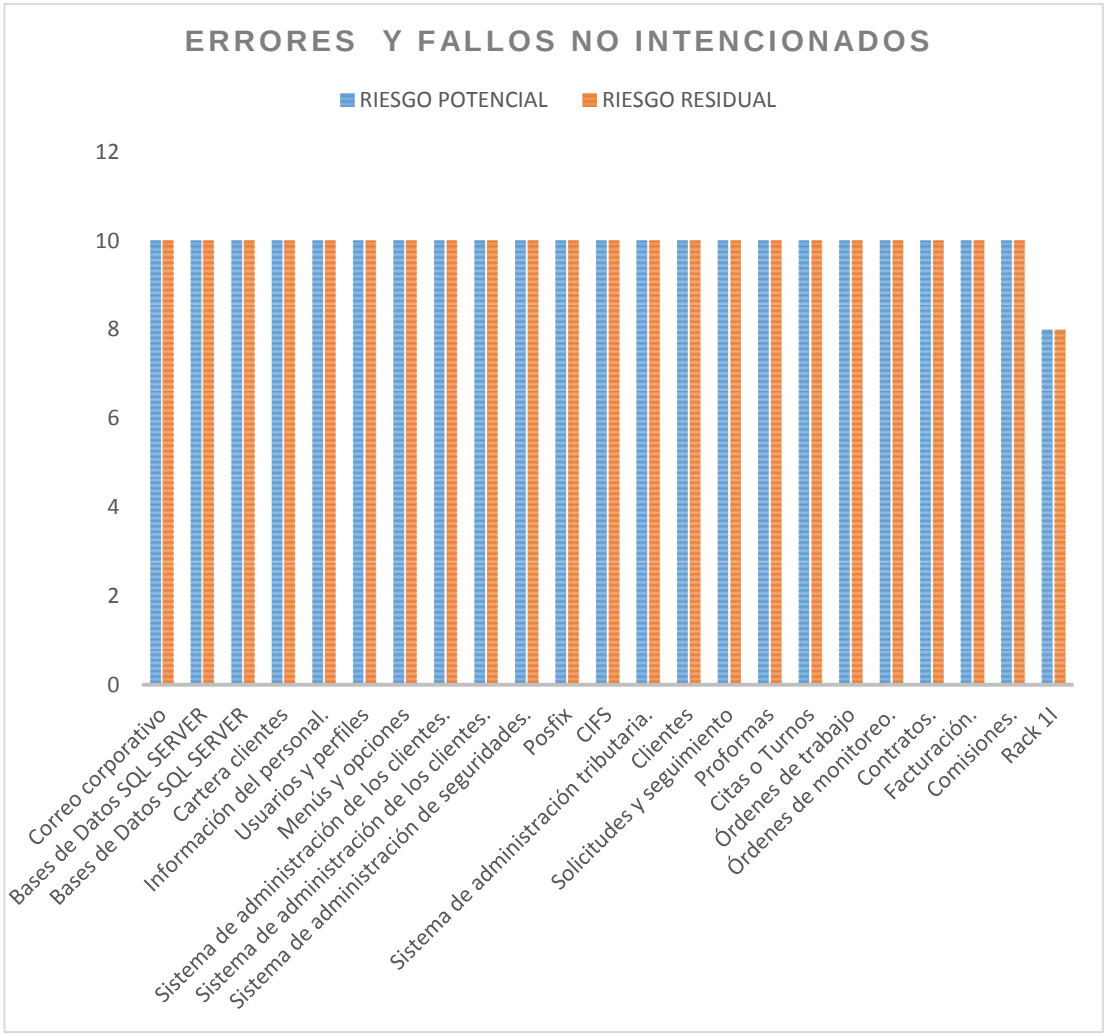

Figura 38. Estimación del Riesgo por Errores y Fallos No intencionados

3.1.10.4. ESTIMACION DEL ESTADO DE RIESGO POR ATAQUES INTENCIONADOS

Tabla 65.

Análisis de Estimación del Riesgo por Ataques Intencionados

AMENAZA	ACTIVO	VALORACION DEL ACTIVO	TIPO DE ACTIVO	EFECTO DE LA AMENAZA	DIMENSIONES AFECTADAS	DEGRADACION DEL VALOR DEL ACTIVO	PROBABILIDAD DE OCURRENCIA DE LA AMENAZA	IMPACTO POTENCIAL	RIESGO POTENCIAL	SALVAGUARDA IMPLEMENTADA	EFICACIA DE LA SALVAGUARDA	DEGRADACION RESIDUAL	PROBABILIDAD RESIDUAL	IMPACTO RESIDUAL	RIESGO RESIDUAL
Manipulación de la configuración	Registro de menús y opciones. Clientes Solicitudes y seguimiento	EX	[D.log]	Configuración incorrecta por parte del administrador. Errores al colocar privilegios de acceso. Información errónea. Los usuarios no autorizados podrían modificar la información a su conveniencia.	1. [I] integridad	100%	MA	EX	MA	NO	DE	100%	MA	EX	MA
Suplantación de la identidad del usuario	Proformas Citas o Turnos Órdenes de trabajo Órdenes de monitoreo. Contratos. Facturación. Comisiones. Ventas.	EX	[D]		1. [I] integridad 2. [C] confidencialidad 3. [A] autenticidad	100%	A	EX	MA	SI	MB	80%	M	EX	MA

Tabla 66.

Análisis de Estimación del Riesgo por Ataques Intencionados

AMENAZA	ACTIVO	VALORACION DEL ACTIVO	TIPO DE ACTIVO	EFECTO DE LA AMENAZA	DIMENSIONES AFECTADAS	DEGRADACION DEL VALOR DEL ACTIVO	PROBABILIDAD DE OCURRENCIA DE LA AMENAZA	IMPACTO POTENCIAL	RIESGO POTENCIAL	SALVAGUARDA IMPLEMENTADA	EFICACIA DE LA SALVAGUARDA	DEGRADACION RESIDUAL	PROBABILIDAD RESIDUAL	IMPACTO RESIDUAL	RIESGO RESIDUAL
Abuso de privilegios de acceso	Clientes Solicitudes y seguimiento Proformas Citas o Turnos Órdenes de trabajo Órdenes de monitoreo. Contratos. Facturación. Comisiones. Ventas.	EX	[D]	Al tener la información errónea podrían llegar a surgir problemas de integridad. Los usuarios podrían crear, modificar y eliminar la información dependiendo de los privilegios que tengan.	1. [C] confidencialidad 2. [I] integridad 3. [D] disponibilidad	100%	M	EX	MA	SI	MB	80%	B	EX	MA
Uso no previsto	Clientes Solicitudes y seguimiento Proformas Citas o Turnos Órdenes de trabajo Órdenes de monitoreo. Contratos. Facturación. Comisiones. Ventas.	EX	[S]	Utilización de los recursos del sistema para fines no previstos, es decir, típicamente de interés personal. Usar los recursos del sistema para juegos, consultas personales, programas personales, etc. Y esto a su vez podrían ser causantes de un servicio incompetente.	1. [D] disponibilidad 2. [C] confidencialidad 3. [I] integridad	60%	M	EX	MA	SI	MA	0%	DE	BA	MB

Tabla 67.

Análisis de Estimación del Riesgo por Ataques Intencionados

AMENAZA	ACTIVO	VALORACION DEL ACTIVO	TIPO DE ACTIVO	EFECTO DE LA AMENAZA	DIMENSIONES AFECTADAS	DEGRADACION DEL VALOR DEL ACTIVO	PROBABILIDAD DE OCURRENCIA DE LA AMENAZA	IMPACTO POTENCIAL	RIESGO POTENCIAL	SALVAGUARDA IMPLEMENTADA	EFICACIA DE LA SALVAGUARDA	DEGRADACION RESIDUAL	PROBABILIDAD RESIDUAL	IMPACTO RESIDUAL	RIESGO RESIDUAL
Alteración de secuencia	Correo corporativo	AL	[S]	Alteración intencional del orden de los mensajes transmitidos. Enviar mails incorrectos con la intención de causar problemas.	1. [I] integridad	60%	A	AL	MA	NO	DE	60%	A	AL	MA
Acceso no autorizado	Clientes Solicitudes y seguimiento Proformas Citas o Turnos Órdenes de trabajo Órdenes de monitoreo. Contratos. Facturación. Comisiones. Ventas.	EX	[D]	Al haber un fallo del sistema de identificación y autorización los usuarios consiguen acceder a los recursos del sistema sin tener autorización. Acceder al sistema sin tener autorización se puede manipular la información dejando datos incorrectos.	1. [I] integridad	100%	MA	EX	MA	NO	DE	100%	MA	EX	MA

3.1.10.4.1. INFORME DEL IMPACTO POTENCIAL Y RESIDUAL POR ATAQUES INTENCIONADOS

Ante las amenazas:

Suplantación de la identidad del usuario, que afecta a los activos: Clientes, Solicitudes y seguimiento, Proformas, Citas o Turnos, Órdenes de trabajo, Órdenes de monitoreo, Contratos, Facturación, Comisiones, Ventas.

Abuso de privilegios de acceso, que afecta a los activos: Clientes, Solicitudes y seguimiento, Proformas, Citas o Turnos, Órdenes de trabajo, Órdenes de monitoreo, Contratos, Facturación, Comisiones, Ventas.

Tienen salvaguardas implementadas para hacerles frente, pero su eficacia es Muy baja por lo que el Impacto residual es igual al impacto Potencial sobre los activos.

Ante las amenazas:

Manipulación de la configuración que afecta al activo: Registro de menús y opciones.

Alteración de secuencia, que afecta al activo: Correo corporativo

Y Acceso no autorizado, que afecta a los activos: Clientes, Solicitudes y seguimiento, Proformas, Citas o Turnos, Órdenes de trabajo, Órdenes de monitoreo, Contratos, Facturación, Comisiones, Ventas.

No tienen salvaguardas para hacerles frente, debido a esto el Impacto Potencial y Residual son iguales.

El grafico se muestra que el Impacto Potencial y el Impacto Residual son iguales ante las amenazas indicadas anteriormente.

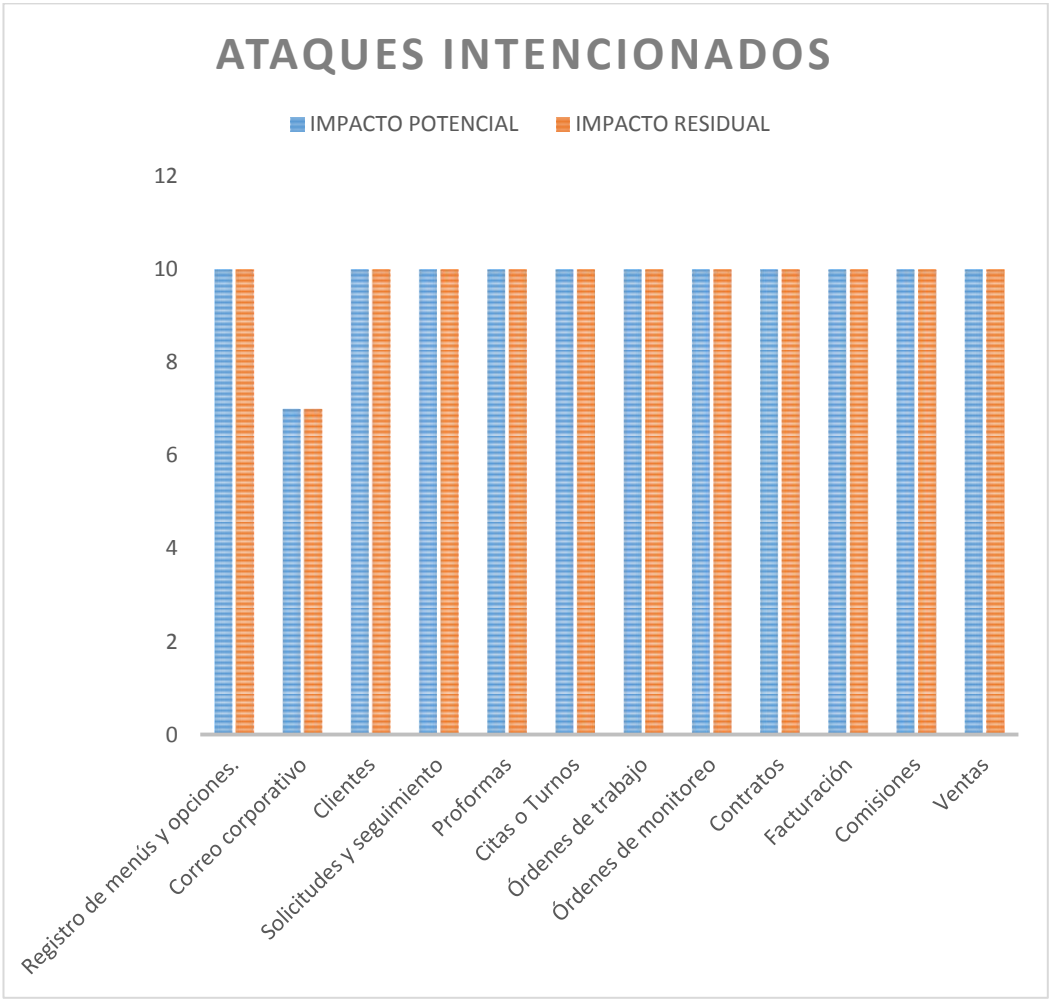

Figura 39. Estimación del Impacto por Ataques Intencionados

3.1.10.4.2. INFORME DEL RIESGO POTENCIAL Y RESIDUAL POR ATAQUES INTENCIONADOS

Ante las amenazas:

Suplantación de la identidad del usuario, que afecta a los activos: Clientes, Solicitudes y seguimiento, Proformas, Citas o Turnos, Órdenes de trabajo, Órdenes de monitoreo, Contratos, Facturación, Comisiones, Ventas.

Abuso de privilegios de acceso, que afecta a los activos: Clientes, Solicitudes y seguimiento, Proformas, Citas o Turnos, Órdenes de trabajo, Órdenes de monitoreo, Contratos, Facturación, Comisiones, Ventas.

Tienen salvaguardas implementadas para hacerles frente, pero su eficacia es Muy baja por lo que el RIESGO residual es igual al RIESGO Potencial sobre los activos.

Ante las amenazas:

Manipulación de la configuración que afecta al activo: Registro de menús y opciones.

Alteración de secuencia, que afecta al activo: Correo corporativo

Y Acceso no autorizado, que afecta a los activos: Clientes, Solicitudes y seguimiento, Proformas, Citas o Turnos, Órdenes de trabajo, Órdenes de monitoreo, Contratos, Facturación, Comisiones, Ventas.

No tienen salvaguardas para hacerles frente, debido a esto el RIESGO Potencial y Residual son iguales.

El gráfico se muestra que el Riesgo Potencial y el Riesgo Residual son iguales ante las amenazas indicadas anteriormente, en ambos tipos es un Riesgo Critico.

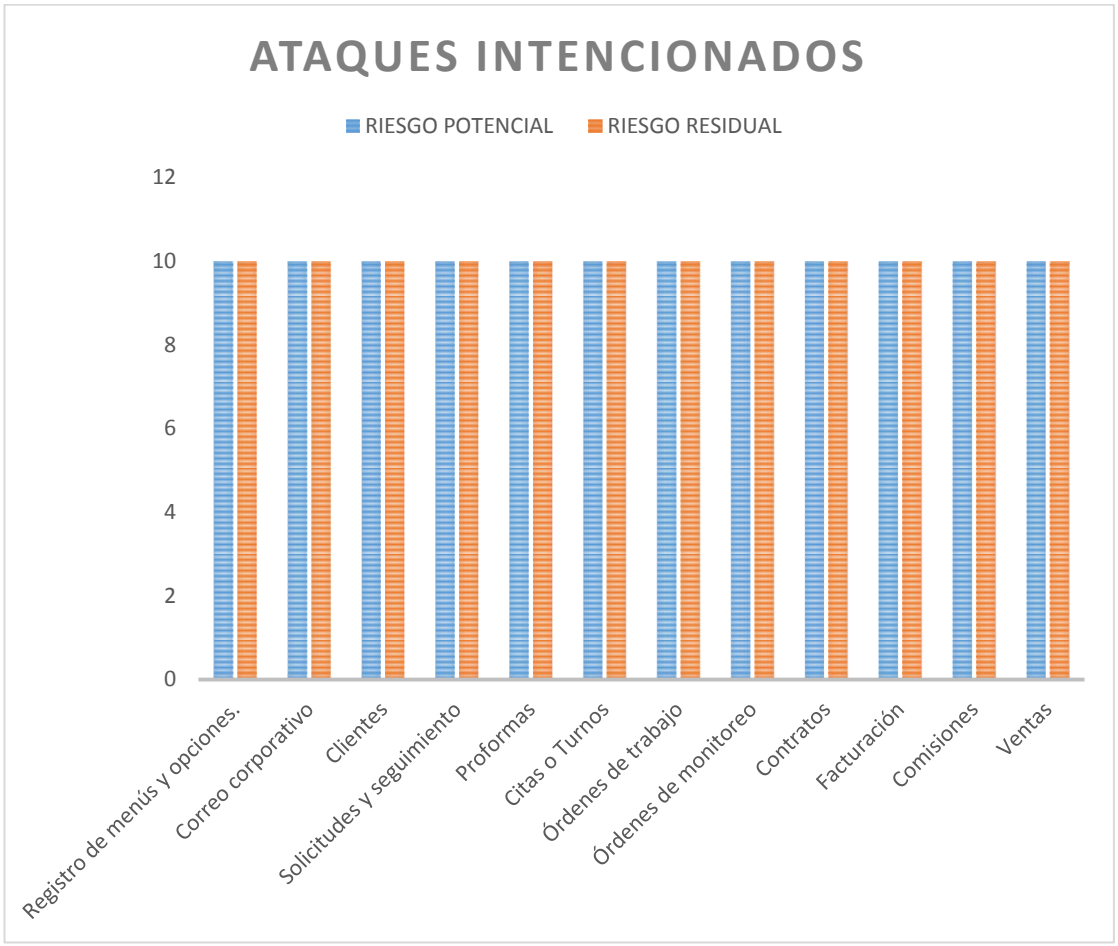

Figura 40. Estimación del Riesgo por Ataques Intencionados

3.1.10.4.3. INFORME DEL IMPACTO POTENCIAL Y RESIDUAL POR USO NO PREVISTO

Ante la amenaza Uso no previsto, existe implementada una salvaguarda altamente eficaz para hacerle frente, por lo que el IMPACTO RESIDUAL se considera Despreciable sobre los activos con Respecto al IMPACTO POTENCIAL, esto se muestra claramente en el gráfico.

Figura 41. Estimación del Impacto por Uso no Previsto

3.1.10.4.4. INFORME DEL RIESGO POTENCIAL Y RESIDUAL POR USO NO PREVISTO

Ante la amenaza Uso no previsto, existe implementada una salvaguarda altamente eficaz para hacerle frente, por lo que el RIESGO RESIDUAL que tienen los activos en que se materialice la amenaza se considera Despreciable con Respecto al RIESGO POTENCIAL, esto se muestra claramente en el gráfico.

Figura 42. Estimación del Riesgo por Uso no Previsto

Tabla 68.

Análisis de Estimación del Riesgo por Ataques Intencionados

AMENAZA	ACTIVO	VALORACION DEL ACTIVO	TIPO DE ACTIVO	EFECTO DE LA AMENAZA	DIMENSIONES AFECTADAS	DEGRADACION DEL VALOR DEL ACTIVO	PROBABILIDAD DE OCURRENCIA DE LA AMENAZA	IMPACTO POTENCIAL	RIESGO POTENCIAL	SALVAGUARDA IMPLEMENTADA	EFICACIA DE LA SALVAGUARDA	DEGRADACION RESIDUAL	PROBABILIDAD RESIDUAL	IMPACTO RESIDUAL	RIESGO RESIDUAL
Repudio	Clientes Solicitudes y seguimiento Proformas Citas o Turnos Órdenes de trabajo Órdenes de monitoreo. Contratos. Facturación. Comisiones. Ventas.	EX	[S]	Negación de acciones realizadas. Al negar que se ha enviado, recibido o entregado mensajes podría afectar de gran manera a la información o servicios ya que esos mensajes podrían ser importantes o urgentes y se llegaría incluso a perder clientes debido a la ineficiencia de los usuarios.	1. [I] integridad	100%	MA	EX	MA	SI	M	40%	M	MA	MA
Modificación deliberada de la información	Inventarios Cartera clientes Cartera proveedores Transacciones contables Contratos Facturación Comisiones Registros de auditoría Información del cliente vehículos	EX	[D]	Modificar intencionalmente la información por obtener algún beneficio o simplemente por perjudicar ya sea a una persona o a la empresa. No dar de baja artículos o dar de baja más de los artículos que en realidad son. Canal incorrecto, datos personales erróneos, vehículos equivocados. Datos personales erróneos. Descuadre al cierre de mes o del año. Servicios y fecha incorrecta. Facturas físicas diferentes a las del sistema. Comisiones a personas incorrectas. Se tendría una inconsistencia sobre los registros.	1. [I] integridad	100%	MA	EX	MA	NO	DE	100%	MA	EX	MA

Tabla 69.

Análisis de Estimación del Riesgo por Ataques Intencionados

AMENAZA	ACTIVO	VALORACION DEL ACTIVO	TIPO DE ACTIVO	EFECTO DE LA AMENAZA	DIMENSIONES AFECTADAS	DEGRADACION DEL VALOR DEL ACTIVO	PROBABILIDAD DE OCURRENCIA DE LA AMENAZA	IMPACTO POTENCIAL	RIESGO POTENCIAL	SALVAGUARDA IMPLEMENTADA	EFICACIA DE LA SALVAGUARDA	DEGRADACION RESIDUAL	PROBABILIDAD RESIDUAL	IMPACTO RESIDUAL	RIESGO RESIDUAL
Destrucción de información	BddConta (SqlServer 2000) BddTrib (SqlServer 2000) BddAcf (Dbase II) BddRrhh MySQL (5.5.23) Remote Desktop BddEval (SQLServer 2005) BddCall1 (Mysql 5.0.77) BddCall2 (Mysql5.0.77) BddCrm (Mysql 5.5.23) BddCrm (Mysql 5.1.27) BddCrm (Mysql 5.5.14) BddExtranet(SQLServer 2005)	EX	[SW]	Bases de datos sin información. Eliminar intencionalmente la información, con ánimo de obtener un beneficio personal o causar daño.	1. [C] confidencialidad	100%	A	EX	MA	SI	B	60%	B	EX	MA
Divulgación de la información	Cartera clientes Información del personal. Usuarios y perfiles Menús y opciones	EX	[D]	Revelar la información a personas ajenas a la compañía. Falsificación de datos del cliente. Falsificación de datos del personal. Falsificación de usuarios y claves. Acceso al sistema a personas que no son parte del personal de la empresa.	1. [C] confidencialidad	100%	MA	EX	MA	SI	M	40%	M	MA	MA

3.1.10.4.5. INFORME DEL IMPACTO POTENCIAL Y RESIDUAL POR ATAQUES INTENCIONADOS

Ante la amenaza:

Repudio, que afecta los activos: Clientes, Solicitudes y seguimiento, Proformas, Citas o Turnos, Órdenes de trabajo, Órdenes de monitoreo, Contratos, Facturación, Comisiones, y Ventas.

Tiene una salvaguarda 60% eficaz, por lo que el IMPACTO RESIDUAL es menor con respecto al IMPACTO POTENCIAL.

Ante la amenaza:

Destrucción de información que afecta a las Bases de Datos, y **Modificación deliberada** que afecta a significativamente a Registros de auditoría, e Información del cliente vehículos, No tienen salvaguardas que se pueden hacer frente por lo Impacto Residual y el Impacto Potencial es el mismo sobre estos activos.

En grafico se muestra las variantes del Impacto:

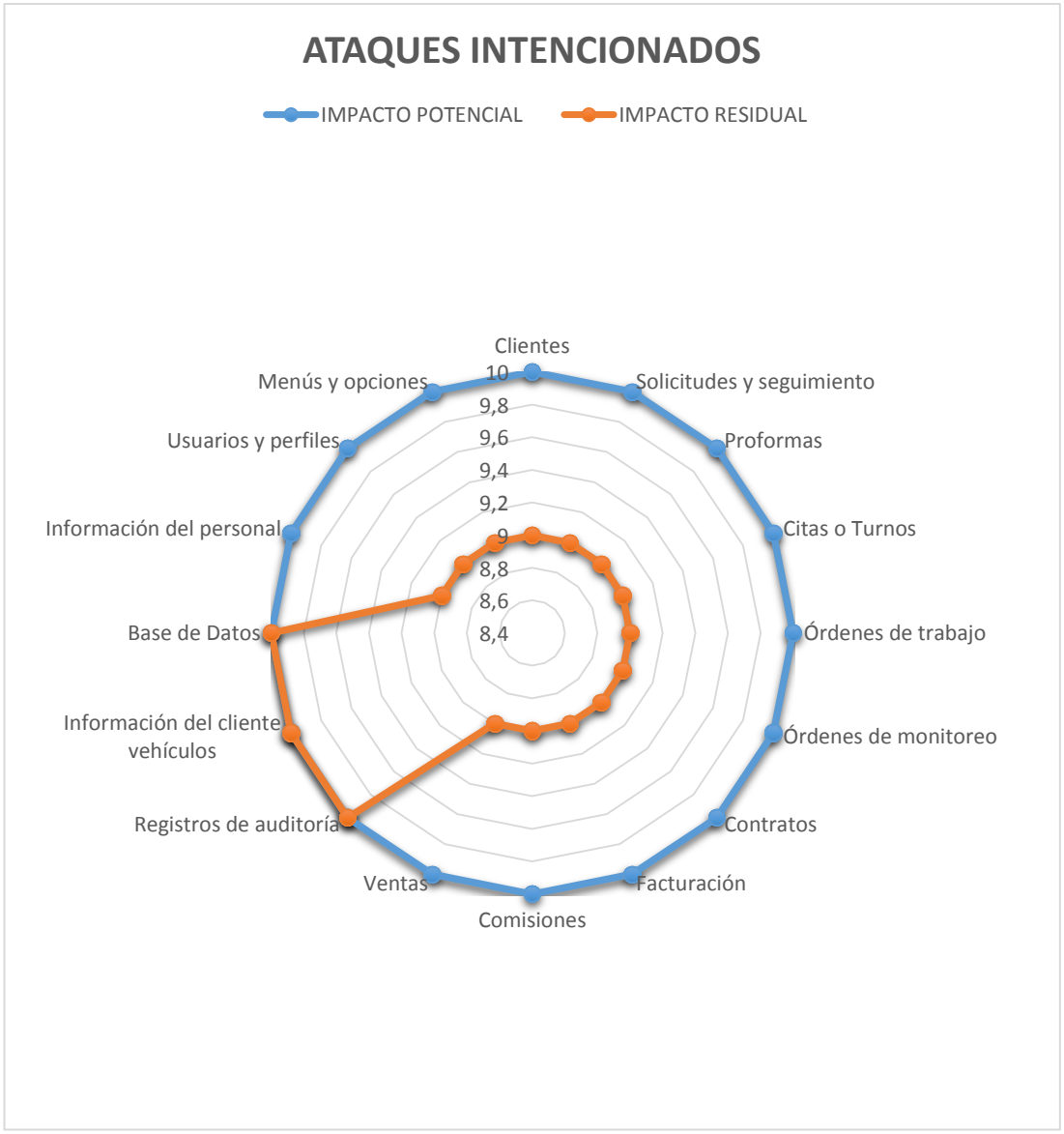

Figura 43. Estimación del Impacto por Ataques Intencionados

3.1.10.4.6. INFORME DEL RIESGO POTENCIAL Y RESIDUAL POR ATAQUES INTENCIONADOS

Ante la amenaza:

Repudio, que afecta los activos: Clientes, Solicitudes y seguimiento, Proformas, Citas o Turnos, Órdenes de trabajo, Órdenes de monitoreo, Contratos, Facturación, Comisiones, y Ventas.

