RESUMEN

El presente trabajo tiene como objetivo aplicar el Modelo MAGERIT "Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información" al Departamento de Servicio Técnico de Servindurama, con la finalidad de que la Dirección de mencionada Organización, tenga un conocimiento veraz sobre el riesgo inherente en su Sistema, y así identificar las áreas que requieren mayor atención.

El modelo MAGERIT fue desarrollado por un equipo multidisciplinario de profesionales que laboran en el Ministerio de Administraciones Públicas de España, los cuales, al observar un aumento significativo en el uso de las Tecnologías de la Información por parte de las Organizaciones, vieron propicia la creación de un modelo que permita identificar las fortalezas y debilidades que posee un Sistema de Información.

El Modelo MAGERIT está compuesto por 3 fases:

1. Planificación del Proyecto: Consta de una estimación inicial de los riesgos que pueden afectar a los Sistemas de Información.

2. Análisis de Riesgos: Se estima el impacto que tendrán los riesgos en la Organización.

3. Gestión de Riesgos: Se identifica y selecciona nuevas funciones de salvaguarda que permitan reducir el riesgo a un nivel aceptable.

Para desarrollar el Proyecto, se utilizará la herramienta PILAR Basic que está desarrollada en base al modelo MAGERIT, esta herramienta nos permitirá realizar el ingreso de datos, recogidos mediante cuestionarios y entrevistas, efectuadas al personal que labora en la Organización.

La herramienta permitirá observar el nivel de riesgo actual y como éste riesgo se puede disminuir incorporando nuevas salvaguardas o mejorando salvaguardas ya implementadas.

PALABRAS CLAVE:

- Análisis
- Gestión
- Riesgos
- Magerit
- Pilar Basic

"CONTROL DE RIESGOS EN EL DEPARTAMENTO DE SERVICIO TÉCNICO DE LA EMPRESA SERVINDURAMA EN LA CIUDAD DE CUENCA"

ÍNDICE

UNIVERSIDAD DE CUENCA

FACULTAD DE CIENCIAS ECONÓMICAS Y ADMINISTRATIVAS

ESCUELA DE CONTABILIDAD Y AUDITORÍA.

"CONTROL DE RIESGOS EN EL DEPARTAMENTO DE SERVICIO TÉCNICO DE LA EMPRESA SERVINDURAMA EN LA CIUDAD DE CUENCA"

Tesis previa a la Obtención del título de:
Contador Público Auditor

AUTORES:
NORMAN ANDRÉS ALVEAR VANEGAS
SANTIAGO ALEJANDRO PLAZA AUQUILLA

DIRECTOR:
ING. COM. WILSON CUEVA

CUENCA – ECUADOR
2011

AGRADECIMIENTO

A nuestro querido Dios, quien nos ha permitido conquistar una meta más en nuestras vidas. A nuestros padres, por darnos su amor incondicional; de igual manera agradecemos a todas las personas que nos brindaron su ayuda y sabiduría en el transcurso de nuestra carrera universitaria: maestros y compañeros, a nuestro Director de Tesis Ing. Com. Wilson Cueva, que de manera desinteresada nos apoyó para la realización de la presente, al Máster Ing. Mauricio Alvear Álvarez, Jefe Nacional de Servindurama, por facilitarnos la información pertinente para el desarrollo de nuestro trabajo; a nuestros amigos con los cuales vivimos momentos inolvidables.

DEDICATORIAS

De una manera muy especial dedico este trabajo a los seres que más amo en este mundo: mi hijo Renato, mi esposa María Augusta, mis padres Norman y Miriam y a mi hermana Lorena, quienes me han sabido brindar su apoyo incondicional y son mi fuente de inspiración.

Andrés

Mi Tesis la dedico con todo mi amor y cariño.
A ti Dios que me diste la oportunidad de vivir y de regalarme una familia maravillosa.
Con mucho cariño principalmente a mis padres que me dieron la vida y han estado conmigo en todo momento. Los quiero con todo mi corazón y este trabajo que nos llevó mucho tiempo hacerlo es para ustedes.

Santiago

Las opiniones, conclusiones y recomendaciones expresadas en esta Tesis son de exclusiva responsabilidad de los Autores.

Norman Andrés Alvear Vanegas.
Santiago Alejandro Plaza Auquilla.

INTRODUCCIÓN

A través de la historia de la humanidad, los riesgos han afectado negativamente la vida de las personas, ya sea de manera individual o de manera colectiva; con el paso de los tiempos la humanidad ha reaccionado y ha tomado conciencia de la utilización de medidas de seguridad que permitan afrontar estos riesgos y de esta manera reducir el impacto de los mismos.