Tiene una salvaguarda 60% eficaz, por lo que el impacto residual es menor con respecto al Impacto Potencial, pero no lo significativamente para poner disminuir el Riesgo, por lo que el Riesgo Potencial y Residual son iguales, estos activos tienen un Riesgo Critico.

Ante la amenaza:

Destrucción de información que afecta a las Bases de Datos, y **Modificación deliberada** que afecta a significativamente a Registros de auditoría, e Información del cliente vehículos, No tienen salvaguardas que se pueden hacer frente por lo Impacto Residual y el Impacto Potencial es el mismo sobre estos activos, y también tienen un Riesgo Critico.

En grafico se muestra la continuidad del Riesgo:

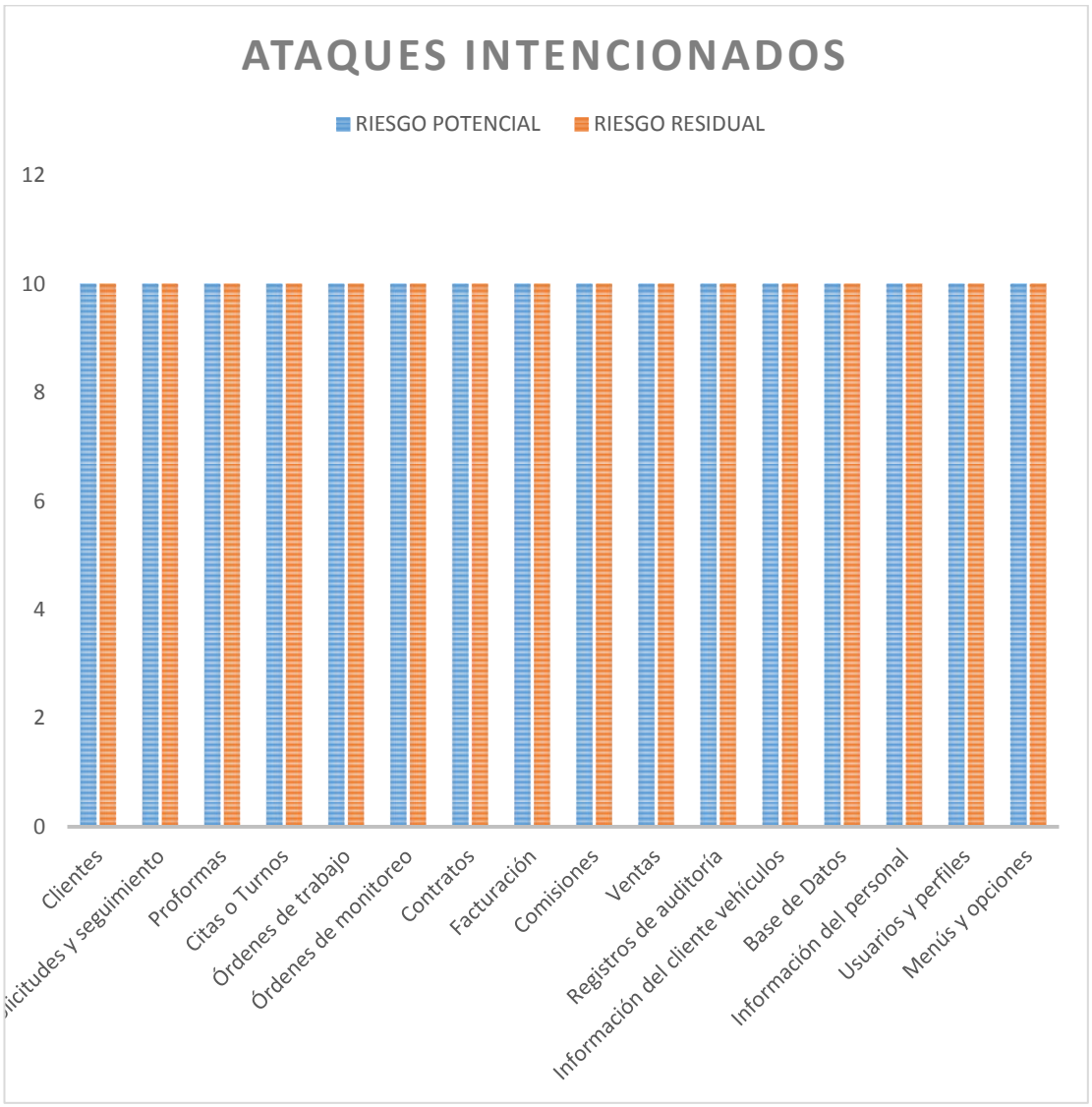

Figura 44. Estimación del Riesgo por Ataques Intencionados

Tabla 70.

Análisis de Estimación del Riesgo por Ataques Intencionados

AMENAZA	ACTIVO	VALORACION DEL ACTIVO	TIPO DE ACTIVO	EFECTO DE LA AMENAZA	DIMENSIONES AFECTADAS	DEGRADACION DEL VALOR DEL ACTIVO	PROBABILIDAD DE OCURRENCIA DE LA AMENAZA	IMPACTO POTENCIAL	RIESGO POTENCIAL	SALVAGUARDA IMPLEMENTADA	EFICACIA DE LA SALVAGUARDA	DEGRADACION RESIDUAL	PROBABILIDAD RESIDUAL	IMPACTO RESIDUAL	RIESGO RESIDUAL
Manipulación de programas	Sistema administrativo financiero. Sistema administración tributaria. Sistema activos fijos. Sistema de gestión humana. Sistema de evaluaciones Sistema de administración de clientes. Accouting interfase. Sistema de administración de seguridades. Call center asterix. Posfix. CIFS Sistema de control de mensajes Sistema de análisis de mensajes Sistema web portal Tracklink. Sistema web portal véstigo. Active directory.	MA	[SW]	Al realizar una alteración intencionada del funcionamiento de los programas, las aplicaciones funcionarían de manera incorrecta. Al modificar el código de los programas se podría capturar los datos y enviar a otra base para uso personal indebido. Dejar con un mal funcionamiento las aplicaciones.	1. [I] integridad 2. [C] confidencialidad 3. [D] disponibilidad	100%	MA	MA	MA	SI	MB	80%	A	MA	MA

3.1.10.4.7. INFORME DEL IMPACTO POTENCIAL Y RESIDUAL POR MANIPULACION DE PROGRAMAS

Ante la amenaza:

Manipulación de programas, hay una salvaguarda para hacerle frente pero eficazmente muy baja, por lo que el Impacto sobre los activos tanto RESIDUAL como POTENCIAL, es el mismo.

En el grafico se muestra la continuidad del IMPACTO

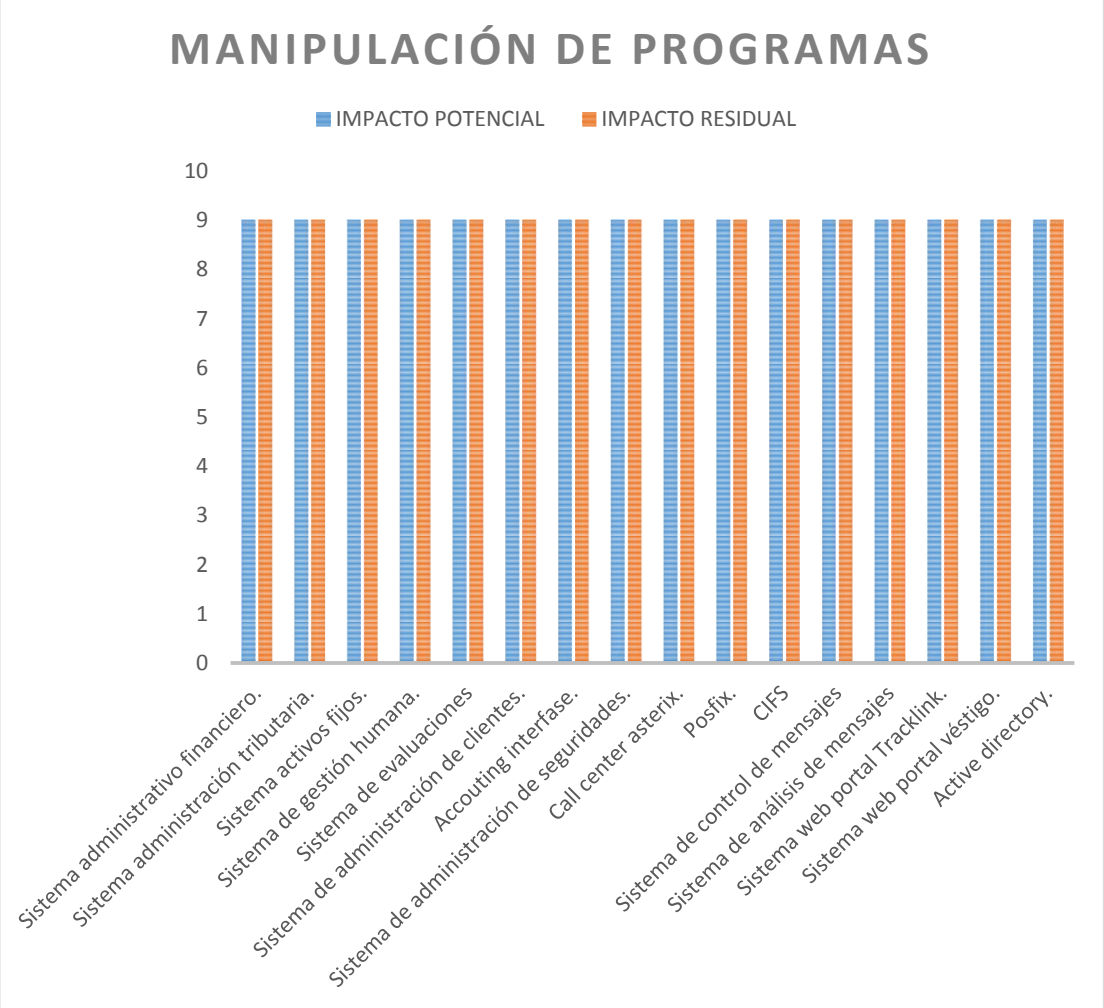

Figura 45. Estimación del Impacto por Manipulación de Programas

3.1.10.4.8. INFORME DEL RIESGO POTENCIAL Y RESIDUAL POR MANIPULACION DE PROGRAMAS

Ante la amenaza:

Manipulación de programas, hay una salvaguarda para hacerle frente pero eficazmente muy baja, por lo que el RIESGO sobre los activos tanto RESIDUAL como POTENCIAL, es el mismo.

En el grafico se muestra la continuidad del RIESGO

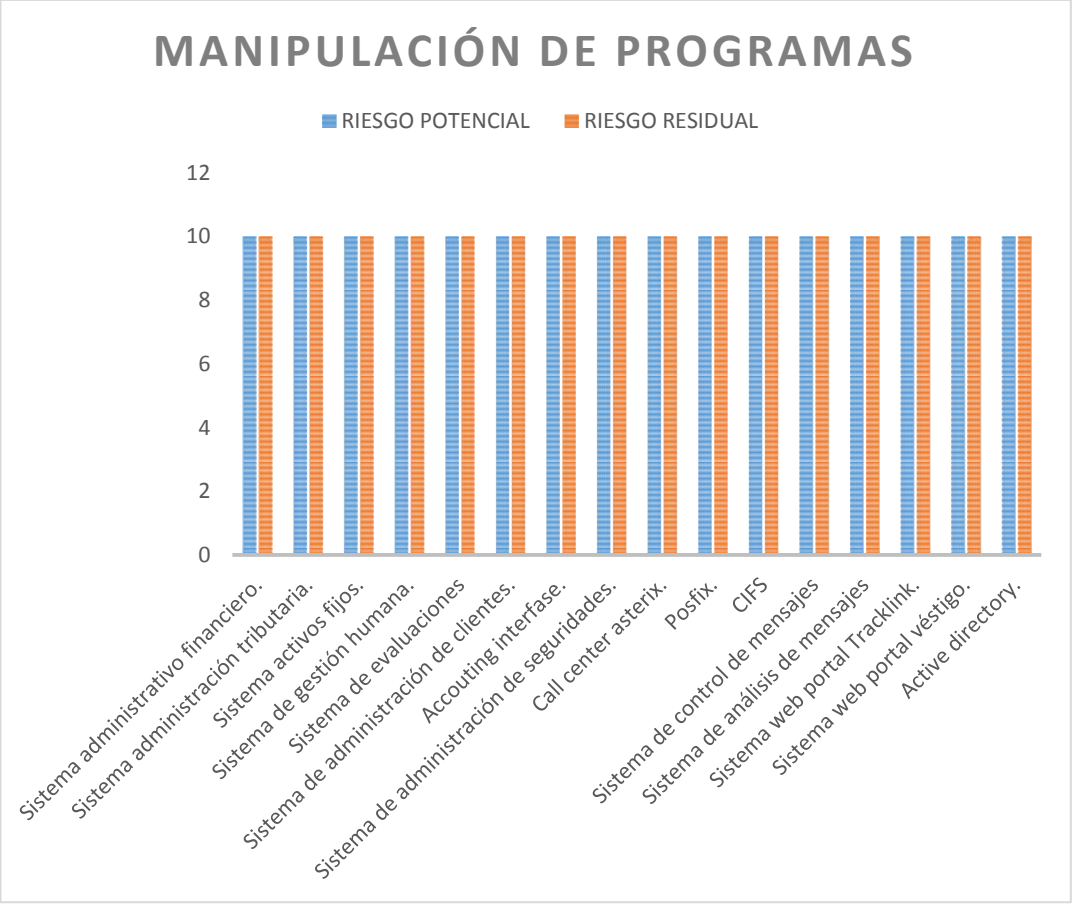

Figura 46. Estimación del Riesgo por Manipulación de Programas

CAPITULO 4.- EVALUACION DE LOS CONTROLES DEL NEGOCIO COBIT

Dentro de los objetivos de Gobierno que nos propone Cobit 5, la Optimización del Riesgo constituye uno de los tres pilares fundamentales para la Creación de Valor junto con la Realización de Beneficios y Optimización de Recursos.

4.1. OPTIMIZACION DEL RIESGO Y LAS METRICAS DE TI

Los Objetivos de la Empresa y las Métricas de TI directamente relacionadas con la Optimización del Riesgo, que formarán parte de nuestro análisis son:

4.1.1. Dimensión Financiera

4.1.1.1. Cumplimiento de Leyes y Regulaciones Externas

Los servicios que brindan los sistemas están actualizados de acuerdo con las leyes y reglamentos vigentes de tal manera que no se ha incurrido en costos relacionados con costos de incumplimientos TI, que hayan tenido impacto o causado pérdida de reputación ni internos ni relacionados con proveedores de TI.

En lo relacionado a la cobertura por evaluaciones de cumplimiento, no existe un proceso de evaluaciones de cumplimiento así como tampoco se han definido los parámetros de cobertura necesarios para suplir este riesgo en caso que fuera necesario.

4.1.1.2. Riesgos de Negocio Gestionado

En el levantamiento de información se determinó que no existían procesos formales de evaluación de riesgos realizados anteriormente, por lo tanto no existen métricas para determinar si fueron adecuadamente gestionados.

4.1.2. Dimensión Cliente

4.1.2.1. Entrega de servicios de TI de acuerdo a los requisitos del negocio

Durante el último año se han registrado 8 de interrupciones de negocio en periodos de tiempo promedio de 30 minutos debidas a incidentes relacionados con los enlaces de comunicaciones, considerando que se trata de un servicio 24h x 7d se ha determinado un porcentaje de disponibilidad del 99.95%.

No se han realizado medidas de satisfacción en la entrega de servicios TI por parte de clientes ni usuarios satisfechos con la calidad de la entrega de servicios TI.

4.1.3. Dimensión Interna

4.1.3.1. Seguridad de la información, infraestructuras de procesamiento y aplicaciones

No se han registrado incidentes de seguridad causantes de pérdidas financieras, interrupción del negocio o vergüenza pública.

Entre los servicios de TI sin requerimientos de seguridad destacables por corresponder a tecnología obsoleta podemos mencionar el sistema de Activos Fijos que no cuenta con un control de seguridad integrado, así como tampoco registros de accesos ni control de cambios.

Existe una deficiencia en lo referente al tiempo necesario para la concesión, cambio y eliminación de privilegios de acceso, relacionado con la falta de un procedimiento interno adecuado.

No se han realizado evaluaciones de seguridad, así como tampoco se han establecido estándares y guías.

4.1.3.2. Cumplimiento con las políticas internas por parte de las TI

No se registran incidentes relacionados con el incumplimiento de políticas debido a que los sistemas mantienen controles adecuados a las políticas internas y los usuarios se encuentran capacitados en las mismas.

Por otra parte es necesario mencionar que las políticas se documentan y revisan únicamente antes de ser modificadas e implementadas.

4.2. OPTIMIZACION DEL RIESGO Y EL GOBIERNO DE TI

Para un adecuado Gobierno de TI, es necesario implementar el proceso de Asegurar la Optimización del Riesgo ya que no se han realizado anteriormente evaluaciones de riesgo por consiguiente no se ha realizado una orientación ni supervisión. Tomamos como marco de referencia el proceso “EDM03 Asegurar la Optimización del Riesgo”.

4.3. OPTIMIZACION DEL RIESGO Y LA GESTION DE TI

En lo referente a la Gestión de TI vamos a tomar en cuenta los siguientes dominios de Cobit relacionados con la Optimización del riesgo:

4.3.1. Alinear, Planificar Organizar (APO)

Como hemos observado, en el levantamiento de información y de acuerdo a los altos niveles de riesgo existente, es necesario implementar un proceso cíclico de la Gestión del Riesgo que permita Alinear, Planificar y Organizar las actividades de manera que continuamente se recopile datos, se analice del nivel de riesgo y se transparente para que pueda ser gestionado. Tomamos como marco de referencia el proceso “APO12 Gestionar el Riesgo”.

Hemos detectado que existe un impacto muy alto sobre los activos en caso de que se materialicen “Amenazas por Ataques Intencionales”, por lo cual Cobit nos sugiere que se defina, gestione y supervise un plan para el tratamiento del riesgo de la seguridad de información (SGSI). Tomamos como marco de referencia el proceso “APO13 Gestionar la Seguridad”.

4.3.2. Construir Adquirir e Implementar (BAI)

Se han identificado los Activos Críticos de TI, sin embargo las salvaguardas actualmente implementadas para su protección no son eficaces al 100%, por lo cual es necesario determinar y gestionar su ciclo de vida para asegurar la capacidad la fiabilidad y capacidad de servicio. En lo referente a la Administración de Licencias se han determinado deficiencias en el control de la cantidad necesaria para cubrir el software instalado y en uso. Tomamos como marco de referencia el proceso “BAI09 Gestionar Los Activos”.

En lo referente a la amenaza derivada de los errores de configuración, de los sistemas de Administración y Seguridades, Clientes, Contratos y Transacciones Contables no se han implementado salvaguardas, por tal razón se debe definir modelos base de referencia, controlar de forma efectiva los puntos de acceso a configuraciones, generar informes de

accesos y cambios así como verificar continuamente su integridad. Tomamos como marco de referencia el proceso “BA10 Gestionar la Configuración”.

4.3.3. Entregar, dar Servicio y Soporte (DSS)

No se han establecido Acuerdos de Nivel de Servicio, así como tampoco se han establecido procedimientos operativos que permitan monitorizar, gestionar y resolver las peticiones de servicios internos y externalizados de TI. Tomamos como marco de referencia el proceso “DSS01 Gestionar Operaciones”, “DSS02 Gestionar Peticiones e Incidentes de Servicio” y “DSS03 Gestionar Problemas”.

Se ha determinado que las salvaguardas eficaces ante algunos tipos de amenazas como Desastres Naturales e Industriales, así como los posibles fallos en los Enlaces de Datos, degradación en los soportes de almacenamiento, no son eficaces, siendo el Riesgo Potencial y Residual críticos. Ante esta situación se hace necesario establecer y gestionar un plan que permita de forma efectiva mantener la continuidad del negocio atendiendo a los servicios más importantes y la disponibilidad de la información. Tomamos como marco de referencia el proceso “DSS04 Gestionar la Continuidad”.

Si bien se mantienen implementados controles de acceso lógico a la información y redes de comunicaciones, se ha determinado que no se han implementado políticas de seguridad para mantener un control de acceso físico a los activos de TI y deficiencias en la administración del acceso a los dispositivos de salida. Ante esta situación se hace necesaria la implementación de dispositivos electrónicos de acceso físico y un levantamiento detallado de los dispositivos de salida activados con el fin de restringir los accesos y su posterior administración. Tomamos como marco de referencia el proceso “DSS05 Gestionar Servicios de Seguridad”.

Es necesario implementar un proceso que permita retroalimentar y gestionar los errores y excepciones de forma eficaz para que se den las acciones correctivas necesarias y a tiempo. Tomamos como marco de referencia el proceso “DSS06 Gestionar Controles de Proceso de Negocio”.

CAPÍTULO 5.- RESULTADOS DE LA EVALUACION

5.1. ESTIMACION DEL ESTADO DEL RIESGO POR DESASTRES DE ORIGEN NATURAL.

5.1.1. ANALISIS DEL IMPACTO

En el grafico se puede ver que el Impacto por Daños por Agua y otros desastres naturales es Mayor, debido a que no existe salvaguarda implementada para hacer frente esta amenaza.

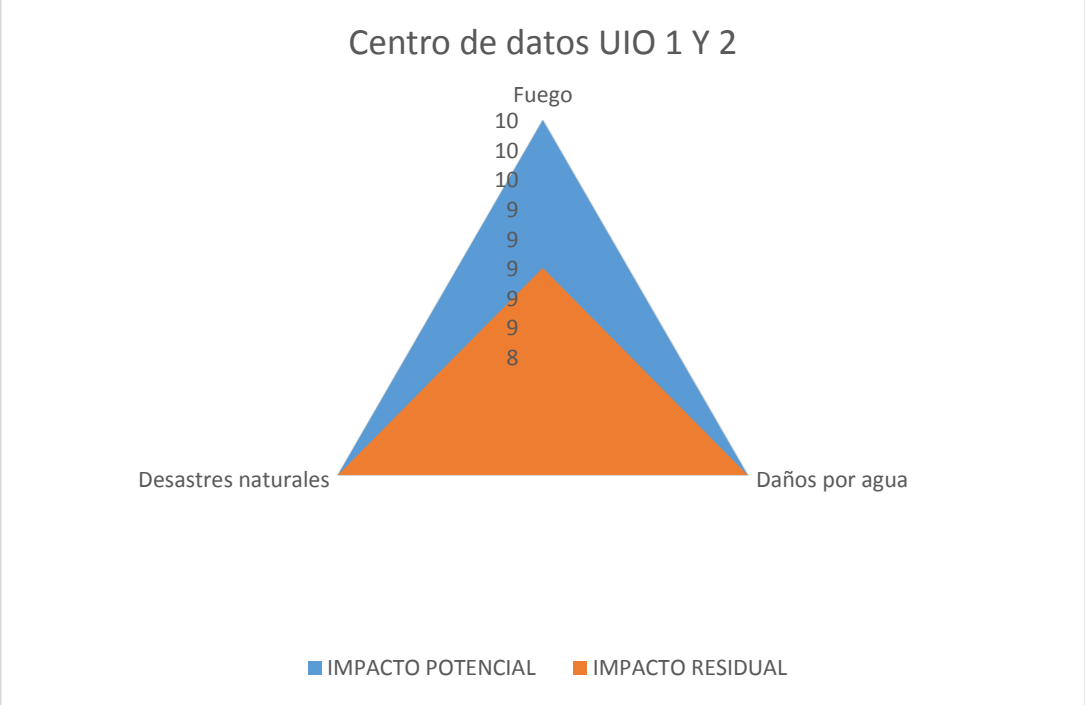

Figura 47. Estimación de Impacto por Desastres Naturales

RESULTADO: IMPACTO MUY ALTO

5.1.2. ANALISIS DEL RIESGO:

En el grafico se puede ver que el Riesgo por Daños por Agua es Mayor, No existe salvaguarda implementada para hacer frente esta amenaza.

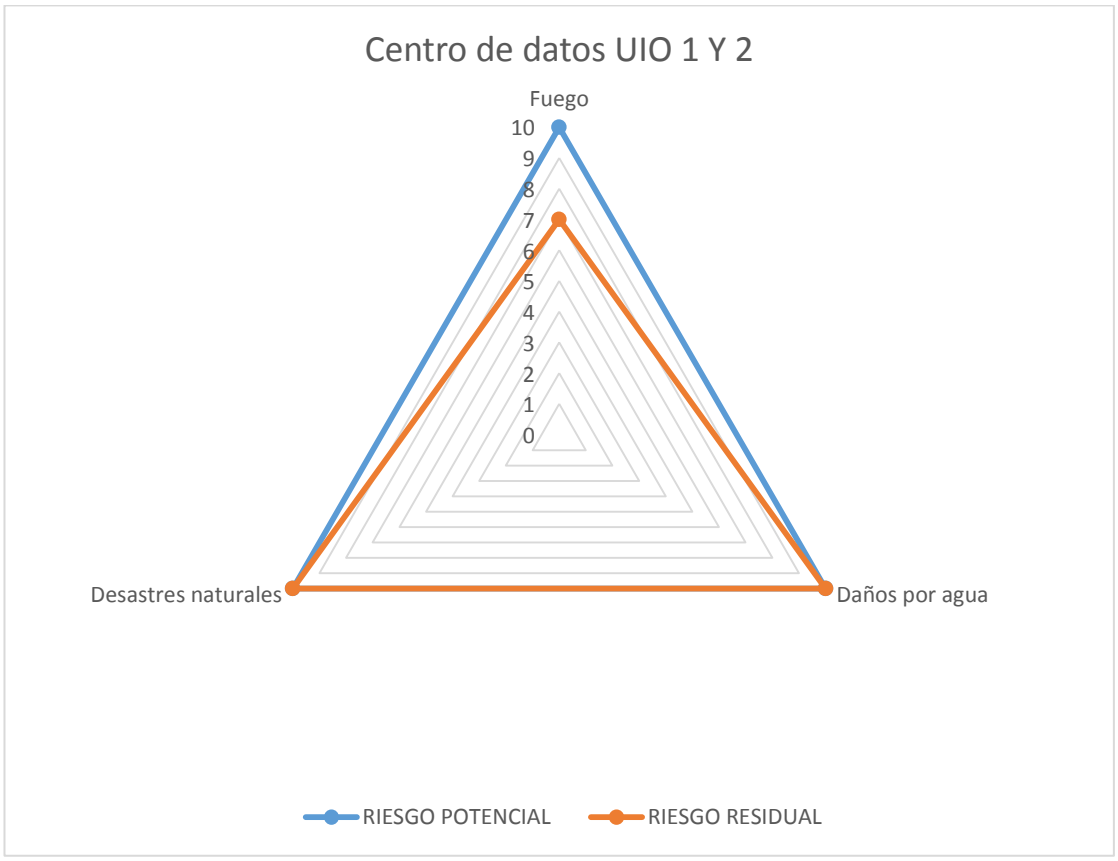

Figura 48. Estimación del Riesgo por Desastres Naturales

RESULTADO: RIESGO CRITICO

5.2. ESTIMACION DEL ESTADO DEL RIESGO POR DESASTRES DE ORIGEN INDUSTRIAL.

5.2.1. ANALISIS DEL IMPACTO

En las Amenazas:

- Fallo de servicios de comunicaciones
- Degradación de los soportes de almacenamiento de la información
- Daños por agua

No tienen implementada una salvaguarda

RESULTADO: IMPACTO MUY ALTO

Las amenazas:

- Condiciones inadecuadas de temperatura o humedad
- Contaminación mecánica
- Avería de origen físico o lógico
- Fuego

Que tienen implementadas salvaguardas aunque no eficaces al 100%, el Impacto Residual es menor con respecto al Impacto Potencial.

RESULTADO: IMPACTO ALTO

En el caso de la amenaza

Corte de Suministro Eléctrico, tiene una salvaguarda 100% Eficaz.

RESULTADO: IMPACTO MUY BAJO

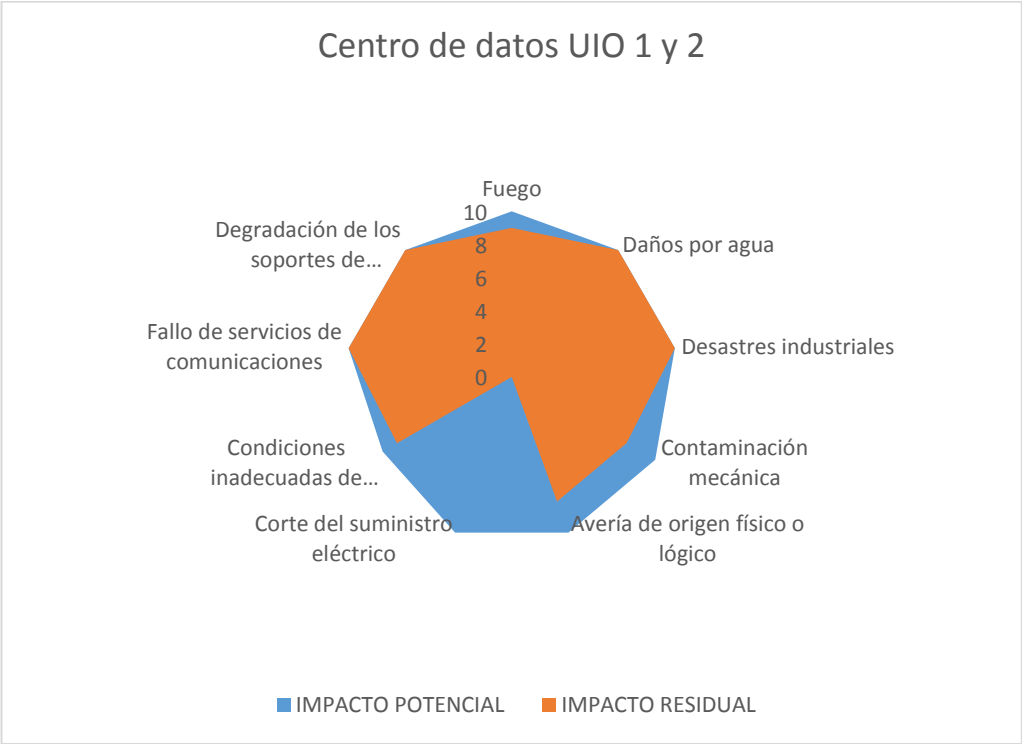

Figura 49. Estimación de Impacto por Desastres de Origen Industrial

5.2.2. ANALISIS DEL RIESGO.

En las Amenazas:

- Fallo de servicios de comunicaciones
- Degradación de los soportes de almacenamiento de la información
- Daños por agua

Que no tienen implementada una salvaguarda.

RESULTADO: RIESGO CRITICO

Las amenazas:

- Condiciones inadecuadas de temperatura o humedad
- Contaminación mecánica
- Avería de origen físico o lógico
- Fuego

Que tienen implementadas salvaguardas aunque no eficaces al 100%, el Impacto Residual es menor con respecto al Impacto Potencial, por tanto el Riesgo Residual también es menor con respecto al Riesgo Potencial.

RESULTADO: RIESGO IMPORTANTE

En el caso de la amenaza

Corte de Suministro Eléctrico, tiene una salvaguarda 100% Eficaz.

RESULTADO: RIESGO DESPRECIABLE

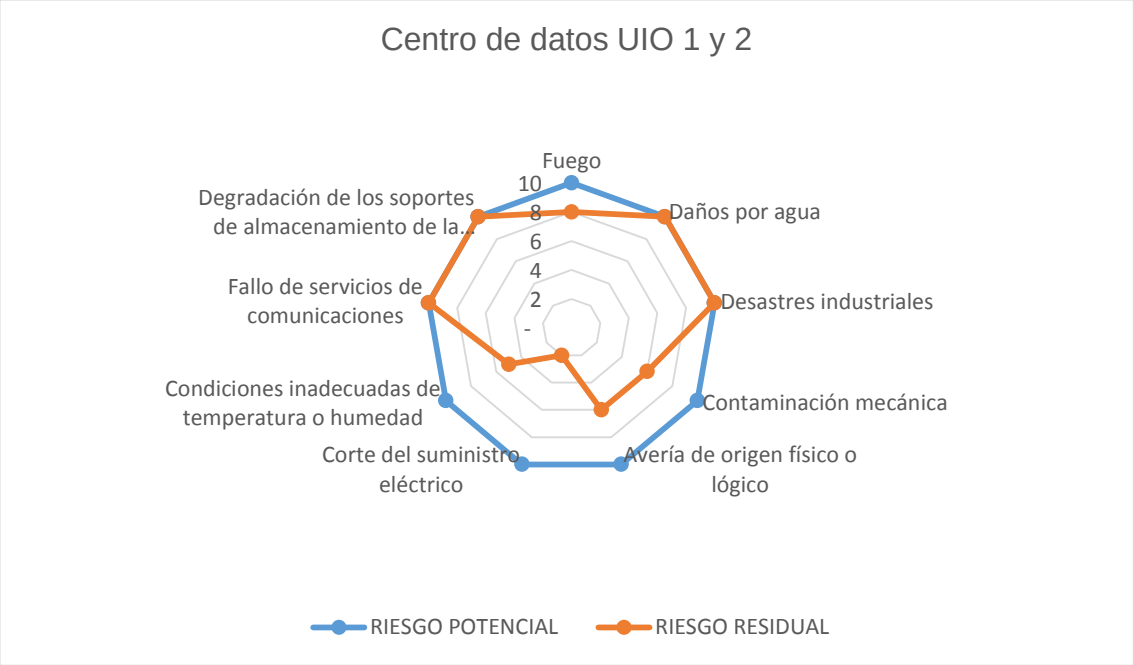

Figura 50. Estimación del Riesgo por Desastres de Origen Industrial

5.3. ESTIMACION DEL ESTADO DEL RIESGO POR ERRORES DE LOS USUARIOS

5.3.1. ANALISIS DE IMPACTO

En el grafico se puede notar que el Impacto Residual baja a 0 en los activos Ordenes de Monitoreo, Contratos y Facturación, debido a la eficacia de las Salvaguardas.

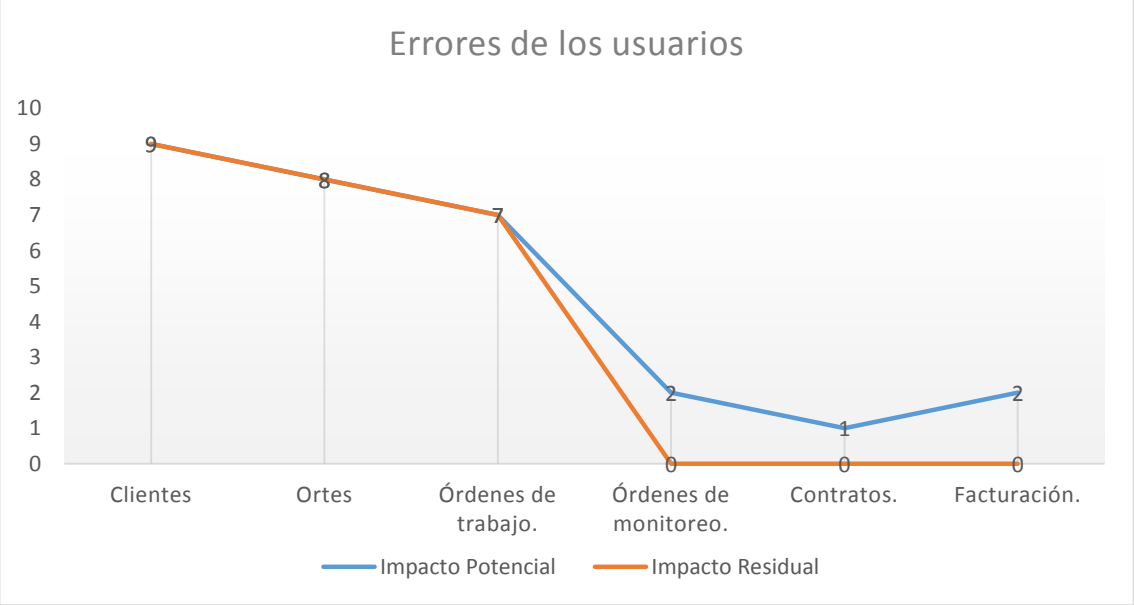

Figura 51. Estimación del Impacto por Errores de los Usuarios

En el Activo Clientes.

RESULTADO: IMPACTO MUY ALTO

En los activos:

- Ortes
- Ordenes de Trabajo

RESULTADO: IMPACTO ALTO

5.3.2. ANALISIS DEL RIESGO

En el grafico se puede notar que el Riesgo Residual baja en los activos Ordenes de Monitoreo, Contratos y Facturación, debido a la eficacia de las Salvaguardas.

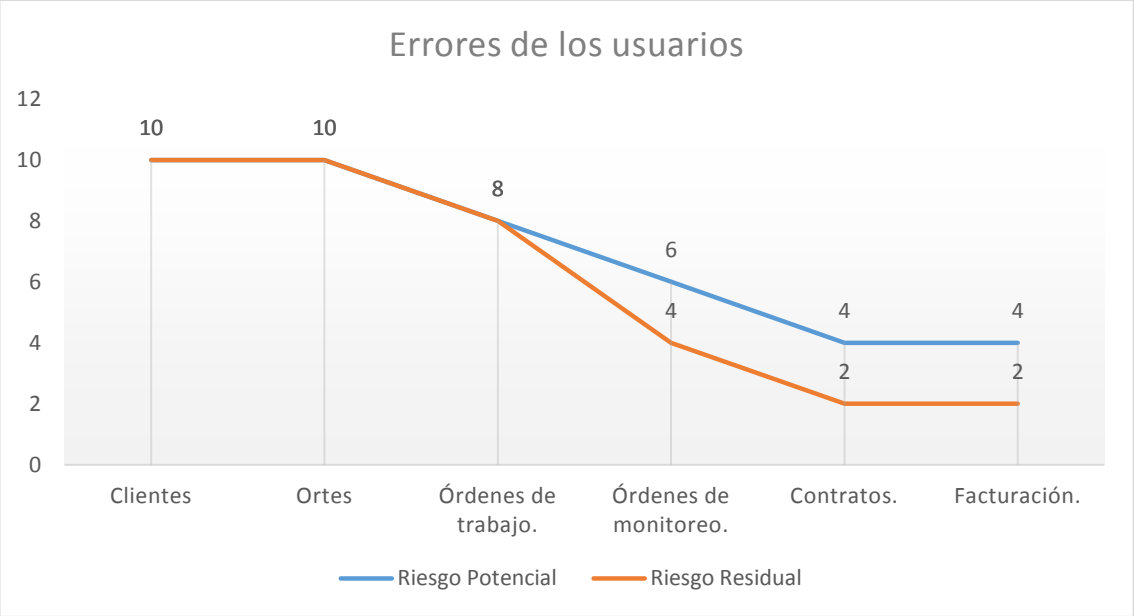

Figura 52. Estimación del Riesgo por Errores de los Usuarios

En los activos:

- Clientes
- Ortes

RESULTADO: RIESGO CRITICO

En el activo:

- Ordenes de Trabajo

RESULTADO: RIESGO IMPORTANTE

5.4. ESTIMACION DEL ESTADO DEL RIESGO POR ERRORES Y FALLOS NO INTENCIONADOS

5.4.1. ANALISIS DE IMPACTO

Para las amenazas Errores del administrador, Errores de monitorización (log) y Errores de configuración, que afectan a los activos: Sistema de administración y seguridades, Clientes, Contratos y Transacciones contables, no existe una salvaguarda implementada.

RESULTADO: IMPACTO MUY ALTO

Para la amenaza Difusión de software dañino que afecta a los activos:

Sistema Administrativo Financiero, Sistema Administración Tributaria, Sistema de activos fijos, Sistema de gestión humana, Sistema de evaluaciones, Sistema de administración de clientes, Accouting Interfase, Sistema de administración de seguridades, Posfix, CIFS, Sistema de control de mensajes, Sistema de análisis de mensajes, Existe una salvaguarda implementada altamente eficaz.

RESULTADO: IMPACTO MUY BAJO

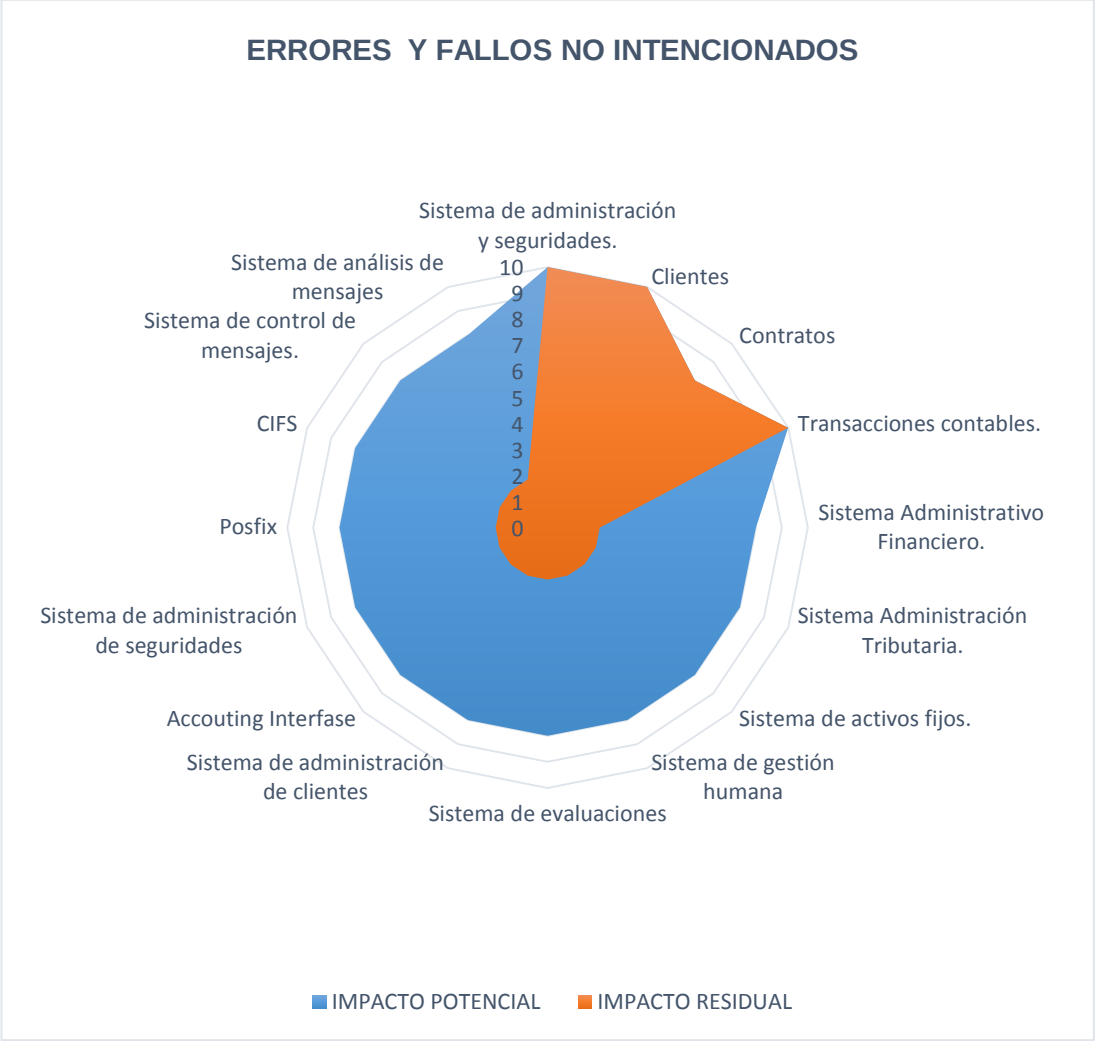

Figura 53. Estimación del Impacto Errores y Fallos No intencionados

5.4.2. ANALISIS DE RIESGO

Para las amenazas Errores del administrador, Errores de monitorización (log) y Errores de configuración, que afectan a los activos: Sistema de administración y seguridades, Clientes, Contratos y Transacciones contables, no existe una salvaguarda implementada.

RESULTADO: RIESGO CRITICO

Para la amenaza Difusión de software dañino que afecta a los activos:

Sistema Administrativo Financiero, Sistema Administración Tributaria, Sistema de activos fijos, Sistema de gestión humana, Sistema de evaluaciones, Sistema de administración de clientes, Accouting Interfase, Sistema de administración de seguridades, Posfix, CIFS, Sistema de control de mensajes, Sistema de análisis de mensajes, Existe una salvaguarda implementada altamente eficaz.

RESULTADO: RIESGO DESPRECIABLE

Figura 54. Estimación del Riesgo por Errores y Fallos No intencionados

5.5. ESTIMACION DEL ESTADO DEL RIESGO POR ERRORES Y FALLOS NO INTENCIONADOS

5.5.1. RESULTADOS ANALISIS DE IMPACTO.

Luego del análisis se encuentra que para el activo:

- Correo corporativo, que no tiene implementada ninguna salvaguarda para enfrentar la amenaza: **Errores de secuencia.**

RESULTADO: IMPACTO ALTO

- Sistema de administración de los clientes, que no tiene implementada ninguna salvaguarda para enfrentar la amenaza: **Vulnerabilidades de los programas (software)**

RESULTADO: IMPACTO MUY ALTO

- Sistema de administración de los clientes
- Sistema de administración de seguridades
- Posfix
- CIFS
- Sistema de administración tributaria.

Que no tiene implementada ninguna salvaguarda para enfrentar la amenaza:

Errores de mantenimiento / actualización de programas (software)

RESULTADO: IMPACTO MUY ALTO

- Clientes
- Solicitudes y seguimiento
- Proformas
- Citas o Turnos

- Órdenes de trabajo
- Órdenes de monitoreo
- Contratos
- Facturación
- Comisiones

Que no tiene implementada ninguna salvaguarda para enfrentar la amenaza:

Caída del sistema por agotamiento de recursos

RESULTADO: IMPACTO MUY ALTO

- Rack 1I

Que no tiene implementada ninguna salvaguarda para enfrentar la amenaza:

Pérdida de equipos

RESULTADO: IMPACTO ALTO

- Bases de Datos SQL y Dbase.

Que tiene implementado una salvaguarda eficientemente muy baja frente la amenaza:

Alteración accidental de la información

RESULTADO: IMPACTO MUY ALTO.

- Bases de Datos SQL y Dbase,

Que tiene implementado una salvaguarda eficientemente muy baja frente la amenaza: **Destrucción de información**

RESULTADO: IMPACTO MUY ALTO.

- Cartera clientes
- Información del personal
- Usuarios y perfiles
- Menús y opciones

Que tiene implementado una salvaguarda eficientemente muy baja frente la amenaza: **Fugas de información, que afecta al activo**:

RESULTADO: IMPACTO MUY ALTO.

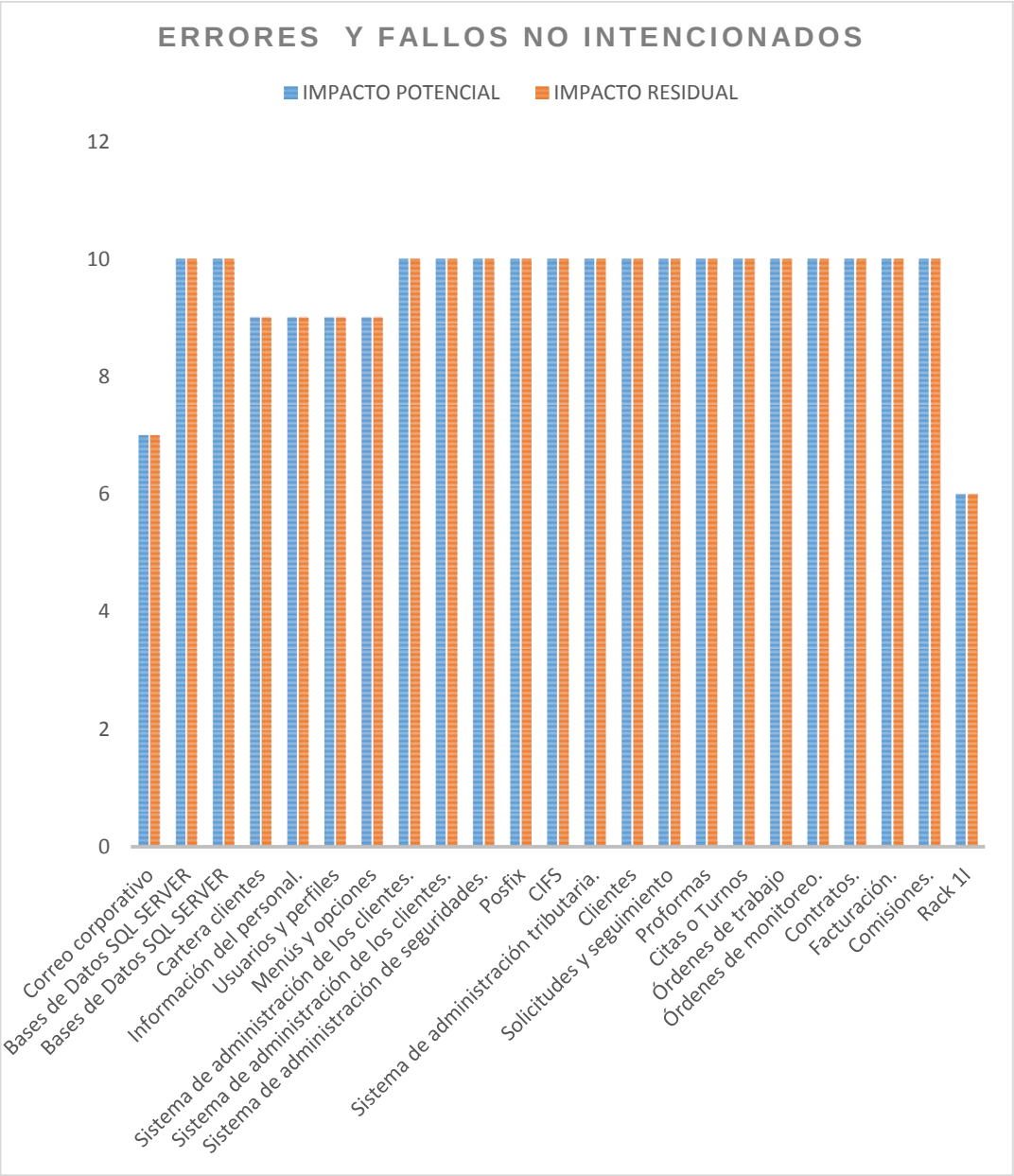

Figura 55. Estimación del Impacto por Errores y Fallos No intencionados

5.5.2. RESULTADOS DEL ANALISIS DE RIESGOS

Luego del análisis se encuentra que para el activo:

- Correo corporativo, que no tiene implementada ninguna salvaguarda para enfrentar la amenaza: **Errores de secuencia.**

RESULTADO: RIESGO CRITICO

- Sistema de administración de los clientes, que no tiene implementada ninguna salvaguarda para enfrentar la amenaza: **Vulnerabilidades de los programas (software)**

RESULTADO: RIESGO CRITICO

- Sistema de administración de los clientes
- Sistema de administración de seguridades
- Posfix
- CIFS
- Sistema de administración tributaria.

Que no tiene implementada ninguna salvaguarda para enfrentar la amenaza:

Errores de mantenimiento / actualización de programas (software)

RESULTADO: RIESGO CRITICO

- Clientes
- Solicitudes y seguimiento
- Proformas
- Citas o Turnos
- Órdenes de trabajo
- Órdenes de monitoreo
- Contratos

- Facturación
- Comisiones

Que no tiene implementada ninguna salvaguarda para enfrentar la amenaza:

Caída del sistema por agotamiento de recursos

RESULTADO: RIESGO CRITICO

- Rack 1I

Que no tiene implementada ninguna salvaguarda para enfrentar la amenaza:

Pérdida de equipos

RESULTADO: ALTO

- Bases de Datos SQL y Dbase.

Que tiene implementado una salvaguarda eficientemente muy baja frente la amenaza:

Alteración accidental de la información

RESULTADO: RIESGO CRITICO

- Bases de Datos SQL y Dbase,

Que tiene implementado una salvaguarda eficientemente muy baja frente la amenaza: **Destrucción de información**

RESULTADO: RIESGO CRITICO

- Cartera clientes
- Información del personal
- Usuarios y perfiles
- Menús y opciones

Que tiene implementado una salvaguarda eficientemente muy baja frente la amenaza, frente a la amenaza: **Fugas de información, que afecta al activo**:

RESULTADO: RIESGO CRITICO

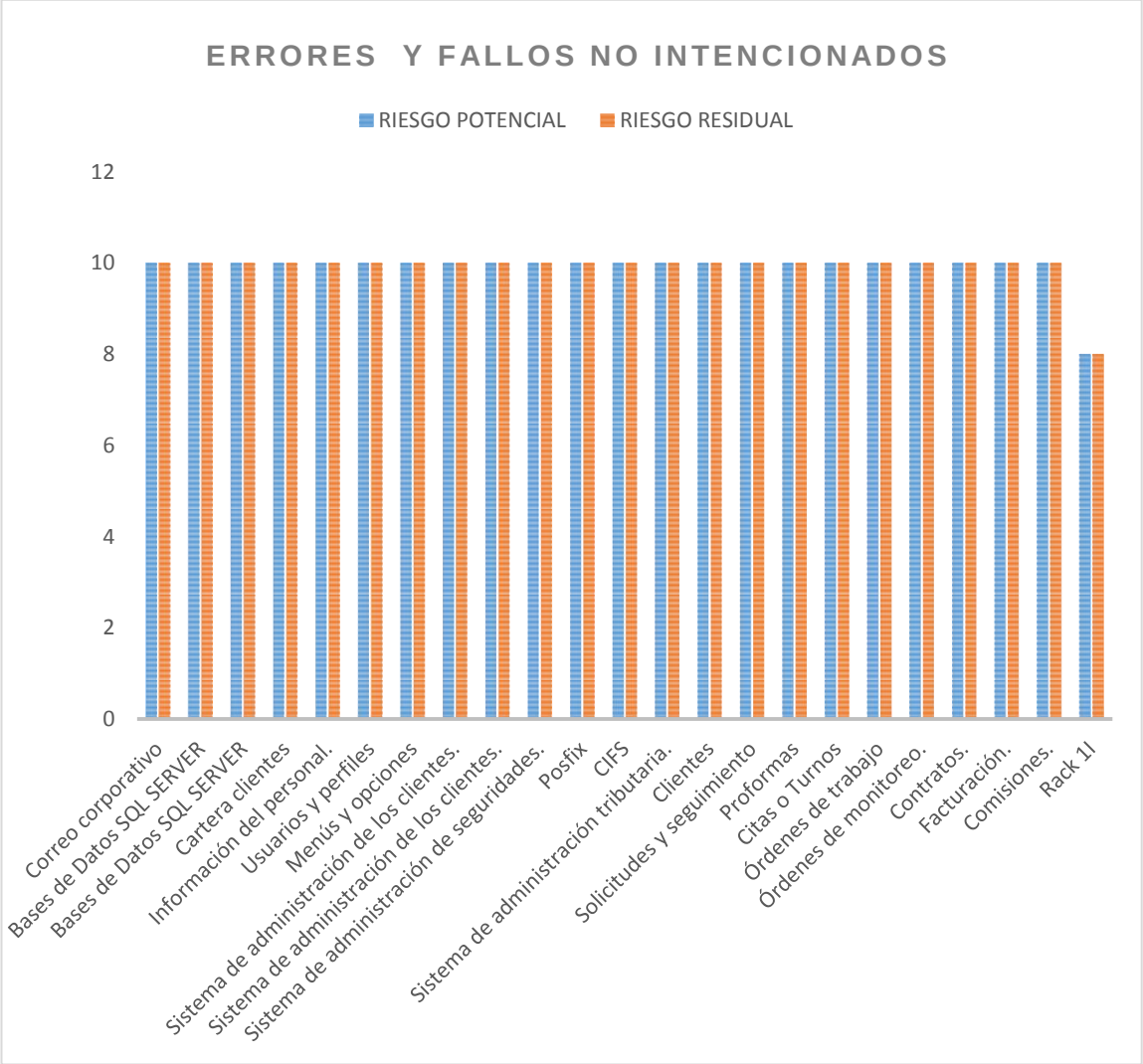

Figura 56. Estimación del Riesgo por Errores y Fallos No intencionados

5.6. ESTIMACION DEL RIESGO POR ATAQUES INTENCIONADOS

5.6.1. RESULTADOS DEL ANALISIS DE IMPACTO

Ante las amenazas, que tienen salvaguardas implementadas para hacerles frente, pero su eficacia es Muy baja por lo que el Impacto residual es igual al impacto Potencial sobre los activos.