Con el avance de la tecnología, se ha incrementado en un porcentaje cada vez mayor, el uso de recursos electrónicos, informáticos y telemáticos por parte de las personas, organizaciones y/o entidades; dichos recursos brindan grandes beneficios al ser utilizados, pero también, el uso de éstos dan lugar a ciertos riesgos, los cuales deben ser minimizados con medidas de seguridad.

Por esta razón, las organizaciones necesitan proteger su información para asegurar que esté disponible cuando se la requiera, que sea fiable en todo momento, y que su distribución este controlada; para que se cumplan los aspectos antes mencionados, se necesita tener un conocimiento a fondo de los recursos utilizados para el desarrollo de la información en una Organización.

Entonces, es necesario el uso de una metodología bien definida y actualizada de seguridad que mantenga el sistema en desarrollo a salvo de los distintos peligros que le acechan. Es muy importante resaltar la importancia de la seguridad puesto que el sistema maneja información personal reservada, luego en el caso de ser objeto de un ataque, los responsables del sistema pasarían de víctimas (del ataque) a inculpados (por violación de la LORTAD, Ley Orgánica de Regulación del Tratamiento Automatizado de los Datos de carácter personal)[1]

Por lo tanto, es preciso integrar a las operaciones una metodología que permita gestionar la Seguridad de los Sistemas de Información. La metodología recomendada es el modelo MAGERIT, desarrollado por el Ministerio de Administraciones Públicas de España, el cual, permite realizar un seguimiento exhaustivo de la seguridad del sistema de información de una organización.

[1] MAÑAS J. Antonio, MAGERIT: Análisis y Gestión de Riesgos. 2010. Ministerio de Administraciones Públicas, España.

CAPÍTULO 1

PLANIFICACIÓN DEL PROYECTO.

1.1 DESCRIPCIÓN DE LA ORGANIZACIÓN.

1.1.1 QUIÉNES SON:

El Departamento de Servicio Técnico cuenta con 25 años de experiencia en el Ecuador, especializado en la reparación de línea blanca y café, ya sean éstos:

- Refrigeradoras
- Congeladores
- Vitrinas Frigoríficas
- Aires Acondicionados
- Cocinas
- Hornos
- Microondas
- Lavadoras de ropa
- Lavavajillas
- Televisores
- LCD
- Equipos de Sonido
- DVD

1.1.2 MISIÓN

Ser la empresa de servicio y asesoramiento técnico de electrodomésticos más reconocida del país, brindando respaldo permanente, oportuno y eficiente; bajo principios de honestidad y amabilidad.

1.1.3 VISIÓN

Solucionar los reclamos de los clientes y usuarios aplicables al funcionamiento del producto con eficiencia y responsabilidad cumpliendo con la garantía concedida por la marca.