Suplantación de la identidad del usuario, que afecta a los activos: Clientes, Solicitudes y seguimiento, Proformas, Citas o Turnos, Órdenes de trabajo, Órdenes de monitoreo, Contratos, Facturación, Comisiones, Ventas

RESULTADO: IMPACTO MUY ALTO

Abuso de privilegios de acceso, que afecta a los activos: Clientes, Solicitudes y seguimiento, Proformas, Citas o Turnos, Órdenes de trabajo, Órdenes de monitoreo, Contratos, Facturación, Comisiones, Ventas

RESULTADO: IMPACTO MUY ALTO

Ante las amenazas:

Manipulación de la configuración que afecta al activo: Registro de menús y opciones.

RESULTADO: IMPACTO MUY ALTO

Alteración de secuencia, que afecta al activo: Correo corporativo

RESULTADO: IMPACTO ALTO

Y Acceso no autorizado, que afecta a los activos: Clientes, Solicitudes y seguimiento, Proformas, Citas o Turnos, Órdenes de trabajo, Órdenes de monitoreo, Contratos, Facturación, Comisiones, Ventas.

RESULTADO: IMPACTO MUY ALTO

El grafico se muestra que el Impacto Potencial y el Impacto Residual son iguales ante las amenazas indicadas anteriormente.

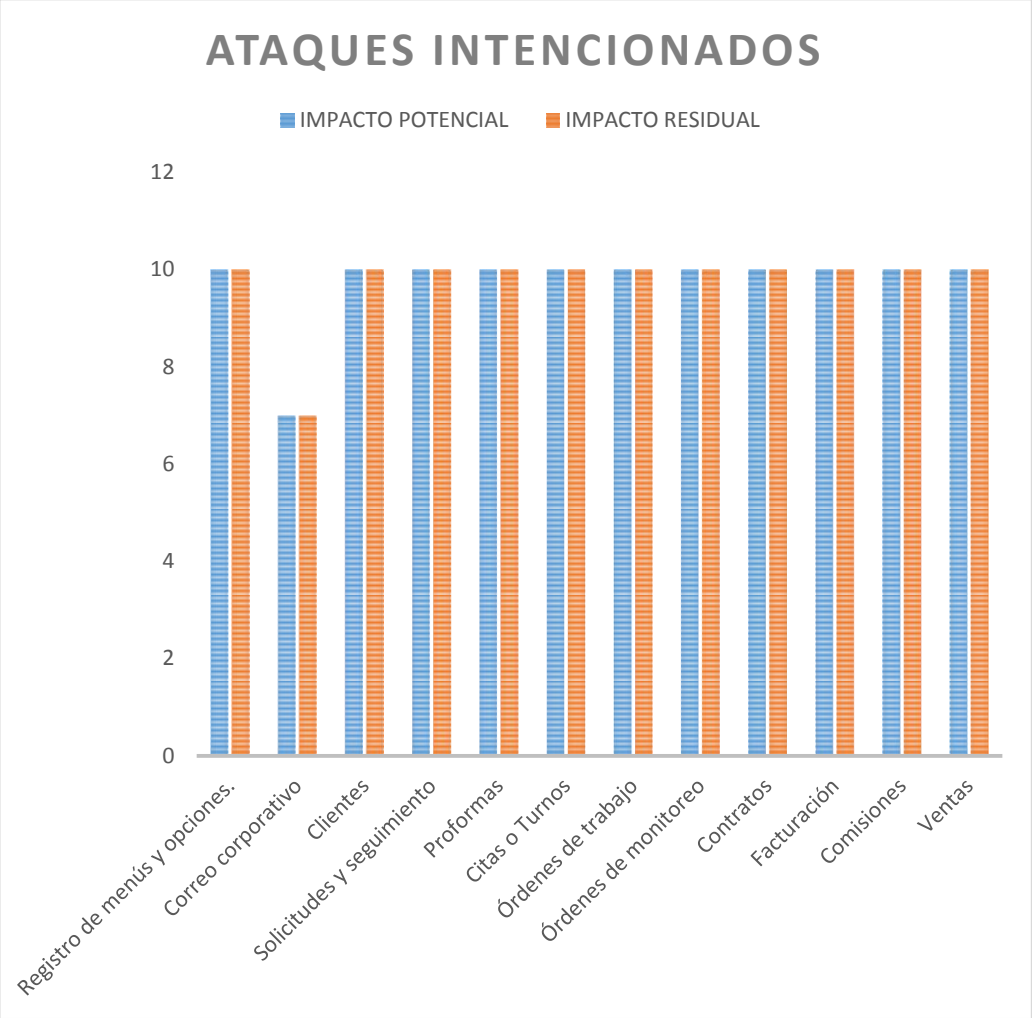

Figura 57. Estimación del Impacto por Ataques Intencionados

5.6.2. RESULTADOS DEL ANALISIS DE RIESGOS

Ante las amenazas:

Suplantación de la identidad del usuario, que afecta a los activos: Clientes, Solicitudes y seguimiento, Proformas, Citas o Turnos, Órdenes de trabajo, Órdenes de monitoreo, Contratos, Facturación, Comisiones, Ventas

RESULTADO: RIESGO CRITICO

Abuso de privilegios de acceso, que afecta a los activos: Clientes, Solicitudes y seguimiento, Proformas, Citas o Turnos, Órdenes de trabajo, Órdenes de monitoreo, Contratos, Facturación, Comisiones, Ventas.

Tienen salvaguardas implementadas para hacerles frente, pero su eficacia es Muy baja por lo que el RIESGO residual es igual al RIESGO Potencial sobre los activos.

RESULTADO: RIESGO CRITICO

Ante las amenazas:

Manipulación de la configuración que afecta al activo: Registro de menús y opciones.

RESULTADO: RIESGO CRITICO

Alteración de secuencia, que afecta al activo: Correo corporativo

RESULTADO: RIESGO CRITICO

Y Acceso no autorizado, que afecta a los activos: Clientes, Solicitudes y seguimiento, Proformas, Citas o Turnos, Órdenes de trabajo, Órdenes de monitoreo, Contratos, Facturación, Comisiones, Ventas

RESULTADO: RIESGO CRITICO.

No tienen salvaguardas para hacerles frente, debido a esto el RIESGO Potencial y Residual son iguales.

El gráfico se muestra que el Riesgo Potencial y el Riesgo Residual son iguales ante las amenazas indicadas anteriormente, en ambos tipos es un Riesgo Critico.

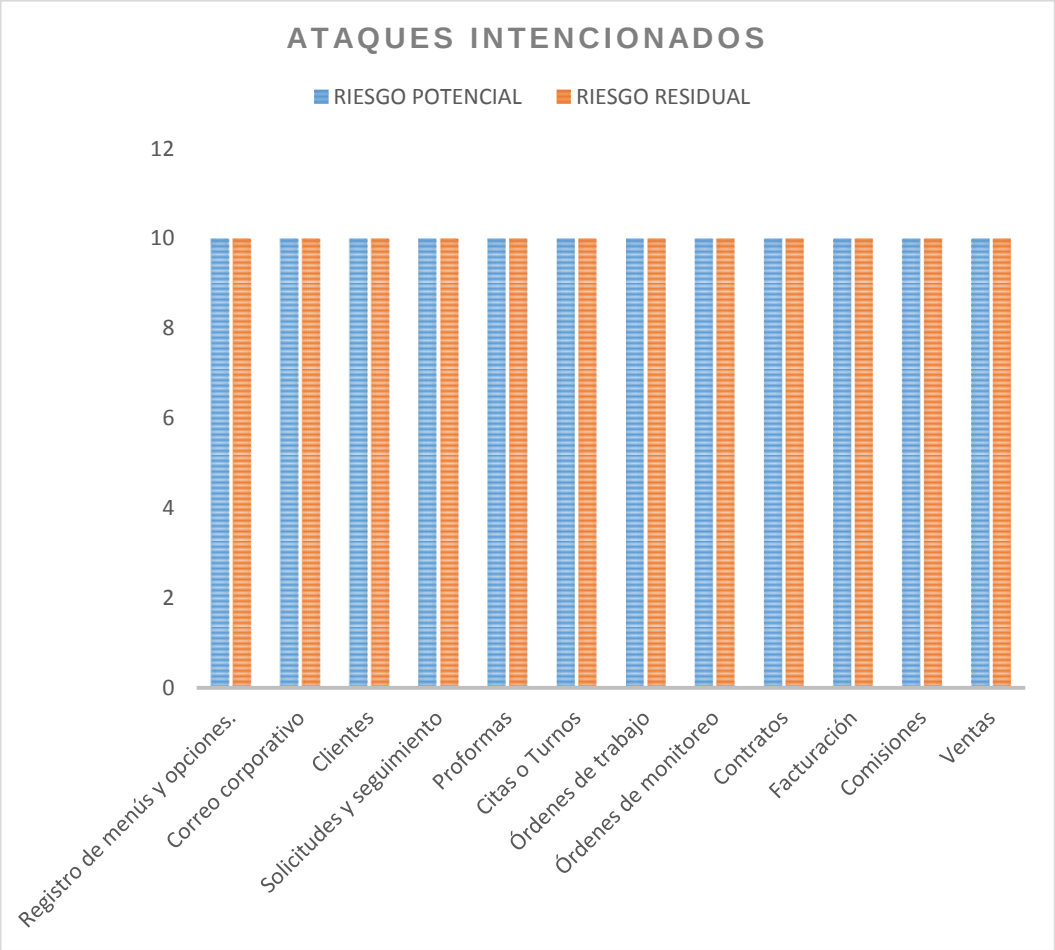

Figura 58. Estimación del Riesgo por Ataques Intencionados

5.6.3. RESULTADO ANALISIS DE IMPACTO POR USO NO PREVISTO

Ante la amenaza Uso no previsto, existe implementada una salvaguarda altamente eficaz para hacerle frente, por lo que el IMPACTO RESIDUAL se considera Despreciable sobre los activos con Respecto al IMPACTO POTENCIAL, esto se muestra claramente en el gráfico.

RESULTADO: IMPACTO MUY BAJO

Figura 59. Estimación del Impacto por Uso no Previsto

5.6.4. RESULTADO ANALISIS DE RIESGO POR USO NO PREVISTO

Ante la amenaza Uso no previsto, existe implementada una salvaguarda altamente eficaz para hacerle frente, por lo que el RIESGO RESIDUAL que tienen los activos en que se materialice la amenaza se considera Despreciable con Respecto al RIESGO POTENCIAL, esto se muestra claramente en el gráfico.

RESULTADO: RIESGO DESPRECIABLE

Figura 60. Estimación del Riesgo por Uso no Previsto

5.7. ESTIMACION DEL ESTADO DEL RIESGO POR ATAQUES INTENCIONADOS

5.7.1. RESULTADO DE ANALISIS DE IMPACTO

Ante la amenaza:

Repudio, que afecta los activos: Clientes, Solicitudes y seguimiento, Proformas, Citas o Turnos, Órdenes de trabajo, Órdenes de monitoreo, Contratos, Facturación, Comisiones, y Ventas.

Tiene una salvaguarda 60% eficaz, por lo que el IMPACTO RESIDUAL es menor con respecto al IMPACTO POTENCIAL.

RESULTADO: IMPACTO MUY ALTO

Ante la amenaza:

Destrucción de información que afecta a las Bases de Datos, y **Modificación deliberada** que afecta a significativamente a Registros de auditoría, e Información del cliente vehículos, No tienen salvaguardas que se pueden hacer frente por lo Impacto Residual y el Impacto Potencial es el mismo sobre estos activos.

RESULTADO: IMPACTO MUY ALTO

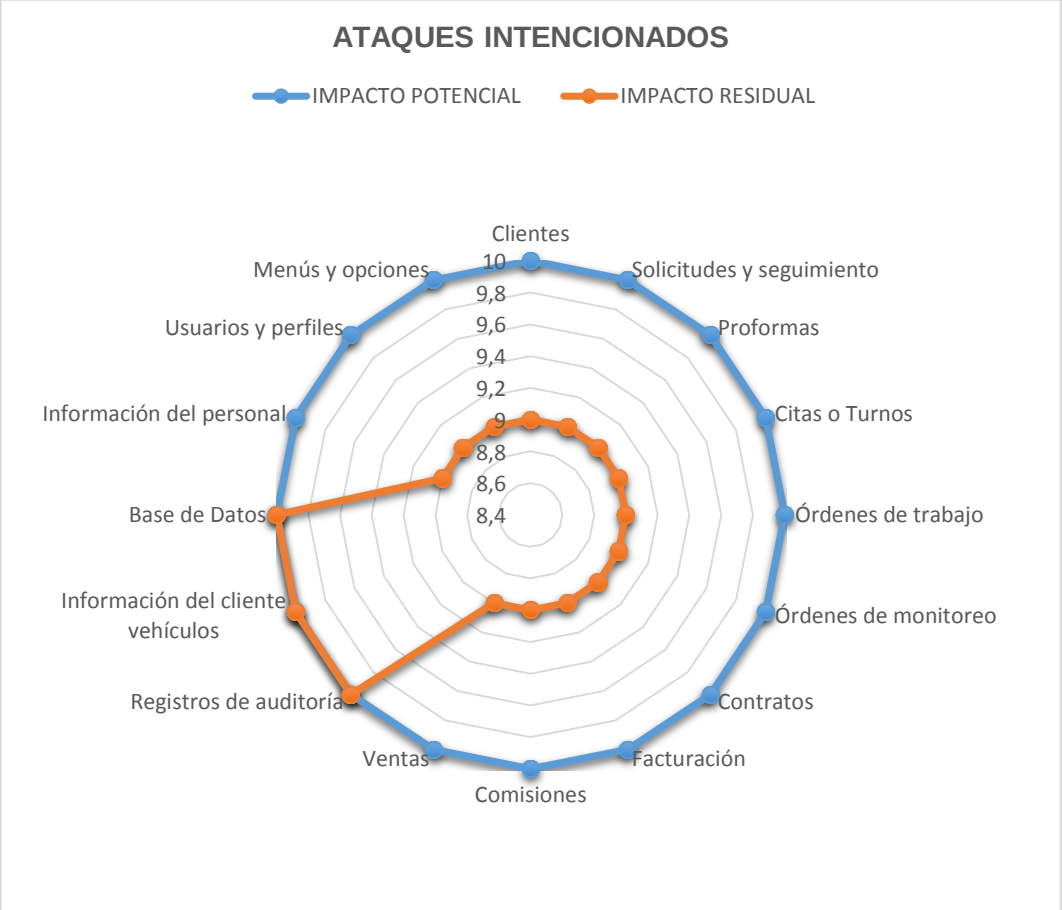

Figura 61. Estimación del Impacto por Ataques Intencionados

5.7.2. RESULTADO DEL ANALISIS DE RIESGOS

Ante la amenaza:

Repudio, que afecta los activos: Clientes, Solicitudes y seguimiento, Proformas, Citas o Turnos, Órdenes de trabajo, Órdenes de monitoreo, Contratos, Facturación, Comisiones, y Ventas.

Tiene una salvaguarda 60% eficaz, por lo que el impacto residual es menor con respecto al Impacto Potencial, pero no lo significativamente para poner disminuir el Riesgo, por lo que el Riesgo Potencial y Residual son iguales, estos activos tienen un Riesgo Critico.

RESULTADO: RIESGO CRITICO

Ante la amenaza:

Destrucción de información que afecta a las Bases de Datos, y **Modificación deliberada** que afecta a significativamente a Registros de auditoría, e Información del cliente vehículos, No tienen salvaguardas que se pueden hacer frente por lo Impacto Residual y el Impacto Potencial es el mismo sobre estos activos, y también tienen un Riesgo Critico.

RESULTADO: RIESGO CRITICO

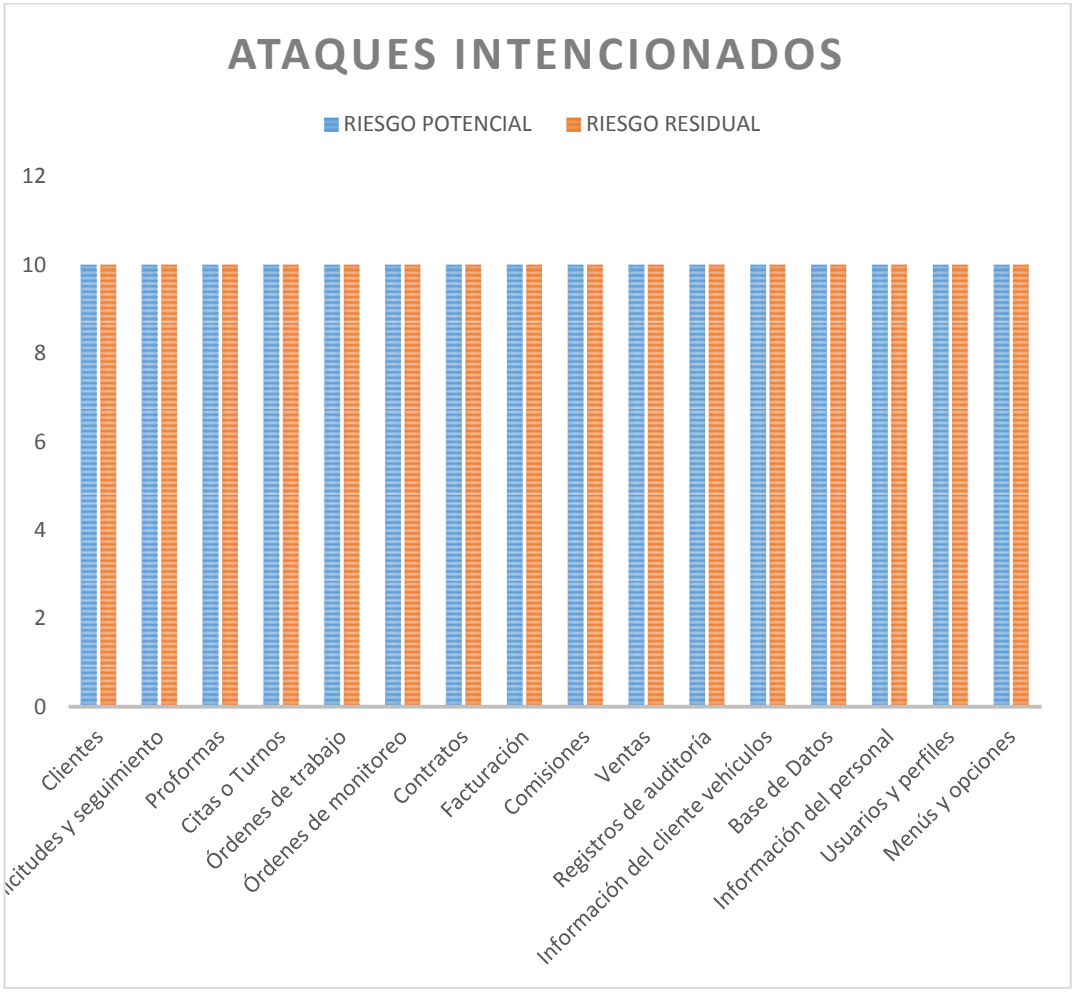

Figura 62. Estimación del Riesgo por Ataques Intencionados

5.8. ESTIMACION DEL ESTADO DEL RIESGO POR MANIPULACION DE PROGRAMA

5.8.1. RESULTADO DE ANALISIS DE IMPACTO

Ante la amenaza, manipulación de programas, hay una salvaguarda para hacerle frente pero eficazmente muy baja, por lo que el Impacto sobre los activos tanto RESIDUAL como POTENCIAL, es el mismo.

RESULTADO: IMPACTO MUY ALTO

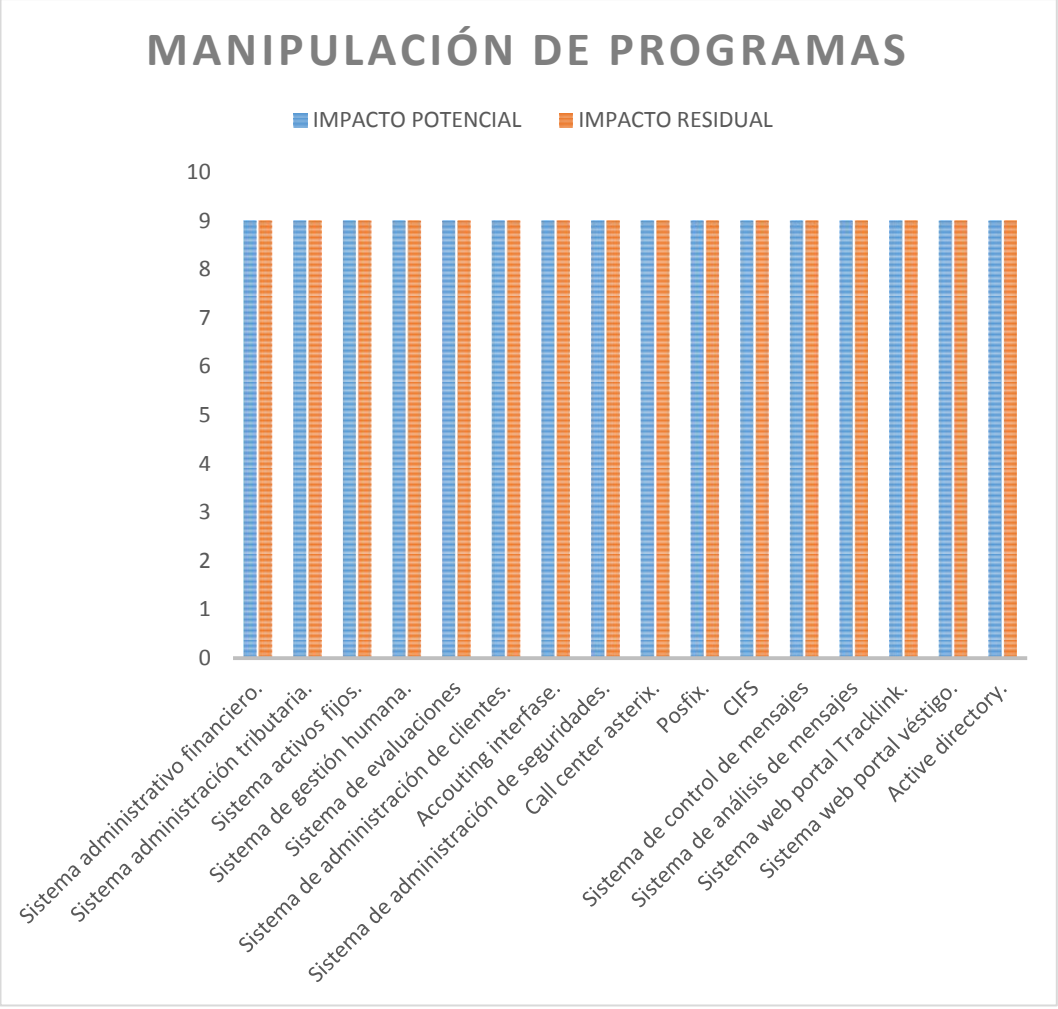

Figura 63. Estimación del Impacto por Manipulación de Programas

5.8.2. RESULTADO DE ANALISIS DE RIESGO

Ante la amenaza, Manipulación de programas, hay una salvaguarda para hacerle frente pero eficazmente muy baja, por lo que el RIESGO sobre los activos tanto RESIDUAL como POTENCIAL, es el mismo.

RESULTADO: RIESGO CRITICO

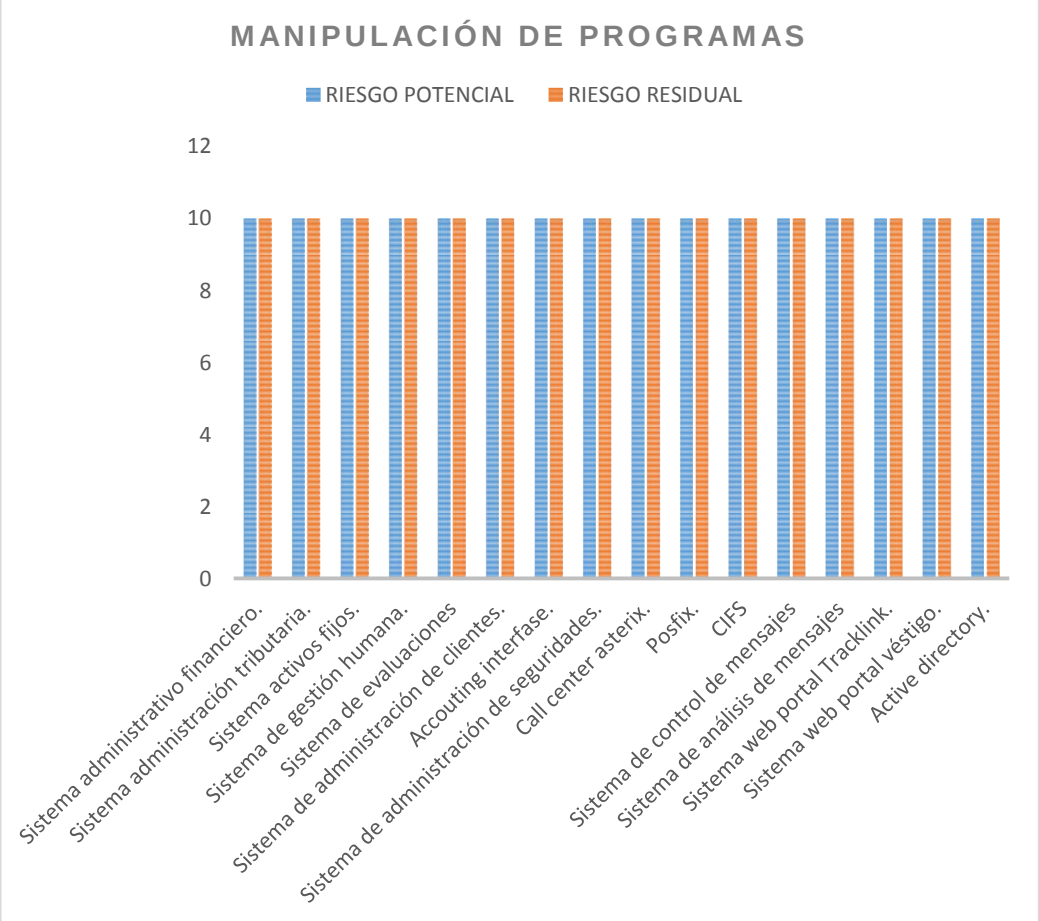

Figura 64. Estimación del Riesgo por Manipulación de Programas

CAPÍTULO 6.- CONCLUSIONES Y RECOMENDACIONES

6.1. CONCLUSIONES

- Al finalizar el análisis de riesgos utilizando Magerit como metodología de análisis de Riesgos, se determinaron vulnerabilidades en el Sistema de información de la empresa, que deben ser atendidas oportunamente, ya que la mayoría de activos están con Riesgo Critico y con Impacto Muy Alto.

– Hacer un análisis de riesgos es esencial en los sistemas de información, ya que estos siempre están expuestos a amenazas.

– La Metodología de Análisis de Riesgos de Sistemas de Información MAGERIT, junto con los Objetivos de Control para la Tecnología de la Información COBIT 5, contribuye a reducir las amenazas y brechas existentes entre los objetivos del negocio y aspectos técnicos de los Sistemas de Información.

– El hacer una Análisis de Riesgos permite detectar la situación real de la compañía.

6.2. RECOMENDACIONES

– Concientizar a los directivos de la compañía la importancia de ejecutar una Gestión de los Riesgos encontrados, los mismos que si no son atendidos oportunamente se van a tener consecuencias No deseadas.

– Promover en el personal de la empresa, la toma de conciencia sobre el manejo de los riesgos.

- Tomar las medidas de Seguridad y aplicar los objetivos de control que mitiguen el riesgo existente.

BIBLIOGRAFIA.

Dirección General de Modernización Administrativa, P. e. (2012). *MAGERIT - version 3.0.* Madrid, España: Ministerio de Hacienda y Administraciones Públicas de España.

Ibarra, J. Á. (2 de Marzo de 2010). *Eventos: ISACA.* Recuperado el 5 de Agosto de 2013, de sitio web de ISACA: http://www.isaca.org/chapters7/Monterrey/Events/Documents/20100302%20Metodolog%C3%ADas%20de%20Riesgos%20TI.pdf

Institute, I. G. (2007). *COBIT® 4.1.* Rolling Meadows, Illinois, Estados unidos: Institute, IT Governance.

Kurt Dillard (MSS), Jared Pfost (SCOE). (15 de Octubre de 2004). *Guía de administración de riesgos de seguridad: Microsoft.* Recuperado el 05 de Agosto de 2013, de Michosoft Technet: http://www.microsoft.com/spain/technet/recursos/articulos/ack_page.mspx

ANEXOS

A continuación se presenta un extracto de los procesos de Cobit 5 relacionados con el Objetivo Optimización del Riesgo:

Objetivos de la Empresa y las Métricas de TI:

Dimensión Financiera

Cumplimiento de Leyes y Regulaciones Externas

1. Coste de incumplimientos TI, incluyendo acuerdos y sanciones e impacto en pérdida de reputación
2. Número de incumplimientos TI reportados al Consejo de Administración o causantes de comentarios o vergüenza públicos
3. Número de incumplimientos relacionados con proveedores de servicios TI.
4. Cobertura de evaluaciones de cumplimiento

Riesgos de Negocio Gestionados (salvaguarda de activos).

1. Porcentaje de procesos TI de negocio críticos, servicios TI y programas de negocio habilitados por TI cubiertos por evaluaciones de riesgo.
2. Número de incidentes TI significativos que no fueron identificados en evaluaciones de riesgos.
3. Porcentaje de evaluaciones de riesgo corporativas que incluyen riesgo TI.
4. Frecuencia de actualización del perfil de riesgo.

Dimensión Cliente

Entrega de servicios de TI de acuerdo a los requisitos del negocio

1. Número de interrupciones de negocio debidas a incidentes de servicios TI.
2. Porcentaje de partes interesadas en el negocio satisfechas de que la entrega de servicios TI cumpla los niveles de servicio acordados.
3. Porcentaje de usuarios satisfechos con la calidad de la entrega de servicios TI.

Interna

Seguridad de la información, infraestructuras de procesamiento y aplicaciones.

1. Número de incidentes de seguridad causantes de pérdidas financieras, interrupción del negocio o vergüenza pública
2. Número de servicios TI sin requerimientos de seguridad destacables
3. Tiempo de concesión, cambio y eliminación de privilegios de acceso comparado con los niveles de servicio acordados.
4. Frecuencia de las evaluaciones de seguridad en relación a los últimos estándares y guías.

Cumplimiento con las políticas internas por parte de las TI.

1. Número de incidentes relacionados con el incumplimiento de políticas
2. Porcentaje de interesados que entienden las políticas
3. Porcentaje de políticas apoyadas por estándares y prácticas de trabajo efectivas.
4. Frecuencia de revisión y actualización de políticas.

OPTIMIZACION DEL RIESGO Y EL GOBIERNO DE TI

De acuerdo con el modelo de referencia de Procesos de Cobit 5, los procesos de gobierno deben preocuparse por el logro de los objetivos de gobierno y entre ellos la Optimización del Riesgo. En este sentido se

requiere que la dirección de TI se preocupe de Evaluar, Orientar y Supervisar.

EDM03 Asegurar la Optimización del Riesgo

Consiste en asegurar que el apetito y la tolerancia al riesgo de la empresa son entendidos, articulados y comunicados y que el riesgo para el valor de la empresa relacionado con el uso de las TI es identificado y gestionado.

Prácticas de Gobierno:

EDM03.01 Evaluar la gestión de riesgos.

Examinar y evaluar continuamente el efecto del riesgo sobre el uso actual y futuro de las TI en la empresa. Considerar si el apetito de riesgo de la empresa es apropiado y el riesgo sobre el valor de la empresa relacionado con el uso de TI es identificado y gestionado.

Actividades:

1. Determinar el nivel de riesgos relacionados con las TI que la empresa está dispuesta a asumir para cumplir con sus objetivos (apetito de riesgo).
2. Evaluar y aprobar propuestas de umbrales de tolerancia al riesgo TI frente a los niveles de riesgo y oportunidad aceptables por la empresa.
3. Determinar el grado de alineación de la estrategia de riesgos de TI con la estrategia de riesgos empresariales.
4. Evaluar proactivamente los factores de riesgo TI con anterioridad a las decisiones estratégicas de la empresa pendientes y asegurar que las decisiones de la empresa se toman conscientes de los riesgos.

5. Determinar si el uso de TI está sujeto a una valoración y evaluación de riesgos adecuada, según lo descrito en estándares nacionales e internacionales relevantes.

6. Evaluar las actividades de gestión de riesgos para garantizar su alineamiento con las capacidades de la empresa para las perdidas relacionadas con TI y la tolerancia de los líderes a los mismos.

EDM03.02 Orientar la gestión de riesgos.

Orientar el establecimiento de prácticas de gestión de riesgos para proporcionar una seguridad razonable de que son apropiadas para asegurar que riesgo TI actual no excede el apetito de riesgo del Consejo.

Actividades:

1. Promover una cultura consciente de los riesgos TI e impulsar a la empresa a una identificación proactiva de riesgos TI, oportunidades e impactos potenciales en el negocio.

2. Orientar la integración de las operaciones y la estrategia de riesgos de TI con las decisiones y operaciones empresariales estratégicas.

3. Orientar la elaboración de planes de comunicación de riesgos (cubriendo todos los niveles de la empresa), así como los planes de acción de riesgo.

4. Orientar la implantación de mecanismos apropiados para responder rápidamente a los riesgos cambiantes y notificar inmediatamente a los niveles adecuados de gestión, soportados principios de escalado acordados (qué informar, cuándo, dónde y cómo).

5. Orientar para que el riesgo, las oportunidades, los problemas y preocupaciones puedan ser identificadas y notificadas por cualquier persona en cualquier momento. El riesgo debe ser gestionado de acuerdo con las políticas y procedimientos publicados y escalados a los decisores relevantes.

6. Identificar los objetivos e indicadores clave de los procesos de gobierno y gestión de riesgos a ser monitorizados y aprobar los enfoques, métodos, técnicas y procesos para capturar y notificar la información de medición.

EDM03.03 Supervisar la gestión de riesgos.

Supervisar los objetivos y las métricas clave de los procesos de gestión de riesgo y establecer cómo las desviaciones o los problemas serán identificados, seguidos e informados para su resolución.

Actividades:

1. Supervisar hasta qué punto se gestiona el perfil de riesgo dentro de los umbrales de apetito de riesgo.
2. Supervisar las metas y métricas clave de gestión de los procesos de gobierno y gestión del riesgo respecto a los objetivos, analizar las causas de las desviaciones e iniciar medidas correctivas para abordar las causas subyacentes.
3. Facilitar la revisión por las principales partes interesadas del progreso de la empresa hacia los objetivos identificados.
4. Informar cualquier problema de gestión de riesgos al Consejo o al Comité de Dirección.

OPTIMIZACION DEL RIESGO Y LA GESTION DE TI

De acuerdo con el modelo de referencia de Procesos de Cobit 5, existen cuatro dominios para la gestión de TI que proporcionan cobertura de extremo a extremo:

- Alinear, Planificar Organizar (APO).
- Construir Adquirir e Implementar (BAI).
- Entregar, dar Servicio y Soporte (DSS).

- Supervisar Evaluar y Valorar (MEA).

Dentro de estos dominios nos enfocaremos en los procesos relacionados con la Optimización del Riesgo.

APO12 Gestionar el Riesgo

Consiste en Identificar, Evaluar y reducir los riesgos relacionados con TI de forma continua, dentro de niveles de tolerancia establecidos por la dirección ejecutiva de la empresa. Integrar la gestión de riesgos empresariales relacionados con TI con la gestión de riesgos empresarial general (ERM) y equilibrar los costes y beneficios de gestionar riesgos empresariales relacionados con TI.

Prácticas de Gestión:

APO12.01 Recopilar datos.

Identificar y recopilar datos relevantes para catalizar una identificación, análisis y notificación efectiva de riesgos relacionados con TI.

Actividades:

1. Establecer y mantener un método para la recogida, clasificación y análisis de datos relacionados con riesgo de TI, dando cabida a múltiples tipos de eventos, múltiples categorías de riesgo de TI y múltiples factores de riesgo.
2. Registrar datos relevantes sobre el entorno de operación interno y externo de la empresa que pudieran jugar un papel significativo en la gestión del riesgo de TI.
3. Medir y analizar los datos históricos de riesgo de TI y de pérdidas experimentadas tomados de datos y tendencias externas disponibles,

empresas similares de la industria – basados en eventos registrados, bases de datos y acuerdos de la industria sobre divulgación de eventos comunes.

4. Registrar datos sobre eventos de riesgo que han causado o pueden causar impactos al beneficio/valor facilitado por TI, a la entrega de programas y proyectos de TI y/o a las operaciones y entrega de servicio de TI. Capturar datos relevantes sobre asuntos relacionados, incidentes, problemas e investigaciones.

5. Para clases o eventos similares, organizar los datos recogidos y destacar factores contribuyentes. Determinar los factores contribuyentes comunes para eventos múltiples.

6. Determinar las condiciones específicas que existían o faltaban cuando ocurrieron los eventos de riesgo y la forma en la cual las condiciones afectaban la frecuencia del evento y la magnitud de la pérdida.

7. Ejecutar análisis periódicos de eventos y de factores de riesgo para identificar asuntos nuevos o emergentes relacionados con el riesgo y para obtener un entendimiento de los asociados factores de riesgo internos y externos.

APO12.02 Analizar el riesgo.

Desarrollar información útil para soportar las decisiones relacionadas con el riesgo que tomen en cuenta la relevancia para el negocio de los factores de riesgo.

Actividades:

1. Definir la amplitud y profundidad apropiada para los esfuerzos en análisis de riesgos, considerando todos los factores de riesgo y la criticidad en el negocio de los activos. Establecer el alcance del análisis de riesgos después de llevar a cabo un análisis coste-beneficio.

2. Construir y actualizar regularmente escenarios de riesgo de TI, que incluyan escenarios compuestos en cascada y/o tipos de amenaza

coincidentes y desarrollar expectativas para actividades de control específicas, capacidades para detectar y otras medidas de respuesta.

3. Estimar la frecuencia y magnitud de pérdida o ganancia asociada con escenarios de riesgo de TI. Tener en cuenta todos los factores de riesgo que apliquen, evaluar controles operacionales conocidos y estimar niveles de riesgo residual.

4. Comparar el riesgo residual con la tolerancia al riesgo e identificar exposiciones que puedan requerir una respuesta al riesgo.

5. Analizar el coste-beneficio de las opciones de respuesta al riesgo potencial, tales como evitar, reducir/mitigar, transferir/compartir y aceptar y explotar/ capturar. Proponer la respuesta al riesgo óptima.

6. Especificar requerimientos de alto nivel para los proyectos o programas que implementarán las respuestas de riesgo seleccionadas. Identificar requerimientos y expectativas para los controles clave que son apropiados para las respuestas de mitigación de riesgos.

7. Validar los resultados de análisis de riesgos antes de usarlos para la toma de decisiones, confirmando que los análisis se alinean con requerimientos de empresa y verificando que las estimaciones fueron apropiadamente calibradas y examinadas ante una posible parcialidad.

APO12.03 Mantener un perfil de riesgo.

Mantener un inventario del riesgo conocido y atributos de riesgo (incluyendo frecuencia esperada, impacto potencial y respuestas) y de otros recursos, capacidades y actividades de control actuales relacionados.

Actividades:

1. Inventariar los procesos de negocio, incluyendo el personal de soporte, aplicaciones, infraestructura, instalaciones, registros manuales críticos, vendedores, proveedores y externalizados y documentar la

dependencia de los procesos de gestión de servicio TI y de los recursos de infraestructuras TI.

2. Determinar y acordar qué servicios TI y recursos de infraestructuras de TI son esenciales para sostener la operación de procesos de negocio. Analizar dependencias e identificar eslabones débiles.

3. Agregar escenarios de riesgo actuales, por categoría, línea de negocio y área funcional.

4. De forma regular, capturar toda la información sobre el perfil de riesgo y consolidarla dentro de un perfil de riesgo agregado.

5. Sobre la base de todos los datos del perfil de riesgo, definir un conjunto de indicadores de riesgo que permitan la identificación rápida y la supervisión del riesgo actual y las tendencias de riesgo.

6. Capturar información sobre eventos de riesgos de TI que se han materializado, para su inclusión en el perfil de riesgo de TI de la empresa.

7. Capturar información sobre el estado del plan de acción del riesgo, para la inclusión en el perfil de riesgo de TI de la empresa.

APO12.04 Expresar el riesgo.

Proporcionar información sobre el estado actual de exposiciones y oportunidades relacionadas con TI de una forma oportuna a todas las partes interesadas necesarias para una respuesta apropiada.

Actividades:

1. Informar de los resultados del análisis de riesgos a todas las partes interesadas afectadas en términos y formatos útiles para soportar las decisiones de empresa. Cuando sea posible, incluir probabilidades y rangos de pérdida o ganancia junto con niveles de confianza que permitan a la dirección equilibrar el retorno del riesgo.

2. Proporcionar a los responsables de toma de decisiones un entendimiento de los escenarios peor y más probables, exposiciones de

diligencia debida y consideraciones sobre la reputación, legales y regulatorias significativas.

3. Informar el perfil de riesgo actual a todas las partes interesadas, incluyendo la efectividad del proceso de gestión de riesgos, la efectividad de los controles, diferencias, inconsistencias, redundancias, estado de la remediación y sus impactos en el perfil de riesgo.

4. Revisar los resultados de evaluaciones objetivas de terceras partes, auditorías internas y revisiones del aseguramiento de la calidad y mapearlos con el perfil de riesgo. Revisar las diferencias y exposiciones identificadas para determinar la necesidad de análisis de riesgos adicionales.

5. De forma periódica, para áreas con un riesgo relativo y una paridad de capacidad del riesgo, identificar oportunidades relacionadas con TI que podrían permitir la aceptación de un mayor riesgo y un crecimiento y retorno mayores.

APO12.05 Definir un portafolio de acciones para la gestión de riesgos.

Gestionar las oportunidades para reducir el riesgo a un nivel aceptable como un portafolio.

Actividades

1. Mantener un inventario de actividades de control que estén en marcha para gestionar al riesgo y que permitan que el riesgo que se tome esté alineado con el apetito y tolerancia al riesgo. Clasificar las actividades de control y mapearlas con las declaraciones de riesgo específicas de TI y agrupaciones de riesgo de TI.

2. Determinar si cada entidad organizativa supervisa el riesgo y acepta la responsabilidad para operar dentro de sus niveles de tolerancia individuales y de portafolio.

3. Definir un conjunto de propuestas de proyecto equilibradas diseñadas para reducir el riesgo y/o proyectos que permitan oportunidades estratégicas

empresariales, considerando costes/beneficios, el efecto en el perfil de riesgo actual y las regulaciones.

APO12.06 Responder al riesgo

Responder de una forma oportuna con medidas efectivas que limiten la magnitud de pérdida por eventos relacionados con TI.

Actividades

1. Preparar, mantener y probar planes que documenten los pasos específicos a tomar cuando un evento de riesgo pueda causar un incidente significativo operativo o evolucionar en un incidente con un impacto de negocio grave. Asegurar que los planes incluyan vías de escalado a través de la empresa.
2. Categorizar los incidentes y comparar las exposiciones reales con los umbrales de tolerancia al riesgo. Comunicar los impactos en el negocio a los responsables de toma de decisiones como parte de la notificación y actualizar el perfil de riesgo.
3. Aplicar el plan de respuesta apropiado para minimizar el impacto cuando ocurren incidentes de riesgo.
4. Examinar eventos adversos/pérdidas del pasado y oportunidades perdidas y determinar sus causas raíz. Comunicar la causa raíz, requerimientos de respuesta adicionales para el riesgo y mejoras de proceso a los responsables de toma de decisiones apropiados y asegurarse de que la causa, los requerimientos de respuesta y la mejora del proceso se incluyan en los procesos de gobierno del riesgo.

APO13 Gestionar la Seguridad

Definir, operar y supervisar un sistema para la gestión de la seguridad de la información.

APO13.01 Establecer y mantener un SGSI.

Establecer y mantener un SGSI que proporcione un enfoque estándar, formal y continuo a la gestión de seguridad para la información, tecnología y procesos de negocio que esté alineados con los requerimientos de negocio y la gestión de seguridad en la empresa.

Actividades:

1. Definir el alcance y los límites del SGSI en términos de las características de la empresa, la organización, su localización, activos y tecnología. Incluir detalles de y justificación para, cualquier exclusión del alcance.
2. Definir un SGSI de acuerdo con la política de empresa y alineada con la empresa, la organización, su localización, activos y tecnología.
3. Alinear el SGSI con el enfoque global de la gestión de la seguridad en la empresa.
4. Obtener autorización de la dirección para implementar y operar o cambiar el SGSI.
5. Preparar y mantener una declaración de aplicabilidad que describa el alcance del SGSI.
6. Definir y comunicar los roles y las responsabilidades de la gestión de la seguridad de la información.
7. Comunicar el enfoque de SGSI.

APO13.02 Definir y gestionar un plan de tratamiento del riesgo de la seguridad de la información.

Mantener un plan de seguridad de información que describa cómo se gestionan y alinean los riesgos de seguridad de información con la estrategia y la arquitectura de empresa. Asegurar que las recomendaciones para implementar las mejoras en seguridad se basan en casos de negocio aprobados, se implementan como parte integral del desarrollo de soluciones y servicios y se operan, después, como parte integral de las operaciones del negocio.

Actividades

1. Formular y mantener un plan de tratamiento de riesgos de seguridad de la información alineado con los objetivos estratégicos y la arquitectura de la empresa. Asegurar que el plan identifica las prácticas de gestión y las soluciones de seguridad apropiadas y óptimas, con los recursos, las responsabilidades y las prioridades asociadas para gestionar los riegos identificados de seguridad de información.
2. Mantener un inventario de componentes de la solución implementados para gestionar los riesgos relacionados con la seguridad como parte de la arquitectura de la empresa.
3. Desarrollar propuestas para implementar el plan de tratamiento de riesgos de seguridad de la información, sustentados en casos de negocio adecuados que incluyan consideren la financiación la asignación de roles y responsabilidades.
4. Proporcionar información para el diseño y desarrollo de prácticas de gestión y soluciones seleccionadas en base al plan de tratamiento de riesgos de seguridad de información.
5. Definir la forma de medición de la efectividad de las prácticas de gestión seleccionadas y especificar la forma de utilizar estas mediciones para evaluar la efectividad y producir resultados reproducibles y comparables.

6. Recomendar programas de formación y concienciación en seguridad de la información.

7. Integrar la planificación, el diseño, la implementación y la supervisión de los procedimientos de seguridad de información y otros controles que permitan la prevención y detección temprana de eventos de seguridad, así como la respuesta a incidentes de seguridad.

APO13.03 Supervisar y revisar el SGSI.

Mantener y comunicar regularmente la necesidad y los beneficios de la mejora continua de la seguridad de información. Recolectar y analizar datos sobre el SGSI y la mejora de su efectividad. Corregir las no conformidades para prevenir recurrencias. Promover una cultura de seguridad y de mejora continua.

Actividades

1. Realizar revisiones periódicas del SGSI, incluyendo aspectos de políticas, objetivos y prácticas de seguridad del SGSI. Considerar los resultados de auditorías de seguridad, incidentes, resultados de mediciones de efectividad, sugerencias y retroalimentación de todas las partes interesadas.

2. Realizar auditorías internas al SGSI a intervalos planificados.

3. Realizar revisiones periódicas del SGSI por la Dirección para asegurar que el alcance sigue siendo adecuado y que se han identificado mejoras en el proceso del SGSI.

4. Proporcionar información para el mantenimiento de los planes de seguridad para que consideren las incidencias de las actividades de supervisión y revisión periódica.

5. Registrar las acciones y los eventos que podrían tener un impacto en la efectividad o el desempeño del SGSI.

BAI09 Gestionar Los Activos

Gestionar los activos de TI a través de su ciclo de vida para asegurar que su uso aporta valor a un coste óptimo, que se mantendrán en funcionamiento (acorde a los objetivos), que están justificados y protegidos físicamente, y que los activos que son fundamentales para apoyar la capacidad del servicio son fiables y están disponibles. Administrar las licencias de software para asegurar que se adquiere el número óptimo, se mantienen y despliegan en relación con el uso necesario para le negocio y que el software instalado cumple con los acuerdos de licencia.

Prácticas de Gestión:

BAI09.01 Identificar y registrar los activos actuales.

Mantener un registro actualizado y exacto de todos los activos de TI necesarios para la prestación de servicios y garantizar su alineación con la gestión de la configuración y la administración financiera.

Actividades

1. Identificar todos los activos en propiedad en un registro que indique el estado actual. Mantener su alineación con los procesos de gestión de cambios y de la configuración, el sistema de gestión de la configuración y los registros contables financieros.
2. Identificar los requisitos legales, reglamentarios o contractuales que deben ser abordados en la gestión de los activos.
3. Verificar la existencia de todos los activos en propiedad mediante la realización periódica de controles de inventario físicos y lógicos y su conciliación, incluyendo la utilización de herramientas software de descubrimiento.
4. Comprobar que los activos se adecuan a sus objetivos (p.ej., están en condiciones útiles).

5. Determinar de forma regular si cada activo continúa proporcionando valor y, si es así, estimar la vida útil prevista de dicha validez.

6. Asegurar la contabilización de todos los activos.

BAI09.02 Gestionar Activos Críticos.

Identificar los activos que son críticos en la provisión de capacidad de servicio y dar los pasos para maximizar su fiabilidad y disponibilidad para apoyar las necesidades del negocio.

Actividades

1. Identificar los activos que son críticos en la provisión de la capacidad del servicio refiriéndose a los requisitos en las definiciones de servicio, ANSs y el sistema de gestión de la configuración.

2. Supervisar el rendimiento de los activos críticos examinando las tendencias de incidentes y, en caso necesario, tomar medidas para reparar o reemplazar.

3. De forma regular, considerar el riesgo de fallo o necesidad del reemplazo de cada activo crítico.

4. Mantener la resiliencia de los activos críticos mediante la aplicación de un mantenimiento preventivo regular, de supervisión del rendimiento y, si fuera necesario, proporcionando alternativas y/o activos adicionales para reducir la probabilidad de fallo. 5. Establecer un plan de mantenimiento preventivo para todo el hardware, considerando un análisis coste-beneficio, recomendaciones del proveedor, el riesgo de interrupción del servicio, personal cualificado y otros factores relevantes.

5. Establecer contratos de mantenimiento que impliquen el acceso de terceros a las instalaciones de TI de la organización para actividades in situ y fuera del sitio (p. ej. externalización). Establecer contratos formales de servicio que contengan o se refieran a todas las condiciones de seguridad necesarias, incluidos los procedimientos de autorización de acceso, para

garantizar el cumplimiento de las políticas y estándares de seguridad de la organización.

6. Comunicar a los clientes y los usuarios afectados el impacto esperado (p. ej., las restricciones de rendimiento) de las actividades de mantenimiento.

7. Asegurar que los servicios de acceso remoto y perfiles de usuario (u otros medios utilizados para el mantenimiento o diagnóstico) están activos sólo cuando sea necesario.

8. Incorporar el tiempo de inactividad previsto en general en el calendario de producción, y programar las actividades de mantenimiento para minimizar el impacto adverso en los procesos de negocio.

BAI09.03 Gestionar el ciclo de vida de los activos.

Gestionar los activos desde su adquisición hasta su eliminación para asegurar que se utilizan tan eficaz y eficientemente como sea posible y son contabilizados y protegidos físicamente

Actividades

1. Adquirir todos los activos basándose en solicitudes aprobadas y de acuerdo con las políticas y las prácticas de adquisición de la empresa.

2. Identificar el origen, recibir, verificar, probar y registrar todos los activos de una manera controlada, incluyendo el etiquetado físico, si fuera necesario.

3. Aprobar los pagos y completar el proceso con proveedores según las condiciones acordadas por contrato.

4. Desplegar los activos siguiendo el ciclo de vida de implementación estándar, incluyendo la gestión de cambios y pruebas de aceptación.

5. Asignar activos a los usuarios, con aceptación y firma de responsabilidades, según corresponda.

6. Reasignar los activos siempre que sea posible cuando ya no sean necesarios debido a un cambio de función de rol del usuario, redundancia dentro de un servicio o finalización de un servicio.

7. Eliminar los activos cuando no sirvan a ningún propósito útil debido a la finalización de todos los servicios relacionados, tecnología obsoleta o falta de usuarios.

8. Eliminar los activos de forma segura, teniendo en cuenta, por ejemplo, la eliminación permanente de los datos registrados en dispositivos y posibles daños al medio ambiente.

9. Planificar, autorizar y realizar las actividades relacionadas con la finalización de uso, manteniendo los registros apropiados para satisfacer las necesidades regulatorias y cambiantes del negocio.

BAI09.04 Optimizar el coste de los activos.

Revisar periódicamente la base global de activos para identificar maneras de optimizar los costes y mantener el alineamiento con las necesidades del negocio.

Actividades:

1. Revisar la base general de activos de forma regular, teniendo en cuenta si está alineada con los requerimientos del negocio.

2. Evaluar los costes de mantenimiento, considerar si son razonables e identificar opciones de menor coste, incluyendo, cuando sea necesario, el reemplazo con nuevas alternativas.

3. Revisar las garantías y considerar la relación calidad-precio y estrategias de reemplazo para determinar opciones de menor coste.

4. Revisar la base general para identificar oportunidades de normalización, abastecimiento único y otras estrategias que pueden disminuir los costes de adquisición, soporte y mantenimiento.

5. Usar estadísticas de capacidad y utilización para identificar activos infrautilizados o redundantes que pudieran ser considerados para su eliminación o sustitución por otro con menores costes.

6. Revisar el estado general para identificar las oportunidades para aprovechar tecnologías emergentes o estrategias de aprovisionamiento alternativas para reducir los costes o incrementar el valor del dinero.

BAI09.05 Administrar Licencias.