1.1.4 ESTRUCTURA ORGANIZACIONAL

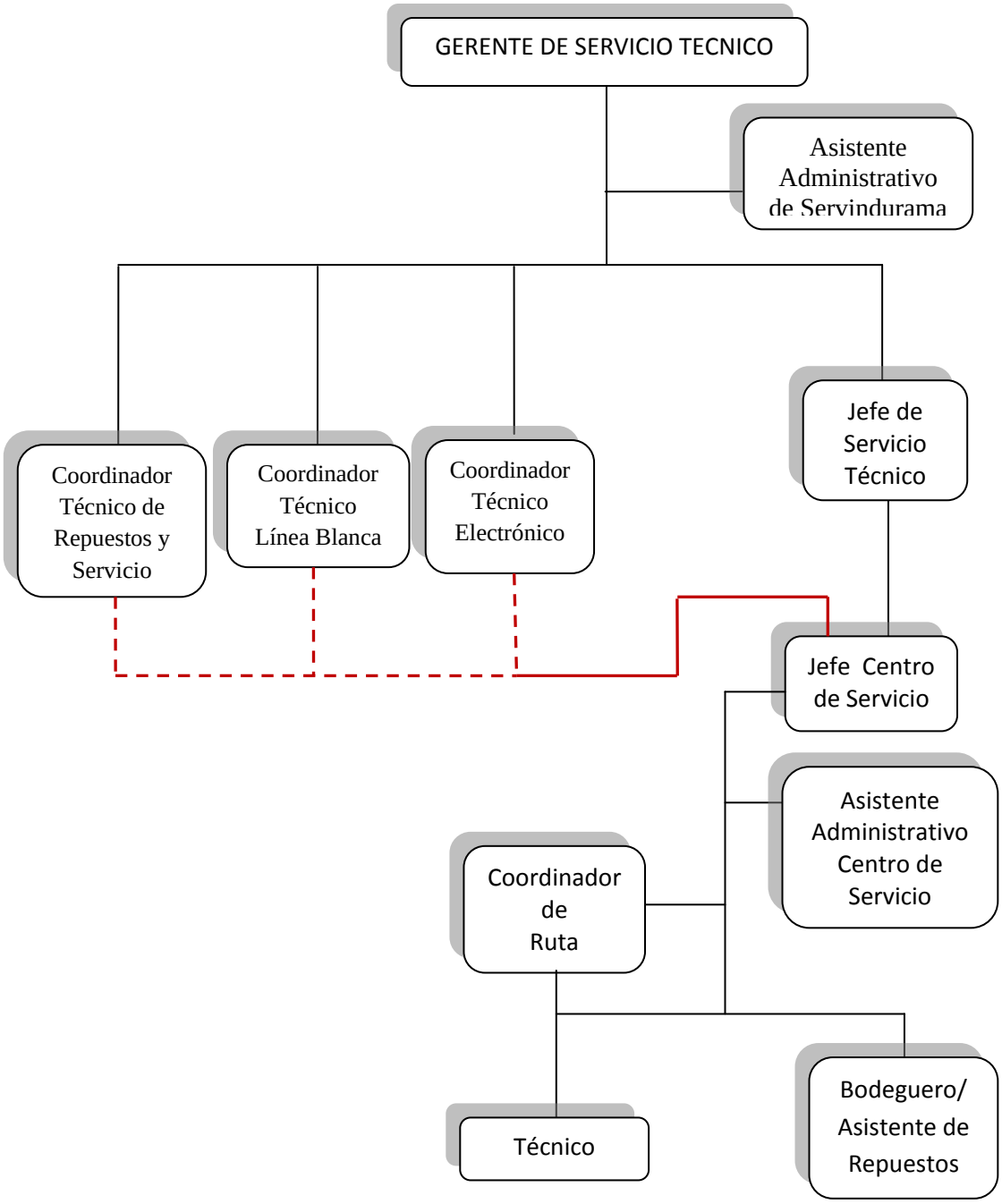


Figura 1: Organigrama.

Fuente: Jefe de Servicio Técnico Servindurama.

Elaborado por: Servindurama.