Administrar las licencias de software de forma que se mantenga el número óptimo de licencias para soportar los requerimientos de negocio y el número de licencias en propiedad sea suficiente para cubrir el software instalado y en uso.

Actividades

1. Mantener un registro de todas las licencias de software adquiridas y sus acuerdos de licencia asociados.
2. De forma regular, llevar a cabo una auditoría para identificar a todos las copias de software instalado con licencia.
3. Comparar el número de copias de software instalado con el número de licencias en propiedad.
4. Cuando las copias sean inferiores al número en propiedad, decidir si existe una necesidad de mantener o cancelar licencias, considerando el potencial de ahorrar en mantenimiento innecesario, formación y otros gastos.
5. Cuando las copias sean superiores al número en propiedad, considerar primero la posibilidad de desinstalar copias que no sean ya necesarias o no estén justificadas, y después, si es necesario, adquirir licencias adicionales para cumplir con los acuerdos de licencia.
6. De forma regular, considerar si se puede obtenerse un mejor valor mediante la actualización de productos y licencias asociadas

BA10 Gestionar la Configuración

Definir y mantener las definiciones y relaciones entre los principales recursos y capacidades necesarias para la prestación de los servicios

proporcionados por TI, incluyendo la recopilación de información de configuración, el establecimiento de líneas de referencia, la verificación y auditoría de la información de configuración y la actualización del repositorio de configuración.

Prácticas de Gestión:

BAI10.01 Establecer y mantener un modelo de configuración.

Establecer y mantener un modelo lógico de la infraestructura, activos y servicios y la forma de registrar los elementos de configuración (CIs del inglés, configuration items) y las relaciones entre ellos. Incluyendo los CIs considerados necesarios para gestionar eficazmente los servicios y proporcionar una sola descripción fiable de los activos en un servicio.

Actividades

1. Definir y acordar el alcance y nivel de detalle para la gestión de la configuración (p.ej., qué servicios, activos y elementos configurables de la infraestructura se incluyen).
2. Establecer y mantener un modelo lógico para la gestión de la configuración, incluyendo información sobre los tipos de elementos de configuración, atributos de los elementos de configuración, tipos de relaciones, atributos de relación y códigos de estado.

BAI10.02 Establecer y mantener un repositorio de configuración y una base de referencia.

Establecer y mantener un repositorio de gestión de la configuración y crear unas bases de referencia de configuración controladas.

Actividades:

1. Identificar y clasificar los elementos de configuración y rellenar el repositorio.

2. Crear, revisar y formalizar un acuerdo sobre las bases de referencia de configuración de un servicio, aplicación o infraestructura.

BAI10.03 Mantener y controlar los elementos de configuración.

Mantener un repositorio actualizado de elementos de configuración rellenado con los cambios.

Actividades:

1. Identificar regularmente todos los cambios en los elementos de configuración.

2. Revisar los cambios propuestos a los elementos de configuración respecto a la base de referencia para garantizar su integridad y precisión.

3. Actualizar los detalles de configuración con los cambios aprobados a los elementos de configuración.

4. Crear, revisar y formalizar acuerdos sobre los cambios en las líneas de referencia de configuración cuando sea necesario.

BAI10.04 Generar informes de estado y configuración.

Definir y elaborar informes de configuración sobre cambios en el estado de los elementos de configuración.

Actividades

1. Identificar cambios en el estado de los elementos de configuración y contrastarlo con la base de referencia.

2. Enlazar todos los cambios de configuración con las peticiones de cambio aprobadas para identificar cualquier cambio no autorizado. Informar de cambios no autorizados a la gestión de cambios.

3. Identificar requisitos de información de todas las partes interesadas, incluyendo contenido, frecuencia y medios. Generar informes según las necesidades identificadas.

BAI10.05 Verificar y revisar la integridad del repositorio de configuración.

Revisar periódicamente el repositorio de configuración y verificar la integridad y exactitud con respecto al objetivo deseado.

Actividades:

1. Verificar periódicamente los elementos de configuración en activo contra el repositorio de configuración comparando configuraciones físicas y lógicas, usando las herramientas apropiadas de descubrimiento, según sea necesario.

2. Informar y revisar todas las desviaciones de las correcciones o acciones aprobadas para eliminar los activos no autorizados.

3. Verificar periódicamente que todos los elementos físicos de configuración, tal como se definen en el repositorio, existen físicamente. Informar de cualquier desviación a la Dirección.

4. Establecer y revisar periódicamente el objetivo de completitud del repositorio de configuración basado en las necesidades del negocio.

5. Periódicamente comparar el grado de completitud y precisión respecto a los objetivos y tomar medidas correctivas, según sea necesario, para mejorar la calidad de los datos del repositorio.

DSS01 Gestionar Operaciones

Coordinar y ejecutar las actividades y los procedimientos operativos requeridos para entregar servicios de TI tanto internos como externalizados, incluyendo la ejecución de procedimientos operativos estándar predefinidos y las actividades de monitorización requeridas.

Prácticas de Gestión:

DSS01.01 Ejecutar procedimientos operativos.

Mantener y ejecutar procedimientos y tareas operativas de forma confiable y consistente.

Actividades

1. Desarrollar y mantener procedimientos operativos y actividades relacionadas para dar apoyo a todos los servicios entregados.
2. Mantener una programación de actividades operativas, ejecutar las actividades y gestionar el desempeño y rendimiento (throughput) de las actividades programadas.
3. Asegurar que se cumple con los estándares de seguridad aplicables para la recepción, procesamiento, almacenamiento y salida de datos de forma tal que se satisfagan los objetivos empresariales, la política de seguridad de la empresa y los requerimientos regulatorios.
4. Verificar que todos los datos esperados para su procesamiento sean recibidos y procesados por completo y de una forma precisa y oportuna. Entregar los resultados de acuerdo con los requisitos de la empresa. Dar soporte a las necesidades de reinicio y reprocesamiento. Asegurar que los usuarios reciben los resultados adecuados de una forma segura y oportuna.
5. Programar, realizar y registrar las copias de respaldo de acuerdo con las políticas y procedimientos establecidos.

DSS01.02 Gestionar servicios externalizados de TI.

Gestionar la operación de servicios externalizados de TI para mantener la protección de la información empresarial y la confiabilidad de la entrega del servicio.

Actividades:

1. Asegurar que los procesos de información se adhieren a los requerimientos de seguridad de la empresa y conformes con los contratos y ANSs con terceros que alojan o proveen servicios.
2. Asegurar que los requerimientos operativos del negocio y de procesamiento de TI, así como a las prioridades en la entrega del servicio se adhieren y son conformes a los contratos y ANSs con terceros que alojan o proveen servicios.
3. Integrar los procesos críticos de gestión interna de TI con los de los proveedores de servicios externalizados cubriendo, por ejemplo, la planificación de la capacidad y el rendimiento, la gestión del cambio, la gestión de la configuración, la gestión de peticiones de servicio y de incidentes, la gestión de problemas, la gestión de la seguridad, la continuidad del negocio y la monitorización y notificación del desempeño de los procesos.
4. Planificar la realización de auditorías y aseguramientos independiente de los entonos operativos de los proveedores de externalización (outsourcing) para confirmar que los requerimientos acordados están recibiendo el tratamiento adecuado.

DSS01.03 Supervisar la infraestructura de TI.

Supervisar la infraestructura TI y los eventos relacionados con ella. Almacenar la suficiente información cronológica en los registros de operaciones para permitir la reconstrucción, revisión y examen de las

secuencias de tiempo de las operaciones y las actividades relacionadas con el soporte a esas operaciones.

Actividades

1. Registrar eventos, identificando el nivel de información a ser grabada sobre la base de una consideración del riesgo y el rendimiento.
2. Identificar y mantener una lista de activos de infraestructura que necesiten ser monitorizados en base a la criticidad del servicio y la relación entre los elementos de configuración y los servicios que de ellos dependen.
3. Definir e implantar reglas que identifiquen y registren violaciones de umbral y condiciones de eventos. Encontrar un equilibrio entre la generación de eventos falsos menores y eventos significativos, de forma tal que los registros de eventos no estén sobrecargados con información innecesaria.
4. Producir registros de eventos y retenerlos por un periodo apropiado para asistir en investigaciones futuras.
5. Establecer procedimientos para supervisar los registros de eventos y llevar a cabo revisiones periódicas.
6. Asegurar que se crean oportunamente los tiques de incidente cuando la monitorización identifica desviaciones de los umbrales definidos.

DSS02 Gestionar Peticiones e Incidentes de Servicio

Proveer una respuesta oportuna y efectiva a las peticiones de usuario y la resolución de todo tipo de incidentes. Recuperar el servicio normal; registrar y completar las peticiones de usuario; y registrar, investigar, diagnosticar, escalar y resolver incidentes.

Prácticas de Gestión:

DSS02.01 Definir esquemas de clasificación de incidentes y peticiones de servicio.

Definir esquemas y modelos de clasificación de incidentes y peticiones de servicio.

Actividades:

1. Definir esquemas de clasificación y priorización de incidentes y peticiones de servicio y criterios para el registro de problemas, para asegurar enfoques consistentes en el tratamiento, informando a los usuarios y realizando análisis de tendencias.
2. Definir modelos de incidentes para errores conocidos con el fin de facilitar su resolución eficiente y efectiva.
3. Definir modelos de peticiones de servicio según el tipo de petición de servicio correspondiente para facilitar la auto-ayuda y el servicio eficiente para las peticiones estándar.
4. Definir reglas y procedimientos de escalamiento de incidentes, especialmente para incidentes importantes e incidentes de seguridad.
5. Definir fuentes de conocimiento de incidentes y peticiones y su uso.

DSS02.02 Registrar, clasificar y priorizar peticiones e incidentes.

Identificar, registrar y clasificar peticiones de servicio e incidentes, y asignar una prioridad según la criticidad del negocio y los acuerdos de servicio.

Actividades:

1. Registrar todos los incidentes y peticiones de servicio, registrando toda la información relevante de forma que pueda ser manejada de manera efectiva y se mantenga un registro histórico completo.
2. Para posibilitar análisis de tendencias, clasificar incidentes y peticiones de servicio identificando tipo y categoría.
3. Priorizar peticiones de servicio e incidentes según la definición de impacto en el negocio del ANS y la urgencia.

DSS02.03 Verificar, aprobar y resolver peticiones de servicio.

Seleccionar los procedimientos adecuados para peticiones y verificar que las peticiones de servicio cumplen los criterios de petición definidos.

Actividades

1. Verificar los derechos para realizar peticiones de servicio usando, cuando sea posible, un flujo de proceso predefinido y cambios estándar.
2. Obtener aprobación financiera y funcional o firmada, si se requiere, o aprobaciones predefinidas para cambios estándar acordados.
3. Completar las peticiones siguiendo el procedimiento de petición seleccionado, utilizando, cuando sea posible, menús automáticos de autoayuda y modelos de petición predefinidos para los elementos solicitados frecuentemente.

DSS02.04 Investigar, diagnosticar y localizar incidentes.

Identificar y registrar síntomas de incidentes, determinar posibles causas y asignar recursos a su resolución.

Actividades

1. Identificar y describir síntomas relevantes para establecer las causas más probables de los incidentes. Hacer referencia a los recursos de conocimiento disponibles (incluyendo errores y problemas conocidos) para identificar posibles resoluciones de incidentes (soluciones temporales y/o soluciones permanentes).
2. Registrar un nuevo problema si un problema relacionado o error conocido no existe aún y si el incidente satisface los criterios acordados para registro de problemas.
3. Asignar incidentes a funciones especialistas si se necesita de un conocimiento más profundo, e implicar al nivel de gestión apropiado, cuando sea necesario.

DSS02.05 Resolver y recuperarse ante incidentes.

Documentar, solicitar y probar las soluciones identificadas o temporales y ejecutar acciones de recuperación para restaurar el servicio TI relacionado.

Actividades:

1. Seleccionar y aplicar las resoluciones de incidentes más apropiadas (soluciones provisionales y/o soluciones permanentes).
2. Registrar si se usaron soluciones temporales para resolver los incidentes.
3. Ejecutar acciones de recuperación, si se requieren.
4. Documentar la resolución del incidente y evaluar si puede usarse como una fuente de conocimiento en el futuro.

DSS02.06 Cerrar peticiones de servicio e incidentes.

Verificar la satisfactoria resolución de incidentes y/o satisfactorio cumplimiento de peticiones, y cierre.

Actividades:

1. Verificar con los usuarios afectados (si lo han acordado) que la petición de servicio ha sido completada o el incidente ha sido resuelto de manera satisfactoria.
2. Cerrar peticiones de servicio e incidentes.

DSS02.07 Seguir el estado y emitir de informes.

Hacer seguimiento, analizar e informar de incidentes y tendencias de cumplimiento de peticiones, regularmente, para proporcionar información para la mejora continua.

Actividades:

1. Supervisar y hacer seguimiento del escalado de incidentes y de resoluciones y de los procedimientos de gestión de resoluciones para progresar hacia la resolución o cumplimentación.

2. Identificar la información para las partes interesadas y sus necesidades de datos o informes. Identificar la frecuencia y el medio para informarles.

3. Analizar incidentes y peticiones de servicio por categoría y tipo para establecer tendencias e identificar patrones de asuntos recurrentes, infracciones de ANSs o ineficiencias. Utilizar la información como entrada a la planificación de la mejora continua.

4. Producir y distribuir informes en tiempo o proporcionar acceso controlado a datos online.

DSS03 Gestionar Problemas

Identificar y clasificar problemas y sus causas raíz y proporcionar resolución en tiempo para prevenir incidentes recurrentes. Proporcionar recomendaciones de mejora.

Prácticas de Gestión:

DSS03.01 Identificar y clasificar problemas.

Definir e implementar criterios y procedimientos para informar de los problemas identificados, incluyendo clasificación, categorización y priorización de problemas.

Actividades:

1. Identificar problemas a través de la correlación de informes de incidentes, registros de error y otros recursos de identificación de problemas. Determinar niveles de prioridad y categorización para dedicarse a la

resolución de problemas en tiempo basándose en los riesgos de negocio y en la definición del servicio.

2. Manejar formalmente todos los problemas con acceso a todos los datos relevantes, incluyendo información sobre el sistema de gestión de cambios y los detalles de incidentes sobre configuración/activos TI.

3. Definir grupos de soporte adecuados para ayudar en la identificación de problemas, en el análisis de la causa raíz, y en la determinación de la solución, para respaldar la gestión de problemas. Determinar grupos de soporte basados en categorías predefinidas, tales como hardware, redes, software, aplicaciones y software de soporte.

4. Definir niveles de prioridad mediante consultas con el negocio para asegurar que la identificación de problemas y el análisis de la causa raíz se llevan a cabo a tiempo de acuerdo con los ANSs acordados. Basar los niveles de prioridad en el impacto en el negocio y en la urgencia.

5. Informar del estado de problemas identificados al centro de servicios de forma que los clientes y la gestión de TI pueden mantenerse informados.

6. Mantener un catálogo de gestión de problemas único para registrar e informar sobre problemas identificados y para establecer pistas de auditoría sobre los procesos de gestión de problemas, incluyendo el estado de cada problema (p. ej., abierto, reabierto, en progreso o cerrado).

DSS03.02 Investigar y diagnosticar problemas.

Investigar y diagnosticar problemas utilizando expertos en las materias relevantes para valorar y analizar las causas raíz.

Actividades

1. Identificar problemas que pueden ser errores conocidos comparando datos de incidentes con la base de datos de errores conocidos y posibles (p. ej., los comunicados por los proveedores externo) y clasificar problemas como errores conocidos.

2. Asociar los elementos de configuración afectados con el error conocido/establecido.

3. Producir informes para comunicar el progreso de la resolución de problemas y para supervisar el impacto continuado de los problemas no resueltos. Supervisar el estado del proceso de gestión de problemas a través de su ciclo de vida, incluyendo aportaciones de la gestión de cambios y de configuración.

DSS03.03 Levantar errores conocidos.

Tan pronto como las causas raíz de los problemas se hayan identificado, crear registros de errores conocidos y una solución temporal apropiada, e identificar soluciones potenciales.

Actividades

1. Tan pronto como las causas raíz de los problemas se han identificado, crear registros de errores conocidos y desarrollar una solución temporal adecuada.
2. Identificar, evaluar, priorizar y procesar (a través de la gestión de cambios) soluciones a los errores conocidos basándose en un caso de negocio coste- beneficio y en el impacto de negocio y la urgencia.

DSS03.04 Resolver y cerrar problemas.

Identificar e iniciar soluciones sostenibles refiriéndose a la causa raíz, levantando peticiones de cambio a través del proceso de gestión de cambios establecido si se requiere para resolver errores. Asegurarse de que el personal afectado está al tanto de las acciones tomadas y de los planes desarrollados para prevenir que vuelvan a ocurrir futuros incidentes.

Actividades

1. Cerrar registros de problemas, bien después de la confirmación de la eliminación satisfactoria del error conocido, bien tras acordar con el negocio cómo gestionar el problema de una manera alternativa.

2. Informar al centro de servicio del calendario de cierre del problema, p. ej., del calendario para solucionar los errores conocidos, la posible solución alternativa o el hecho de que el problema permanecerá hasta que el cambio se haya implementado, y las consecuencias de la solución escogida. Mantener adecuadamente informados a los usuarios y a los clientes afectados.

3. A través del proceso de resolución, obtener informes periódicos de gestión de cambios acerca del progreso en la resolución de problemas y errores.

4. Supervisar el continuo impacto de los problemas y errores conocidos en los servicios.

5. Revisar y confirmar la resolución satisfactoria de problemas graves.

6. Asegurar que el conocimiento aprendido de esta revisión se incorpora en una reunión de revisión del servicio con el cliente de negocio.

DSS03.05 Realizar una gestión de problemas proactiva.

Recoger y analizar datos operacionales (especialmente registros de incidentes y cambios) para identificar tendencias emergentes que puedan indicar problemas. Registrar problemas para permitir la valoración.

Actividades

1. Capturar información de problemas relacionada con cambios e incidentes TI y comunicarla a las partes interesadas clave. Esta comunicación podría tomar la forma de informes y reuniones periódicas entre los responsables de los procesos de gestión de incidentes, problemas, cambios y configuración para considerar problemas recientes y acciones correctivas potenciales.

2. Asegurar que los responsables de los procesos y los responsables de gestión de incidentes, problemas, cambios y configuración se reúnen regularmente para discutir problemas conocidos y cambios futuros planificados.

3. Permitir a la empresa supervisar los costes totales de problemas, capturar esfuerzos de cambio resultantes de las actividades del proceso de gestión de problemas (p. ej., soluciones a problemas y errores conocidos) e informar de ellos.

4. Producir informes para supervisar la resolución de problemas respecto a los requisitos de negocio y ANSs. Asegurar el adecuado escalado de problemas, p. ej., escalado a un nivel de gestión superior de acuerdo con los criterios acordados, contactando proveedores externos, o enviando al comité de gestión de cambios para incrementar la prioridad de una petición de cambio urgente para implementar una solución temporal.

5. Optimizar el uso de recursos y reducir las soluciones temporales y hacer seguimiento de las tendencias de problemas.

6. Identificar e iniciar soluciones sostenibles (soluciones permanentes) identificando la causa raíz, y levantar peticiones de cambio a través de los procesos de gestión de cambios establecidos.

DSS04 Gestionar la Continuidad

Consiste en Establecer y mantener un plan para permitir al negocio y a TI responder a incidentes e interrupciones de servicio para la operación continua de los procesos críticos para el negocio y los servicios TI requeridos y mantener la disponibilidad de la información a un nivel aceptable para la empresa.

Prácticas de Gestión:

DSS04.01 Definir la política de continuidad de negocio, objetivos y alcance.

Definir la política y alcance de continuidad de negocio alineada con los objetivos de negocio y de las partes interesadas.

Actividades:

1. Identificar procesos de negocio internos y subcontratados y actividades de servicio que son críticas para las operaciones de la empresa o necesarias para cumplir con las obligaciones legales y/o contractuales.

2. Identificar las partes interesadas clave y los roles y responsabilidades para definir y acordar la política de continuidad y su alcance.

3. Definir y documentar los objetivos y el alcance mínimos acordados de la política de continuidad del negocio e imbricar la planificación de continuidad en la cultura empresarial.

4. Identificar procesos de soporte al negocio esenciales y servicios TI relacionados.

DSS04.02 Mantener una estrategia de continuidad.

Evaluar las opciones de gestión de la continuidad de negocio y escoger una estrategia de continuidad viable y efectiva en coste, que pueda asegurar la continuidad y recuperación de la empresa frente a un desastre u otro incidente mayor o disrupción.

Actividades

1. Identificar escenarios potenciales probables que puedan dar pie a eventos que puedan causar incidentes disruptivos importantes.

2. Realizar un análisis de impacto en el negocio para evaluar el impacto en tiempo de una disrupción en funciones críticas del negocio y el efecto que tendría en ellas.

3. Establecer el tiempo mínimo necesario para recuperar un proceso de negocio y su soporte de TI, basándose en una duración aceptable de interrupción del negocio y la interrupción máxima tolerable.

4. Analizar la probabilidad de amenazas que puedan causar pérdidas de continuidad de negocio e identificar medidas que puedan reducir la probabilidad y el impacto, mejorando la prevención e incrementando la resiliencia.

5. Analizar los requerimientos de continuidad para identificar las posibles estrategias de negocio y opciones técnicas.

6. Determinar las condiciones y los responsables de decisiones clave que puedan causar la invocación de los planes de continuidad.

7. Identificar los requerimientos de recursos y costes para cada opción técnica estratégica y realizar recomendaciones estratégicas.

8. Obtener la aprobación de los ejecutivos de negocio para las opciones estratégicas seleccionadas.

DSS04.03 Desarrollar e implementar una respuesta a la continuidad del negocio.

Desarrollar un plan de continuidad de negocio (BCP) basado en la estrategia que documente los procedimientos y la información lista para el uso en un incidente para facilitar que la empresa continúe con sus actividades críticas

Actividades

1. Definir las acciones y comunicaciones de respuesta a incidentes que deben ser realizadas en un evento de disrupción. Definir los roles y responsabilidades relacionados, incluyendo la responsabilidad para la política y la implementación.

2. Desarrollar y mantener planes de continuidad de negocio operativos que contengan los procedimientos que deben ser seguidos para permitir continuar operando los procesos críticos de negocio y/o planes temporales de proceso, incluyendo enlaces a los planes de proveedores de servicio externalizados.

3. Asegurar que los proveedores y socios externos clave tengan implantados planes de continuidad efectivos. Obtener evidencias auditadas si es necesario.

4. Definir las condiciones y procedimientos de recuperación que permitan la reanudación de los procesos de negocio, incluyendo la actualización y conciliación de las bases de datos para preservar la integridad de la información.

5. Definir y documentar los recursos necesarios para soportar los procedimientos de continuidad y recuperación, considerando personas, instalaciones e infraestructura de TI.

6. Definir y documentar los requerimientos de información de respaldo para soportar los planes, incluyendo planes y documentos en papel así como ficheros de datos y considerar las necesidades de seguridad y almacenamiento en otra ubicación.

7. Determinar las habilidades necesarias para los individuos implicados en la ejecución de los planes y procedimientos.

8. Distribuir los planes y la documentación de soporte de modo seguro a las partes interesadas y apropiadamente autorizadas y asegurar que estén accesibles en escenarios de desastre.

DSS04.04 Ejercitar, probar y revisar el BCP.

Probar los acuerdos de continuidad regularmente para ejercitar los planes de recuperación respecto a unos resultados predeterminados, para permitir el desarrollo de soluciones innovadoras y para ayudar a verificar que el plan funcionará, en el tiempo, como se espera.

Actividades

1. Definir los objetivos para ejercitar y probar los sistemas del plan (de negocio, técnicos, logísticos, administrativos, procedimentales y operacionales) para verificar la completitud del plan de continuidad de negocio (BCP) para enfrentarse a los riesgos de negocio.

2. Definir y acordar ejercicios que sean razonables con las partes interesadas, validar los procedimientos de continuidad, e incluir roles y responsabilidades y acuerdos de retención de datos que ocasionen la mínima disrupción en los procesos de negocio.

3. Asignar roles y responsabilidades para realizar ejercicios y pruebas del plan de continuidad.

4. Planificar ejercicios y actividades de prueba tal como esté definido en el plan de continuidad.

5. Realizar un análisis y revisión post-ejercicio para considerar el logro.

6. Desarrollar recomendaciones para mejorar el plan de continuidad actual en base a los resultados de la revisión.

DSS04.05 Revisar, mantener y mejorar el plan de continuidad.

Realizar una revisión por la Dirección de la capacidad de continuidad a intervalos regulares para asegurar su continua idoneidad, adecuación y efectividad. Gestionar los cambios en el plan de acuerdo al proceso de control de cambios para asegurar que el plan de continuidad se mantiene actualizado y refleja continuamente los requerimientos actuales del negocio.

Actividades

1. Revisar el plan y la capacidad de continuidad de forma regular frente a las asunciones hechas y los objetivos de negocio actuales, tanto estratégicos como operativos.

2. Considerar si es necesario una revisión del análisis de impacto en el negocio, dependiendo en la naturaleza de los cambios.

3. Recomendar y comunicar los cambios en la política, planes, procedimientos, infraestructura, roles y responsabilidades para la aprobación de la dirección y su realización mediante el proceso de gestión de cambios.

4. Revisar el plan de continuidad regularmente para considerar el impacto de cambios nuevos o mayores en: organización de la empresa,

procesos de negocio, acuerdos de externalización, tecnologías, infraestructura, sistemas operativos y sistemas de aplicaciones.

DSS04.06 Proporcionar formación en el plan de continuidad.

Proporcionar a todas las partes implicadas, internas y externas, de sesiones formativas regulares que contemplen los procedimientos y sus roles y responsabilidades en caso de disrupción.

Actividades

1. Definir y mantener los planes y requerimientos de formación para quienes realicen de manera continuada planificación de la continuidad, análisis de impacto, evaluaciones de riesgos, comunicación con los medios y respuesta a incidentes. Asegurar que los planes de formación consideren la frecuencia de formación y los mecanismos de entrega de la formación.
2. Desarrollar competencias basadas en formación práctica que incluyan la participación en ejercicios y pruebas.
3. Supervisar habilidades y competencias basándose en los resultados de los ejercicios y las pruebas.

DSS04.07 Gestionar acuerdos de respaldo.

Mantener la disponibilidad de la información crítica del negocio.

Actividades:

1. Hacer copias de seguridad de sistemas, aplicaciones, datos y documentación de acuerdo a una planificación definida, considerando:
   a. Frecuencia (mensual, semanal, diaria, etc.)
   b. Modo de copias de seguridad (por ejemplo, discos espejo para copias de seguridad en tiempo real frente a DVD-ROM para retenciones de larga duración)

c. Tipo de copias de seguridad (por ejemplo, completa frente a incremental)

d. Tipo se soporte

e. Copias de seguridad automatizadas en línea

f. Tipos de datos (por ejemplo, voz, óptica)

g. Creación de registros

h. Datos de cálculos críticos de usuario final (por ejemplo, hojas de cálculo)

i. Localización física y lógica de las fuentes de los datos

j. Seguridad y derechos de acceso

k. Cifrado

2. Asegurar que los sistemas, aplicaciones, datos y documentación mantenidos o procesados por terceras partes están adecuadamente respaldados o asegurados de otra forma. Considerar el hecho de requerir el retorno de las copias de seguridad de terceras partes. Considerar acuerdos de depósito (escrow).

3. Definir los requerimientos del almacenamiento de las copias de seguridad, dentro y fuera de la propia ubicación, que satisfagan los requerimientos del negocio. Considerar la accesibilidad requerida a las copias de seguridad.

4. Extender la concienciación y la formación en Planes de Continuidad de Negocio (BCP).

5. Probar y mantener legibles las copias de seguridad y las archivadas periódicamente.

DSS04.08 Ejecutar revisiones post-reanudación.