1.1.5. INFRAESTRUCTURA.

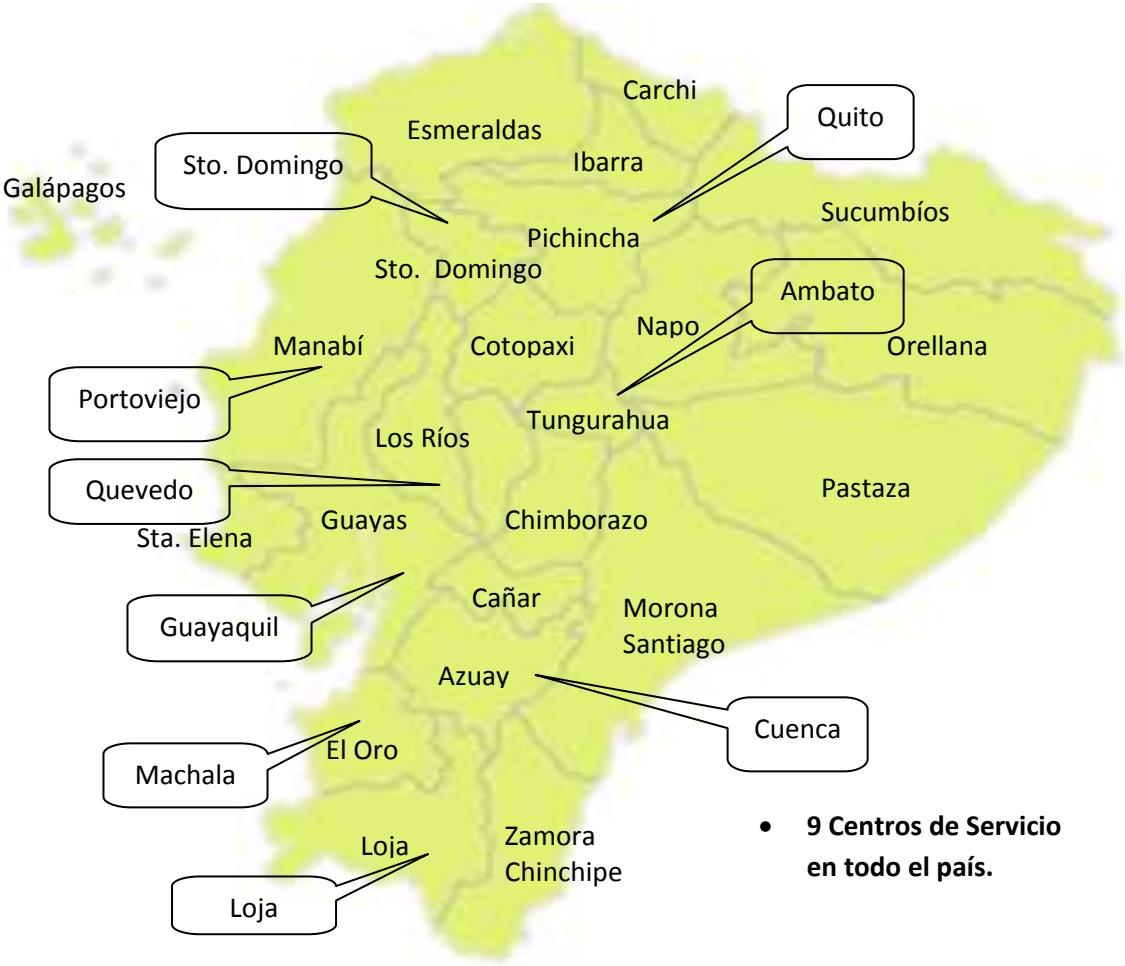


Figura 2: Cobertura de Servicio Técnico en Ecuador.

Fuente: Jefe de Servicio Técnico Servindurama.

Elaborado por: Servindurama.

1.1.5.1 COBERTURA.

El Departamento de Servicio Técnico, cuenta con 9 oficinas a nivel nacional y con técnicos residentes en varios puntos del país, en los cuales su oferta de servicio es en 24 horas. Para zonas foráneas aplica calendario de visitas de 7 a 15 días.

1.1.5.2 RECURSO HUMANO.

CENTRO DE SERVICIO	PERSONAL TECNICO	PERSONAL ADMINISTRATIVO	TOTAL
CUENCA	6	3	9
GUAYAQUIL	24	6	30
QUITO	12	5	17
MACHALA	6	3	9
LOJA	2	1	3
AMBATO	5	3	8
STO. DOMINGO	5	3	8
PORTOVIEJO	7	3	10
QUEVEDO	3	2	5
MATRIZ		5	5
TOTAL	**70**	**34**	**104**

Tabla 1: Distribución del Personal por Provincias.

Fuente: Jefe de servicio Técnico Servindurama.

Elaborado por: Servindurama.

1.1.5.3 RECURSO FÍSICO – TÉCNICO.

El Departamento de Servicio Técnico, cuenta con:

- 53 camionetas que permiten la movilización y traslado del producto
- 2 Motocicletas
- Equipos y Herramientas
- Cámaras Digitales
- Scanner

1.1.5.4 RECURSO TECNOLÓGICO Y COMUNICACIONES.

El Departamento de Servicio Técnico, cuenta con los siguientes recursos:

- Sistema de Computación JD Edwards (JDE), que permite el registro de órdenes por cliente, manejo de Recursos, Customer Service Management System.
- Internet Banda Ancha.
- Sistema de comunicación mediante radios.
- Líneas Telefónicas.

Además, el Departamento de Servicio Técnico, cuenta con el área "Contact Center" (1800-30-30-30), que brinda atención al cliente, en donde el interesado podrá obtener información centralizada sobre la gestión del servicio técnico y telefónico.

En resumen, el Departamento Técnico es el encargado de realizar un seguimiento minucioso a los productos que presenten fallas después de que éstos sean adquiridos por los clientes.

1.2 ASPECTOS CONCEPTUALES.

1.2.1 ANÁLISIS Y GESTIÓN DE RIESGOS.

Para realizar un Análisis y Gestión de Riesgos a las TIC's dentro de una Organización, debemos tener pleno conocimiento de lo que es la Seguridad, la cual se define como: "*la capacidad de las redes o Sistemas de Información para resistir, con un determinado nivel de confianza, los accidentes, acciones ilícitas o malintencionadas que comprometan la confidencialidad, integridad, disponibilidad y autenticidad de los datos almacenados o transmitidos y de los servicios que dichas redes y sistemas ofrecen o hacen accesibles*"[2]

De esta manera, la misión de una Organización será proteger su información, considerando las siguientes dimensiones de seguridad:

- **Disponibilidad:**

  Aseguramiento de que los autorizados tengan acceso a la información y a los activos asociados cuando lo necesiten.