Evaluar la adecuación del Plan de Continuidad de Negocio (BCP) después de la reanudación exitosa de los procesos de negocio y servicios después de una disrupción.

Actividades:

1. Evaluar la observancia del Plan de Continuidad de Negocio (BCP) documentado.

2. Determinar la efectividad del plan, capacidades de continuidad, roles y responsabilidades, habilidades y competencias, resiliencia a incidentes, infraestructura técnica y estructuras organizativas y relaciones.

3. Identificar debilidades u omisiones en el plan y las capacidades y hacer recomendaciones para la mejora.

4. Obtener la aprobación de la dirección para los cambios en el plan y aplicarlos mediante el proceso de control de cambios de la empresa.

DSS05 Gestionar Servicios de Seguridad

Proteger la información de la empresa para mantener aceptable el nivel de riesgo de seguridad de la información de acuerdo con la política de seguridad. Establecer y mantener los roles de seguridad y privilegios de acceso de la información y realizar la supervisión de la seguridad.

Prácticas de Gestión:

DSS05.01 Proteger contra software malicioso (malware).

Implementar y mantener efectivas medidas, preventivas, de detección y correctivas (especialmente parches de seguridad actualizados y control de virus) a lo largo de la empresa para proteger los sistemas de información y tecnología del software malicioso (por ejemplo, virus, gusanos, software espía –spyware- y correo basura).

Actividades

1. Divulgar concienciación sobre el software malicioso y forzar procedimientos y responsabilidades de prevención.

2. Instalar y activar herramientas de protección frente a software malicioso en todas las instalaciones de proceso, con ficheros de definición de software malicioso que se actualicen según se requiera (automática o semi-automáticamente).

3. Distribuir todo el software de protección de forma centralizada (versión y nivel de parcheado) usando una configuración centralizada y la gestión de cambios.

4. Revisar y evaluar regularmente la información sobre nuevas posibles amenazas (por ejemplo, revisando productos de vendedores y servicios de alertas de seguridad).

5. Filtrar el tráfico entrante, como correos electrónicos y descargas, para protegerse frente a información no solicitada (por ejemplo, software espía y correos de phishing).

6. Realizar formación periódica sobre software malicioso en el uso del correo electrónico e Internet. Formar a los usuarios para no instalarse software compartido o no autorizado.

DSS05.02 Gestionar la seguridad de la red y las conexiones.

Utilizar medidas de seguridad y procedimientos de gestión relacionados para proteger la información en todos los modos de conexión.

Actividades:

1. Basándose en el análisis de riesgos y en los requerimientos del negocio, establecer y mantener una política de seguridad para las conexiones.

2. Permitir sólo a los dispositivos autorizados tener acceso a la información y a la red de la empresa. Configurar estos dispositivos para forzar la solicitud de contraseña.

3. Implementar mecanismos de filtrado de red, como cortafuegos y software de detección de intrusiones, con políticas apropiadas para controlar el tráfico entrante y saliente.

4. Cifrar la información en tránsito de acuerdo con su clasificación.
5. Aplicar los protocolos de seguridad aprobados a las conexiones de red.
6. Configurar los equipamientos de red de forma segura.
7. Establecer mecanismos de confianza para dar soporte a la transmisión y recepción segura de información.
8. Realizar pruebas de intrusión periódicas para determinar la adecuación de la protección de la red.
9. Realizar pruebas periódicas de la seguridad del sistema para determinar la adecuación de la protección del sistema.

DSS05.03 Gestionar la seguridad de los puestos de usuario final.

Asegurar que los puestos de usuario final (es decir, portátil, equipo sobremesa, servidor y otros dispositivos y software móviles y de red) están asegurados a un nivel que es igual o mayor al definido en los requerimientos de seguridad de la información procesada, almacenada o transmitida.

Actividades:

1. Configurar los sistemas operativos de forma segura.
2. Implementar mecanismos de bloqueo de los dispositivos.
3. Cifrar la información almacenada de acuerdo a su clasificación.
4. Gestionar el acceso y control remoto.
5. Gestionar la configuración de la red de forma segura.
6. Implementar el filtrado del tráfico de la red en dispositivos de usuario final.
7. Proteger la integridad del sistema.
8. Proveer de protección física a los dispositivos de usuario final.
9. Deshacerse de los dispositivos de usuario final de forma segura.

DSS05.04 Gestionar la identidad del usuario y el acceso lógico.

Asegurar que todos los usuarios tengan derechos de acceso a la información de acuerdo con los requerimientos de negocio y coordinar con las unidades de negocio que gestionan sus propios derechos de acceso con los procesos de negocio.

Actividades:

1. Mantener los derechos de acceso de los usuarios de acuerdo con los requerimientos de las funciones y procesos de negocio. Alinear la gestión de identidades y derechos de acceso a los roles y responsabilidades definidos, basándose en los principios de menor privilegio, necesidad de tener y necesidad de conocer.
2. Identificar unívocamente todas las actividades de proceso de la información por roles funcionales, coordinando con las unidades de negocio y asegurando que todos los roles están definidos consistentemente, incluyendo roles definidos por el propio negocio en las aplicaciones de procesos de negocio.
3. Autenticar todo acceso a los activos de información basándose en su clasificación de seguridad, coordinando con las unidades de negocio que gestionan la autenticación con aplicaciones usadas en procesos de negocio para asegurar que los controles de autenticación han sido administrados adecuadamente.
4. Administrar todos los cambios de derechos de acceso (creación, modificación y eliminación) para que tengan efecto en el momento oportuno basándose sólo en transacciones aprobadas y documentadas y autorizadas por los gestores individuales designados.
5. Segregar y gestionar cuentas de usuario privilegiadas.
6. Realizar regularmente revisiones de gestión de todas las cuentas y privilegios relacionados.

7. Asegurar que todos los usuarios (internos, externos y temporales) y su actividad en sistemas de TI (aplicaciones de negocio, infraestructura de TI, operaciones de sistema, desarrollo y mantenimiento) son identificables unívocamente. Identificar unívocamente todas las actividades de proceso de información por usuario.

8. Mantener una pista de auditoría de los accesos a la información clasificada como altamente sensible.

DSS05.05 Gestionar el acceso físico a los activos de TI.

Definir e implementar procedimientos para conceder, limitar y revocar acceso a locales, edificios y áreas de acuerdo con las necesidades del negocio, incluyendo emergencias. El acceso a locales, edificios y áreas debe estar justificado, autorizado, registrado y supervisado. Esto aplicará a todas las personas que entren en los locales, incluyendo empleados, empleados temporales, clientes, vendedores, visitantes o cualquier otra tercera parte.

Actividades:

1. Gestionar las peticiones y concesiones de acceso a las instalaciones de procesamiento. Las peticiones formales de acceso deben ser completadas y autorizadas por la dirección de la ubicación de TI, y guardado el registro de petición. Los formularios deberían identificar específicamente las áreas a las que el individuo tiene acceso concedido.

2. Asegurar que los perfiles de acceso están actualizados. El acceso a las ubicaciones de TI (salas de servidores, edificios, áreas o zonas) debe basarse en funciones de trabajo y responsabilidades.

3. Registrar y supervisar todos los puntos de entrada a las ubicaciones de TI. Registrar todos los visitantes de la ubicación, incluyendo contratistas y vendedores.

4. Instruir a todo el personal para mantener visible la identificación en todo momento. Prevenir la expedición de tarjetas o placas de identidad sin la autorización adecuada.

5. Escoltar a los visitantes en todo momento mientras estén en la ubicación. Si se encuentra a un individuo que no va acompañado, que no resulta familiar y que no lleva visible la identificación de empleado, se deberá alertar al personal de seguridad.

6. Restringir el acceso a ubicaciones de TI sensibles estableciendo restricciones en el perímetro, tales como vallas, muros y dispositivos de seguridad en puertas interiores y exteriores. Asegurar que los dispositivos registren el acceso y disparen una alama en caso de acceso no autorizado. Ejemplos de estos dispositivos incluyen placas o tarjetas llave, teclados (keypads), circuitos cerrados de televisión y escáneres biométricos.

7. Realizar regularmente formación de concienciación de seguridad física.

DSS05.06 Gestionar documentos sensibles y dispositivos de salida.

Establecer salvaguardas físicas apropiadas, prácticas de contabilidad y gestión del inventario para activos de TI sensibles, tales como formularios especiales, títulos negociables, impresoras de propósito especial o credenciales (token) de seguridad.

Actividades

1. Establecer procedimientos para gobernar la recepción, uso, eliminación y destrucción de formularios especiales y dispositivos de salida, dentro, en y fuera de la empresa.

2. Asignar privilegios de acceso a documentos sensibles y dispositivos de salida basados en el principio del menor privilegio, equilibrando riesgo y requerimientos de negocio.

3. Establecer un inventario de documentos sensibles y dispositivos de salida, y realizar regularmente conciliaciones.

4. Establecer salvaguardas físicas apropiadas sobre formularios especiales y dispositivos sensibles.

5. Destruir la información sensible y proteger dispositivos de salida (por ejemplo, desmagnetizando soportes magnéticos, destruir físicamente dispositivos de memoria, poniendo trituradoras o papeleras cerradas disponibles para destruir formularios especiales y otros documentos confidenciales).

DSS05.07 Supervisar la infraestructura para detectar eventos relacionados con la seguridad.

Usando herramientas de detección de intrusiones, supervisar la infraestructura para detectar accesos no autorizados y asegurar que cualquier evento esté integrado con la supervisión general de eventos y la gestión de incidentes.

Actividades

1. Registrar los eventos relacionados con la seguridad reportada por las herramientas de monitorización de la seguridad de la infraestructura, identificando el nivel de información que debe guardarse en base a la consideración de riesgo. Retenerla por un periodo apropiado para asistir en futuras investigaciones.
2. Definir y comunicar la naturaleza y características de los incidentes potenciales relacionados con la seguridad de forma que sean fácilmente reconocibles y sus impactos comprendidos para permitir una respuesta conmensurada.
3. Revisar regularmente los registros de eventos para detectar incidentes potenciales.
4. Mantener un procedimiento para la recopilación de evidencias en línea con los procedimientos de evidencias forenses locales y asegurar que todos los empleados están concienciados de los requerimientos.

Asegurar que los tiques de incidentes de seguridad se crean en el momento oportuno cuando la monitorización identifique incidentes de seguridad potenciales.

DSS06 Gestionar Controles de Proceso de Negocio

Definir y mantener controles apropiados de proceso de negocio para asegurar que la información relacionada y procesada dentro de la organización o de forma externa satisface todos los requerimientos relevantes para el control de la información. Identificar los requisitos de control de la información y gestionar y operar los controles adecuados para asegurar que la información y su procesamiento satisfacen estos requerimientos.

Prácticas de Gestión:

DSS06.01 Alinear actividades de control embebidas en los procesos de negocio con los objetivos corporativos.

Evaluar y supervisar continuamente la ejecución de las actividades de los procesos de negocio y controles relacionados, basados en el riesgo corporativo, para asegurar que el procesamiento de controles está alineado con las necesidades del negocio.

Actividades

1. Identificar y documentar las actividades de control de los procesos de negocio claves para satisfacer los requerimientos de control para los objetivos estratégicos, operacionales, de informes y cumplimiento.
2. Priorizar las actividades de control basadas en el riesgo inherente del negocio e identificar controles clave.
3. Asegurar la propiedad de las actividades de control claves.

4. Supervisar continuamente las actividades de control de extremo a extremo para identificar oportunidades de mejora.

5. Mejorar continuamente el diseño y operación de los controles de procesos de negocio.

DSS06.02 Controlar el procesamiento de la información.

Operar la ejecución de las actividades de proceso de negocio y controles relacionados, basados en el riesgo corporativo, para asegurar que el procesamiento de la información es válido, completo, preciso, oportuno y seguro (es decir, refleja el uso de negocio autorizado y legitimado).

Actividades

1. Crear transacciones por individuos autorizados siguiendo los procedimientos establecidos, incluyendo, cuando sea apropiado, la adecuada segregación de tareas en relación al origen y aprobación de esas transacciones.

2. Autenticar la fuente de las transacciones y verificar que él o ella tiene la autoridad para originar las transacciones.

3. Introducir transacciones en el momento oportuno. Verificar que las transacciones son precisas, completas y válidas. Validar los datos de entrada y la edición o, cuando sea aplicable, la devolución para su corrección tan cerca al punto de origen como sea posible.

4. Corregir y reenviar datos cuya entrada fue erróneamente aceptada, sin comprometer los niveles de autorización de la transacción original. Cuando sea apropiado para la reconstrucción, conservar los documentos fuentes originales durante tiempo apropiado.

5. Mantener la integridad y validez de los datos a través del ciclo de procesamiento. Asegurar que la detección de transacciones erróneas no interrumpe el procesamiento de las transacciones válidas.

6. Mantener la integridad de los datos durante interrupciones no esperadas en el procesamiento de negocio y confirmar la integridad de los datos después de los fallos de procesamiento.

7. Manejar la salida de una forma autorizada, entregarla al beneficiario apropiado y proteger la información durante la transmisión. Verificar la precisión y completitud de la salida.

8. Antes de pasar datos de la transacción entre las aplicaciones internas y las funciones operacionales o de negocio (dentro o fuera de la organización), comprobar el correcto direccionamiento, autenticidad de origen e integridad del contenido. Mantener la autenticidad e integridad durante la transmisión o la generación del informe.

DSS06.03 Gestionar roles, responsabilidades, privilegios de acceso y niveles de autorización.

Gestionar los roles de negocio, responsabilidades, niveles de autoridad y segregación de tareas necesarias para apoyar los objetivos del proceso de negocio. Autorizar el acceso a cualquier activo de información relativo a los procesos de información del negocio, incluyendo aquellos bajo la custodia del negocio, de TI y de terceras partes. Esto asegura que el negocio sabe dónde están los datos y quien los está manejando en su nombre.

Actividades:

1. Asignar roles y responsabilidades sobre la base de la descripción aprobada de puestos y actividades de procesos de negocio asignadas.

2. Asignar niveles de autoridad para la aprobación de transacciones, límites y cualquier otra decisión relativa a los procesos de negocio, basadas en los roles de trabajo aprobados.

3. Asignar derechos de acceso y privilegios solo sobre lo que es necesario para ejecutar las actividades de trabajo, basados en los roles de puesto pre- definidos. Eliminar o revisar los derechos de acceso inmediatamente si el rol del puesto cambia o un miembro del personal deja

el área de proceso de negocio. Revisar periódicamente para asegurar que el acceso es adecuado para las actuales amenazas, riesgos, tecnología y necesidades del negocio.

4. Asignar roles para las actividades sensibles de manera que haya una segregación clara de funciones.

5. Proporcionar concienciación y formación en relación a los roles y responsabilidades de forma regular para que todo el mundo entienda sus responsabilidades; la importancia de los controles; y la integridad, confidencialidad y privacidad de la información de la empresa en todas sus formas.

6. Revisar periódicamente las definiciones de control de acceso, registros e informes de excepciones para asegurar que todos los privilegios de acceso son válidos y están alineados con el personal actual y sus roles asignados.

DSS06.04 Gestionar errores y excepciones.

Gestionar las excepciones y errores de los procesos de negocio y facilitar su corrección. Incluir escalada errores y excepciones en los procesos de negocio y la ejecución de acciones correctivas definidas. Esto proporciona garantía de precisión e integridad del proceso de información del negocio.

Actividades:

1. Definir y mantener procedimientos para asignar propiedad, corregir errores, remplazar errores y manejar las condiciones fuera de equilibrio.

2. Revisar errores, excepciones y desviaciones.

3. Hacer seguimiento, corregir, aprobar y reenviar documentos fuente y transacciones.

4. Mantener evidencia de las medidas correctivas.

5. Informar acerca de errores de proceso de información relevantes de manera oportuna para realizar el análisis de tendencias y causas raíces.

DSS06.05 Asegurar la trazabilidad de los eventos y responsabilidades y de información.

Asegurar que la información de negocio puede ser rastreada hasta los responsables y eventos de negocio que la originan. Esto permite trazabilidad de la información a lo largo de su ciclo de vida y procesos relacionados. Proporciona garantías de que la información que conduce el negocio es de confianza y ha sido procesada acorde a los objetivos definidos.

Actividades

1. Definir requerimientos de retención, basados en los requerimientos de negocio, para conocer las necesidades operativas, de reporte financiero y cumplimiento.
2. Capturar la fuente de información, evidencia que la soporta y el registro de las transacciones.
3. Eliminar la fuente de información, la evidencia que la soporta y el registro de transacciones de acuerdo con la política de retención.

DSS06.06 Asegurar los activos de información.

Asegurar los activos de información accesibles por el negocio a través de los métodos aprobados, incluyendo la información en formato electrónico (tales como métodos para crear nuevos activos en cualquier forma, dispositivos portátiles, aplicaciones de usuario y dispositivos de almacenamiento), información en formato físico (tales como documentos fuente o informes de salida) e información en tránsito. Esto beneficia al negocio proporcionando una salvaguarda de la información de comienzo a fin.

Actividades

1. Aplicar las políticas de clasificación de datos y uso aceptable y seguridad y los procedimientos para proteger los activos de información bajo el control del negocio.
2. Proporcionar concienciación y formación de un uso aceptable.
3. Restringir el uso, la distribución y el acceso físico a la información acorde a su clasificación.
4. Identificar e implementar procesos, herramientas y técnicas para verificar razonablemente el cumplimiento.
5. Informar al negocio y otros grupos de interés acerca de violaciones y desviaciones.

ARTICULO CIENTIFICO

Evaluación de Riesgos de los Sistemas de Información de Audioauto S.A. utilizando MAGERIT apoyados en los Objetivos de control de COBIT

Bethy Janneth Cruz Quinzo, Juan Carlos Chamorro Noboa

Departamento de Ciencias de la Computación; Escuela Politécnica del Ejercito, Sangolquí, Ecuador

cruz_bethy@hotmail.com , jchamorro_noboa@hotmail.com

Resumen: El presente artículo describe la Evaluación de Riesgos realizada en Audioauto S.A. para establecer la situación de riesgo en que se encuentran los Sistemas de Información y las acciones que se deben tomar para controlarlo y mitigarlo. Comenzamos con un levantamiento de la estructura interna de la organización y los principales procesos del negocio, determinamos los Sistemas de Información que los soportan y realizamos un mapeo para establecer los principales Activos de TI. A continuación aplicamos Magerit para realizar una caracterización y valoración cuantitativa de los Activos, sus Amenazas y Salvaguardas para determinar el Estado del Riesgo. Posteriormente desde la perspectiva de la Optimización del Riesgo de Cobit en las dimensiones Financiera, Cliente e Interna, establecemos las debilidades relacionadas con el Gobierno y Gestión de TI. Como resultado de esta evaluación, habiendo aplicando Magerit y Cobit determinamos el Riesgo a el que se encuentran expuestos los principales Activos de TI, y las áreas en las que se requiere priorizar la Optimización del Riesgo.

Palabras Clave: Evaluación Riesgos, Optimización Riesgos, Sistemas Información, Magerit, Cobit.

Abstract: This article describes the Evaluation of Risks performed in Audioauto S.A. to establish the situation of risk in the Information Systems and the actions to be taken to control and mitigate. We began with a survey of the internal structure of the organization and key business processes to determinate the Information Systems that support the processes and performed a mapping to establish Major IT Assets. Then we applied Magerit for a characterization and quantitative evaluation of the assets, their threats and safeguards for establish the State Risk. Subsequently, from the perspective of Optimization Cobit Risk in Financial, Internal and Client dimensions, we established weaknesses related IT Governance and Management. As a result of this evaluation, having applied Magerit and Cobit, we found level of risk to which Major IT Assets are exposed and the Areas that required to be prioritized in the risk optimization.

Key Words: Evaluation Risks, Optimization Risks, Information Systems, Magerit, Cobit.

I. Introducción

Siendo Audioauto una empresa dedicada a brindar servicios de Localización Satelital, actividad dependiente de tecnologías de información y comunicaciones que interactúan en tiempo real por una parte con los dispositivos de localización y por otra parte con los usuarios del servicio, se necesita mantener un alto grado de disponibilidad y confidencialidad en los servicios y la información que maneja.

A nivel mundial, así como en nuestro país y sobre todo en organizaciones que brindan servicios relacionados con tecnologías de información, la seguridad y disponibilidad de la información no son un valor agregado, si no que forma parte del servicio en sí mismo y por ende es un requisito fundamental.

Para cumplir este objetivo es fundamental realizar la Evaluación de Riesgos y determinar la situación de riesgo en que se encuentran los Sistemas de Información así como establecer las acciones que se deben tomar para controlarlo y mitigarlo.

Como metodologías para este análisis seleccionamos MAGERIT ya que nos brinda los procedimientos, técnicas y herramientas necesarias para evaluación del nivel de riesgo al que están expuestos de los Activos de TI y nos apoyamos en los Objetivos de Control de COBIT logramos determinar el Modelo de Valor de los Activos de TI, la evaluación de las Amenazas y Salvaguardas, realización del Mapa de Riesgos, así como las debilidades relacionadas con el Gobierno y Gestión de TI.

II. Estado del Arte

En la actualidad existen diversas metodologías que nos dan las herramientas necesarias para identificar, controlar, mitigar y gestionar los riesgos.

Microsoft en su metodología “Guía de Administración de Riesgos”(Kurt Dillard (MSS), Jared Pfost (SCOE), 2004) expone que las infraestructuras de TI extremadamente conectadas de hoy en día existen en un entorno que es cada vez más hostil debido a los ataques frecuentes, nuevas legislaciones que incluyen preocupaciones de privacidad, obligaciones financieras, gobierno corporativo, entre otras, obligan a que la seguridad se administre proactivamente, para minimizar o evitar los riesgos a los cuales están expuestos ejecutivos y las organizaciones.

En la presentación realizada por José Ángel Peña Ibarra Vicepresidente de ISACA (Ibarra, 2010) expone que algunas de las metodologías más relevantes para el análisis de riesgos son:

OCTAVE (Operationally Critical Thread, Asset and Vulnerability Evaluation), enfocada a que la organización sea capaz de: Dirigir y gestionar sus evaluaciones de riesgos, Tomar decisiones basándose en sus riesgos, Proteger los activos claves de información y Comunicar de forma efectiva la información clave de seguridad.

MAGERIT (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información), enfocada al establecimiento de un Plan de Proyecto de Riesgos, mediante el análisis de los riesgos estimando el impacto que tendrán en la organización así como del tiempo y los recursos que su tratamiento conllevará, seleccionando las posibles soluciones para cada riesgo y los mecanismos que implementarán las soluciones seleccionadas, con el fin de Concienciar a los responsables de las

organizaciones de información de la existencia de riesgos y de la necesidad de gestionarlos, Ofrecer un método sistemático para analizar los riesgos derivados del uso de Tecnologías de la Información y Comunicaciones (TIC), Ayudar a descubrir y planificar el tratamiento oportuno para mantener los riesgos bajo control.

ISO/IEC 27005, que describe las recomendaciones y directrices generales para la gestión de riesgos en sistemas de seguridad de la información, poniendo énfasis en la Identificación de riegos, su Evaluación, Análisis de Riesgo contrastado con la organización, Establecimiento de Escenarios de Riesgo y Respuesta a los Riesgos.

RiskITISACA, que establece las mejores prácticas con el fin de establecer un marco para las organizaciones para identificar, gobernar y administrar los riesgos asociados a su negocio. Es utilizado para ayudar a implementar el gobierno de TI y, las organizaciones que han adoptado (o están planeando adoptar) COBIT como marco de su gobierno de TI.

III. Marco Teórico

Para analizar el Riesgo MAGERIT nos plantea las siguientes definiciones:

Riesgo: estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la Organización. El riesgo indica lo que le podría pasar a los activos si no se protegieran adecuadamente. Es importante saber qué características son de interés en cada activo, así como saber en qué medida estas características están en peligro, es decir, analizar el sistema.

Análisis de riesgos: proceso sistemático para estimar la magnitud de los riesgos a que está expuesta una Organización. Sabiendo lo que podría pasar, hay que tomar decisiones.

Tratamiento de los riesgos: es un proceso destinado a mitigar el riesgo.

Hay múltiples formas de tratar un riesgo: evitar las circunstancias que lo provocan, reducir las posibilidades de que ocurra, acotar sus consecuencias, compartirlo con otra organización, o, en última instancia, aceptando que pudiera ocurrir y previendo recursos para actuar cuando sea necesario.

A veces se acepta riesgos operacionales para acometer actividades que pueden reportar beneficios que superan al riesgo, o que tenemos la obligación de afrontar. Esto es muy delicado e incluye la decisión de aceptar un cierto nivel de riesgo.

Según MAGERIT, las dimensiones de seguridad a evaluar para Gestionar el Riesgo son:

Disponibilidad: O disposición de los servicios a ser usados cuando sea necesario. La carencia de disponibilidad supone una interrupción del servicio.

Integridad: O mantenimiento de las características de completitud y corrección de los datos. Contra la integridad, la información puede aparecer manipulada, corrupta o incompleta. La integridad afecta directamente al correcto desempeño de las funciones de una Organización.

Confidencialidad: O que la información llegue solamente a las personas autorizadas.

De estas dimensiones primordiales de la seguridad se derivan otras que nos acerquen a la percepción de los usuarios de los sistemas de información:

Autenticidad: Propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos.

Trazabilidad: Aseguramiento de que en todo momento se podrá determinar quién hizo qué y en qué momento.

El proceso que sigue MAGERIT para la evaluación de riesgos consiste en determinar los activos más relevantes, su interrelación y valor, posteriormente se identifican las amenazas a las que están expuestos y las salvaguardas que se podrían implementar y su efectividad frente al riesgo. Con esto se estima el impacto sobre el activo derivado de la materialización de la amenaza y el riesgo, definido como el impacto ponderado con la tasa de ocurrencia:

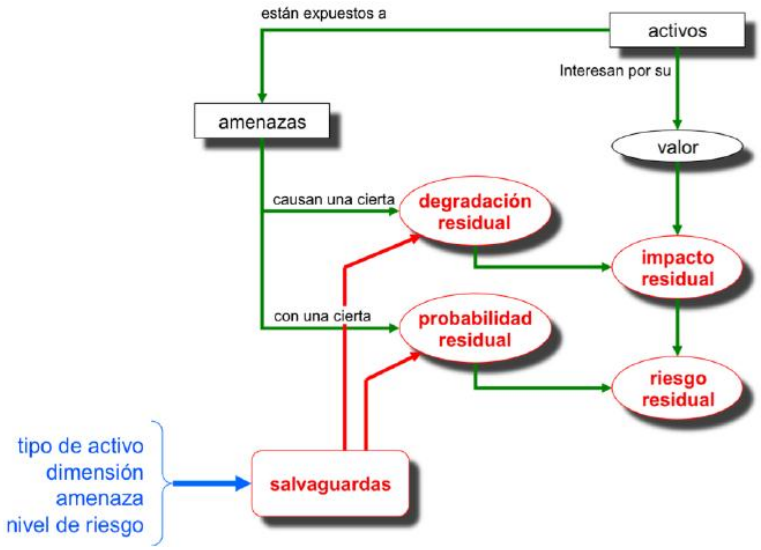

Figura 65. Procesos MAGERIT - AT

La misión de COBIT es: Investigar, desarrollar, hacer público y promover un marco de control de gobierno de TI autorizado, actualizado y aceptado internacionalmente. Nos plantea la necesidad de saber si con la información administrada en la empresa es posible:

- Lograr que toda la estrategia de TI, así como las metas fluyan de forma gradual a toda la empresa.
- Garantizar el logro de sus objetivos
- Sea suficientemente flexible para aprender y adaptarse
- Se cuente con un manejo juicioso de los riesgos que enfrenta
- Se reconozca de forma apropiada las oportunidades y actúe de acuerdo a ellas.

Considerando estas necesidades, COBIT provee un marco de trabajo integrado para la entrega de valor, administrando los riesgos y el control sobre la información, enfocada en la mejora del gobierno de TI, alineando la estrategia de TI con la estrategia del negocio, orientado a procesos, basado en controles e impulsado por mediciones.

- Orientado al negocio: La orientación a negocios es el tema principal de COBIT. Está diseñado para ser utilizado no sólo por proveedores de servicios, usuarios y auditores de TI, sino también y principalmente, como guía integral para la gerencia y para los dueños de los procesos de negocio.
- Orientado a Procesos: COBIT define las actividades de TI en un modelo genérico de procesos organizado en cuatro dominios. Estos dominios son Planear y Organizar, Adquirir e Implementar, Entregar y Dar Soporte y Monitorear y Evaluar. Los dominios se equiparan a las áreas tradicionales de TI de planear, construir, ejecutar y monitorear.

Un modelo de procesos fomenta la propiedad de los procesos, permitiendo que se definan las responsabilidades. Para gobernar

efectivamente TI, es importante determinar las actividades y los riesgos que requieren ser administrados. Normalmente se ordenan dentro de dominios de responsabilidad de plan, construir, ejecutar y Monitorear, el principio básico de COBIT:

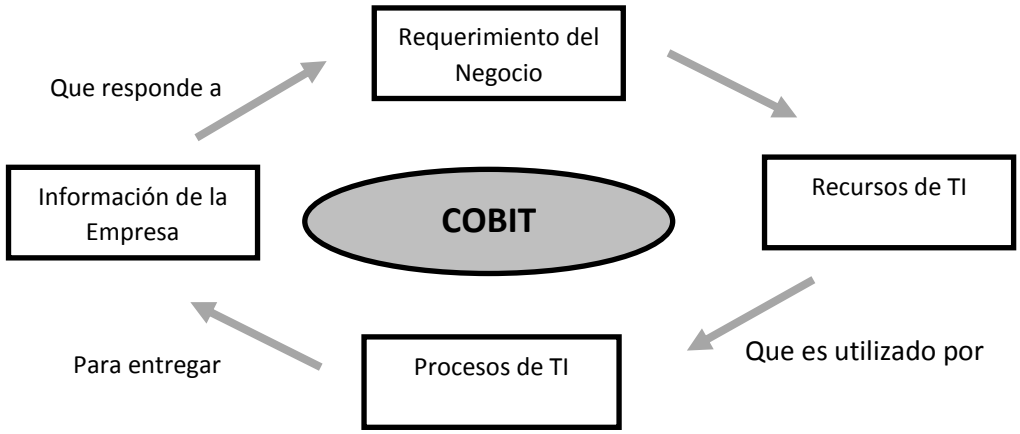

Figura 66. Principio Básico de COBIT - AT

De acuerdo con COBIT, los criterios que debe cumplir la información son:

- **Efectividad**: La información debe ser relevante y pertinente para los procesos del negocio, así como que sea entregada de manera oportuna, correcta, consistente y utilizable.
- **Eficiencia**: La entrega de información se haga mediante la utilización óptima de los recursos.
- **Confidencialidad**: Protección de la información sensible contra divulgación no autorizada.
- **Integridad**: Precisión y completitud de la información, así como a su validez de acuerdo con los valores y expectativas del negocio.
- **Disponibilidad**: Debe estar disponible cuando la requieran los procesos del negocio ahora y en el futuro. También concierne a las salvaguardas de los recursos necesarios y sus capacidades necesarias asociadas.

- **Cumplimiento**: Debe cumplir con el acatamiento las leyes, regulaciones y compromisos contractuales a los cuales están sujetos los procesos del negocio, es decir, criterios de negocio impuestos externamente así como políticas internas.
- **Confiabilidad**: Se relaciona con la provisión de la información apropiada para que la gerencia administre la entidad y ejerza sus responsabilidades de confianza y gobierno.

Los recursos de TI identificados en COBIT son:

- **Las Aplicaciones** son tanto los sistemas automatizados de usuario como los procedimientos manuales con los que se procesa la información.
- **La Información** son los datos de cualquier forma utilizados por el negocio, que entran a, son procesados por y salen de los sistemas de información.
- **La Infraestructura** es la tecnología y las instalaciones (hardware, sistemas operativos, sistemas de administración de base de datos, redes, multimedia, etc., así como el sitio donde se encuentran y el ambiente que los soporta).
- **Los recursos Humanos** son los requeridos para planear, organizar, adquirir, implementar, entregar, soportar, monitorear y evaluar los sistemas y los servicios de información.

IV. Situación actual de la Organización

Para determinar la situación actual de la organización realizamos un levantamiento de su Misión, Visión, Valores así como sus Estructuras Geográfica, Organizacional y Jerárquica. Se realizó un levantamiento de los recursos administrados por el departamento de sistemas en lo referente a la infraestructura de Hardware, Software y los responsables de su administración. Con este análisis pudimos obtener una visión general de la Organización, su cultura, tamaño y nivel de complejidad.

VI. Evaluación de los Riesgos

Para realizar la evaluación de los riesgos comenzamos identificando de forma detallada los principales activos de TI, tanto de Hardware como Software, En lo referente al Hardware encontramos compontes como:

- Centros de Datos
- Servidores de Correo, de Aplicación, de Base de Datos y Administración de Archivos, Backups y Otros Servidores
- Equipos de Comunicaciones
- Enlaces de Comunicaciones

En lo referente al Software encontramos:

- Sistemas Administrativo Financieros, Administracion Tributaria, Activos Fijos, etc.
- Sistemas de Gestión del Recurso Humano, Evaluaciones.
- Sistemas para la Administración de Clientes
- Sistemas de Interfase entre los diversos componentes.
- Sistemas para la Administración de Seguridades.
- Sistemas de Control y Análisis de Mensajes de localización Satelital
- Portales Web
- Sistemas para Backup y Recuperación

Con la Información levantada del Harware y Software, se procedió a identificar los servicios que brindan y establecer un mapeo entre:

- Servicios -> Aplicaciones -> Servidores
- Servicios -> Aplicaciones -> Bases de Datos

Se procedió a identificar los procesos más críticos de la organización soportados por los servicios de TI, con el fin de establecer el valor de cada Activo de TI de acuerdo al mapeo realizado anteriormente. Los procesos identificados fueron:

- Nuevas Instalaciones

- Renovaciones del Servicio Normal y Fee
- Chequeo de Dispositivos de Localización
- Pago de Comisiones Externas e Internas
- Importación de Dispositivos de Localización.
- Compra de Materiales y Suministros
- Ensamblaje y Acondicionamiento de Kits de Instalación
- Gestión de Cobranzas
- Interacción de Clientes en la Extranet

Aplicando Magerit se realizó la caracterización y valoración de los Activos de TI, sus Amenazas y Salvaguardas de acuerdo con las especificaciones sugeridas por Magerit clasificando las Amenazas de acuerdo su la naturaleza.

Se procedió a determinar el Estado del Riesgo de acuerdo a las escalas sugeridas por Magerit para lo cual, establecemos la influencia que tienen las amenazas en los activos de acuerdo a la **"Degradación"** que le provocarían y a la **"Probabilidad"** de que la amenaza se materialice. Como resultado obtenemos la estimación de lo que puede ocurrir es decir el "Impacto" de lo que probablemente ocurra o "Riesgo". Con estos elementos establecemos:

El **"Impacto Potencial"** que es la medida del daño que le puede causar la materialización de la amenaza sin tomar en cuenta las salvaguardas existentes.

El **"Impacto Acumulado"** tomando en cuenta el valor del activo más el valor de todos los activos que dependen de él y las amenazas a las que está expuesto.

El **"Impacto Repercutido"** que es el Impacto Potencial tomando en cuenta su propio valor y las amenazas de a las que están expuestos los activos de los que depende.

El **“Impacto Residual”** que corresponde a la medida del daño que se le puede causar a un activo tomando en cuenta las salvaguardas implementadas.

El **“Riesgo Potencial”, “Riesgo Acumulado” y** el **“Riesgo Repercutido”** corresponden a la medida del probable daño al sistema tomando en cuenta la probabilidad de ocurrencia y su Impacto Potencial, Acumulado y Repercutido respectivamente.

La **“Degradación Residual”** que corresponde a la degradación que n consiguen contrarrestar las salvaguardas.

El **“Riesgo Residual”** que corresponde al riesgo al que está sometido el Activo una vez establecidas las salvaguardas.

Para la determinación de la degradación del Activo “D” tomamos en cuenta una escala porcentual 0 a 100%.

Para establecer la Probabilidad de que una amenaza materialice su Ocurrencia utilizamos la frecuencia esperada anual de ocurrencia (ARO – Annual Rate of Occurrence) en la escala que se muestra:

Probabilidad		Ocurrencia	Equivalencia
MA	muy alta	casi seguro	Fácil
A	Alta	muy alto	Medio
M	Media	posible	Difícil
B	Baja	poco probable	muy difícil
MB	muy baja	muy raro	extremadamente difícil

Tabla 71. Probabilidad Anual de Materialización de la Amenaza - AT

Para establecer el valor de los Activos tomamos en cuenta la siguiente:

Valor del Activo			Observación
EX	Extremo	10	Activos que requieren atención inmediata
MA	Muy Alto	9	
AL	Alto	6 - 8	
ME	Medio	3 - 5	
BA	Bajo	1 – 2	
DE	Despreciable	0	Activos que no requieren atención

Tabla 72. Escala de Valor de los Activos - AT

Para determinar el Riesgo tomamos utilizamos la siguiente escala:

Riesgo	Impacto	Valor
MA	Crítico	9 - 10
A	Importante	7 - 8
M	Apreciable	5 - 6
B	Bajo	3 - 4
MB	Despreciable	0 - 2

Tabla 73. Escala de Riesgo -AT

Para determinar el Impacto = V(valor del activo) x D(% de degradación):

Impacto		% de Degradación del Activo				
		20%	40%	60%	80%	100%
Valor del Activo	EX	AL	MA	EX	EX	EX
	MA	ME	AL	MA	MA	MA
	AL	BA	ME	AL	AL	AL
	ME	DE	BA	ME	ME	ME
	BA	DE	DE	BA	BA	BA
	DE	DE	DE	DE	DE	DE

Tabla 74. Impacto en función del Valor del Activo y % de Degradación - AT

Para calcular el Riesgo = I (Impacto) × F (frecuencia o probabilidad de que se materialice la amenaza):

Riesgo		Probabilidad que se materialice una amenaza				
		MB	B	M	A	MA
Impacto	EX	MA	MA	MA	MA	MA
	MA	A	MA	MA	MA	MA
	AL	M	A	A	MA	MA
	ME	B	M	M	A	A
	BA	MB	B	B	M	M
	DE	MB	MB	MB	B	B

Tabla 75. Riesgo en función del Impacto y la frecuencia - AT

Se aplicaron las escalas obteniendo como resultado los informes de impacto y riesgos potenciales y residuales clasificados por los siguientes tipos de amenazas:

- Desastres de Origen Natural
- Desastres de Origen Industrial
- Errores de Usuarios
- Errores y Fallos no Intencionados
- Ataques Intencionados
- Uso no previsto
- Manipulación de Programas

Informe del Riesgo potencial y residual por Desastres de Origen Natural.- Se evidenció una diferencia entre el riesgo potencial y residual debido a las salvaguardas implementadas en referencia al Fuego, pero el riesgo residual es alto.

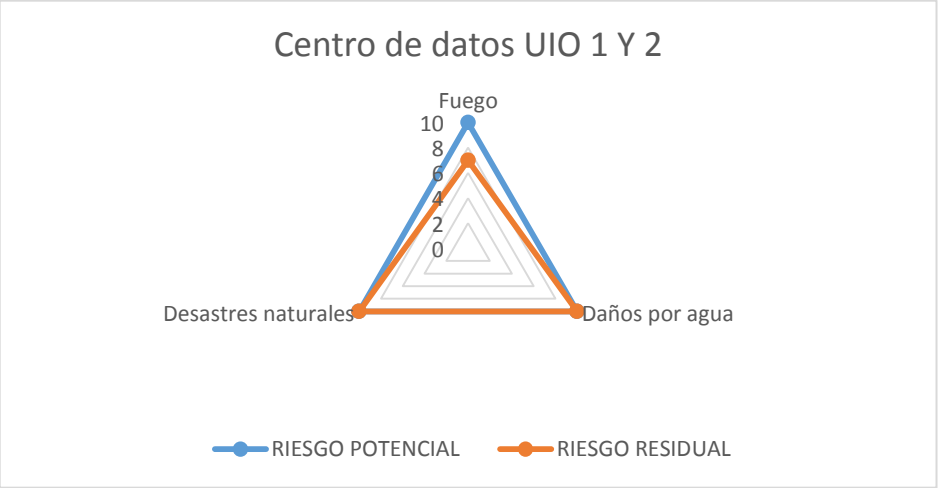

Figura 67. Riesgo Desastres Naturales - AT

Informe del Riesgo potencial y residual por Desastres de Origen Industrial.- Se evidenció una diferencia entre el riesgo potencial y residual debido a las salvaguardas implementadas en referencia al Fuego, Contaminación Mecánica, Averías de origen Físico o Lógico, Cortes de Suministro Eléctrico, Humedad. El principal problema radica en Fallos de servicios de comunicaciones, Soportes de Almacenamiento de información y otros Desastres Industriales.

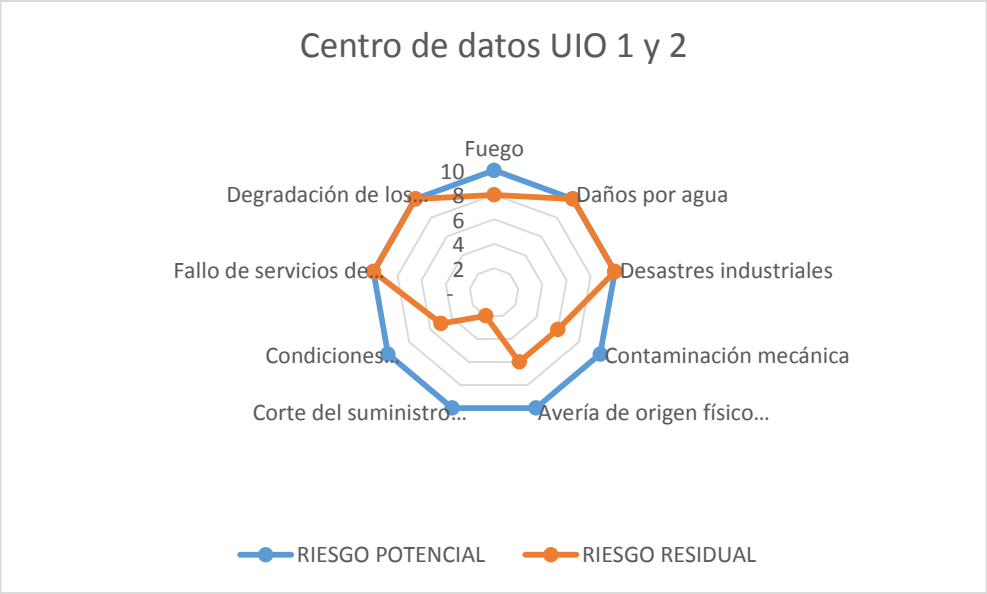

Figura 68. Riesgo Desastres Industriales - AT

Informe del Riesgo potencial y residual por errores de los usuarios.- Se evidenció una diferencia entre el riesgo potencial y residual debido a las salvaguardas implementadas en Órdenes de Monitoreo, Contratos y Facturación.

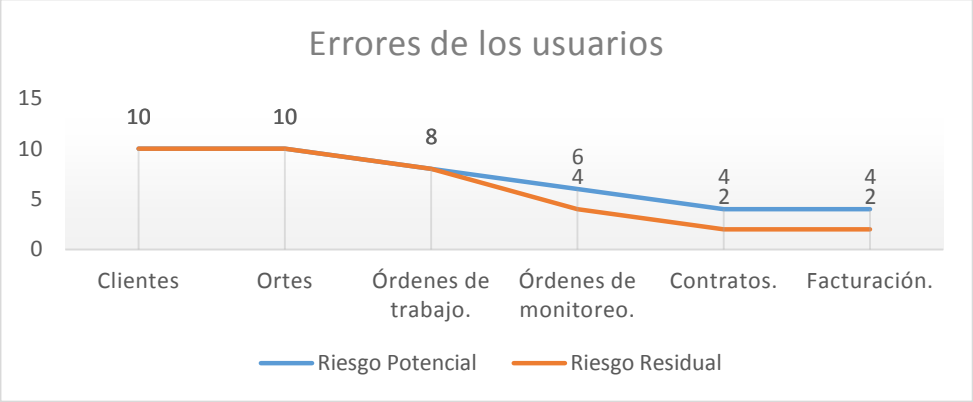

Figura 69. Riesgo Errores de los usuarios - AT

Informe del Riesgo potencial y residual por errores y fallos no intencionados.- Se evidenció una gran diferencia entre el riesgo potencial y

residual de la mayoría de Activos, logrando que el riesgo sea despreciable, pero en lo referente a la Administración de Seguridades, Clientes, Contratos y Transacciones Contables no se han implementado salvaguardas efectivas.

Figura 70. Riesgo Errores y Fallos no Intencionados AT

Informe del Riesgo potencial y residual por ataques intencionados.- Se evidenció que el riesgo potencial y residual es crítico, debido a que no se encuentran implementadas salvaguardas.

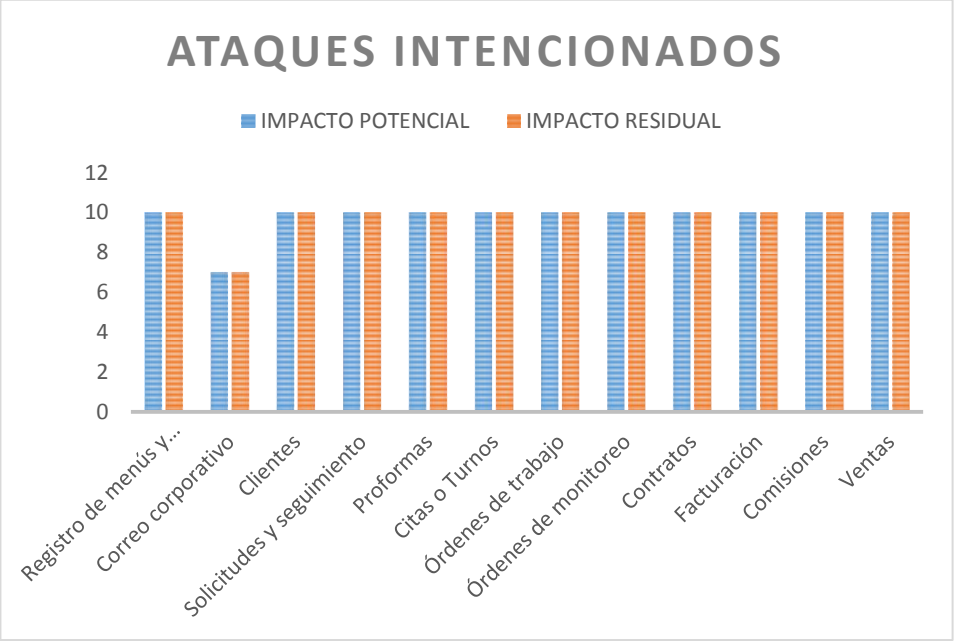

Figura 71. Riesgo Errores y Fallos no Intencionados - AT

Informe del Riesgo potencial y residual por uso no previsto.- Se evidenció que existe implementada una salvaguarda altamente eficaz, por lo que el el riesgo residual es despreciable.

Figura 72. Riesgo Uso no Previsto - AT

Informe del Riesgo potencial y residual por manipulación de programas.- Se evidenció que existe una salvaguarda implementada eficazmente baja, por lo que el riesgo residual es alto.

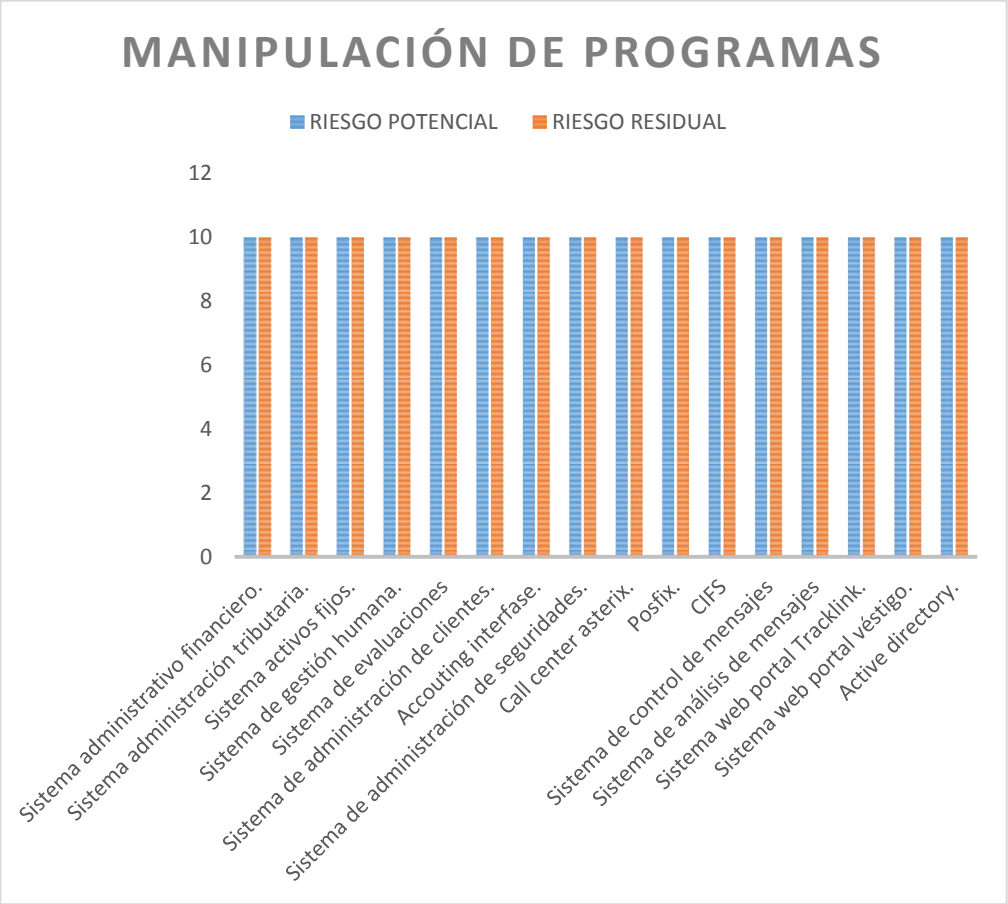

Figura 73. Riesgo por Manipulación de Programas - AT

Aplicando Cobit 5 se realizó la evaluación de los controles del negocio centrados en la Optimización del Riesgo en las dimensiones Financiera, del Cliente e Interna.

En lo referente a la **Dimensión Financiera** se determinó una debilidad relacionada con la inexistencia de un proceso de evaluaciones de cumplimiento de Leyes y Regulaciones Externas y no se han establecido los parámetros de cobertura necesarios para suplir este riesgo, así como tampoco existen procesos formales de evaluación de riesgos ni métricas para determinar si fueron adecuadamente gestionados.

En lo relacionado con la **Dimensión Cliente** existen deficiencias relacionadas con la falta de medidas de satisfacción con la calidad en la entrega de servicios de TI.

En lo referente con la **Dimensión Interna** se han encontrado sistemas con tecnología obsoleta que no cuentan con un control de seguridad integrado como es el caso de Activos Fijos y se ha determinado deficiencias relacionadas con el tiempo necesario para la concesión, cambio y eliminación de privilegios de acceso y falta de procedimientos internos adecuados. No se han realizado evaluaciones de seguridad y tampoco establecido estándares y guías.

Con respecto a la **Gestión de TI** hemos observado la necesidad de implementar un proceso cíclico de Gestión del Riesgo que permita **Alinear, Planificar y Organizar** de manera que continuamente se recopilen datos, se analice el nivel de riesgo y se transparenta para que sea gestionado “APO12 Gestionar el Riesgo”. Se ha determinado que existe un impacto muy alto por “Amenazas por Ataques Intencionales” para lo cual es necesario definir, gestionar y supervisar un plan para el tratamiento del riesgo SGSI tomando como marco de referencia “APO13 Gestionar la Seguridad”.

En lo referente a **Construir, Adquirir e Implementar** tomamos como referencia e; proceso “BAI09 Gestionar los Activos” y encontramos que se hace necesario gestionar el ciclo de vida de los Activos de TI para asegurar la fiabilidad y capacidad de servicio, adicionalmente se han determinado deficiencias en el control y cantidad necesaria de Licencias para cubrir el software instalado y en uso.

En lo relacionado con **Entregar, Dar Servicio y Soporte**, determinamos que no se han establecido procedimientos que permitan gestionar y resolver las peticiones de servicios internos y externalizados, tomamos como marco

de referencia “DSS01 Gestionar Operaciones”, “DSS02 Gestionar Peticiones e Incidentes de Servicio” y “DSS03 Gestionar Problemas”. Se determinó la necesidad de establecer y gestionar un plan que permita mantener la continuidad del negocio atendiendo a los servicios más importantes y la disponibilidad de la información tomando como marco de referencia el proceso “DSS04 Gestionar la Continuidad” e implementar un proceso para retroalimentar y gestionar errores tomando como referencia “DSS06 Gestionar Controles de Proceso de Negocio”.

V. Conclusiones y Recomendaciones

Conclusiones.-

La aplicación de Magerit ha transparentado la real situación de riesgo de los Sistemas de Información de AudioAuto S.A. determinado que existen niveles de riesgo críticos y muy altos para varias tipos de amenazas, los cuales deben ser objeto de atención inmediata.

Mediante Cobit se encontró que existen debilidades desde el punto de vista del Gobierno y Gestión de TI que permitan una adecuada administración de los activos y genere valor dentro de la organización.

La realización del análisis de riesgos utilizando Magerit y Cobit ha permitido tener una visión global de la organización, permitiendo establecer los elementos necesarios para el emprendimiento de un proyecto de mejoramiento de seguridad y su posterior evaluación, control y mejora.

Recomendaciones.-

Una vez determinada la situación de riesgo de los sistemas de información es fundamental concientizar a la gerencia sobre la necesidad de

invertir en la implementación de las salvaguardas que permitan el control y mitigación el riesgo.

Es necesario poner especial atención en establecimiento de un proceso de evaluación periódica de cumplimiento de Políticas Internas, así como Leyes y Regulaciones Externas.

Es conveniente establecer medidas de satisfacción de la calidad en la entrega de servicios, establecer procedimientos internos, estándares y guías de TI.

Es necesario definir, gestionar y supervisar un plan para el tratamiento de riesgos SGSI y establecer y gestionar un plan que permita mantener la continuidad del negocio atendiendo a los servicios más importantes y la disponibilidad de la información.

VI. Referencias

Dirección General de Modernización Administrativa, P. e. (2012). *MAGERIT - version 3.0.* Madrid, España: Ministerio de Hacienda y Administraciones Públicas de España.

Ibarra, J. Á. (2 de Marzo de 2010). *Eventos: ISACA.* Recuperado el 5 de Agosto de 2013, de sitio web de ISACA: http://www.isaca.org/chapters7/Monterrey/Events/Documents/20100302%20Metodolog%C3%ADas%20de%20Riesgos%20TI.pdf

Institute, I. G. (2007). *COBIT® 4.1.* Rolling Meadows, Illinois, Estados unidos: Institute, IT Governance.

Kurt Dillard (MSS), Jared Pfost (SCOE). (15 de Octubre de 2004). *Guía de administración de riesgos de seguridad: Microsoft.* Recuperado el 05 de Agosto de 2013, de Michosoft Technet: http://www.microsoft.com/spain/technet/recursos/articulos/ack_page.mspx