  La carencia de disponibilidad, obliga a una interrupción de las operaciones o del servicio.

- **Integridad:**

  Garantía de exactitud y completitud de información y métodos de procesado.

[2] MAÑAS J. Antonio, MAGERIT: Análisis y Gestión de Riesgos. 2010. Ministerio de Administraciones Públicas, España, p. 7.

Cualquier falla en la Integridad, afectará el desempeño de las funciones de una Organización.

- **Confidencialidad:**

  Aseguramiento de que la información sea accesible únicamente al personal autorizado.

- **Autenticidad (persona que haga uso de los datos o servicios):**

  Que no haya duda de quién se hace responsable de una información o prestación de un servicio, generalmente en esta dimensión se presentan suplantación de identidades.

Lo que una Organización pretende como objetivo primordial, es que su información posea todas las características antes mencionadas, pero esto generalmente no se llega a concretar, por lo tanto, es necesario aplicar un Análisis y Gestión de Riesgos; para entender esto debemos partir de la definición de Riesgo.

- **Riesgo:**

  Estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la Organización[3]. Es decir, el riesgo nos indica lo que le podría suceder a nuestros activos, si es que no son protegidos correctamente.

Es de vital importancia conocer como los riesgos pueden afectar a nuestros activos, esto lo podemos saber a través de un análisis del sistema.

- **Análisis de Riesgos:**

  Es un proceso sistemático que permite estimar la magnitud de los riesgos a los que está expuesta una Organización.

Conociendo la magnitud de los riesgos, es necesario tomar decisiones que nos permitirán contrarrestar dichos riesgos.

[3] MAÑAS J. Antonio, MAGERIT – versión 2, Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. 2006. Ministerio de Administraciones Públicas, España. p. 8

- **Gestión de Riesgos:**

  Implica la selección e implantación de salvaguardas que nos permitirán conocer, prevenir, impedir, reducir o controlar los riesgos identificados.

Es común que en una Organización no se pueda reducir el riesgo a cero, esto es porque prácticamente la seguridad absoluta no existe, por lo tanto, hay que aceptar siempre un nivel de riesgo, el cual debe ser conocido y reducido a su mínima expresión.

El hecho de aceptar cierto nivel de riesgo en una Organización, obliga a que se tenga pleno conocimiento de las condiciones en las cuales se trabaja, para que de esta manera se pueda ajustar el sistema a las actividades cotidianas de la Organización.

Para realizar el Análisis y Gestión de Riesgos de las Tecnologías de Información y Comunicación (TIC'S) en una Organización, se debe determinar una metodología que permita gestionar la Seguridad de los Sistemas de Información. La metodología recomendada es el modelo MAGERIT, el cual permite realizar un seguimiento exhaustivo de la Seguridad del Sistema de Información de una Organización.

Según el documento MAGERIT versión 2, publicado por el Ministerio de Política Territorial y Administración Pública de España, MAGERIT (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información), es un método formal para investigar los riesgos que soportan los Sistemas de Información y para recomendar las medidas apropiadas que deberían adoptarse para controlar estos riesgos.

El modelo MAGERIT se basa en los siguientes aspectos fundamentales [ISO 27005.08]:

- Determinar los objetivos, estrategias y políticas de seguridad de la información,
- Determinar los requerimientos de seguridad de la información,

- Identificar y analizar las amenazas y las vulnerabilidades de los activos de la información,
- Identificar y analizar los riesgos de seguridad,
- Especificar salvaguardas adecuadas teniendo en cuenta las amenazas, vulnerabilidades y riesgos identificados,
- Supervisar la implementación y el funcionamiento de las salvaguardas especificadas,
- Asegurar la concienciación de todo el personal en materia de seguridad de la Información,
- Detectar los posibles incidentes de seguridad y reaccionar ante ellos.

Para poder aplicar el modelo MAGERIT en una Organización, es necesario implementar la herramienta PILAR Basic, la cual relaciona los activos TIC's de un sistema con las amenazas posibles, calcula los riesgos y ayuda a incorporar salvaguardas que permitan reducir el riesgo a su mínima expresión. Esto nos permite fundamentar la confianza en el sistema.

PILAR Basic, es una aplicación informática que reúne los activos del sistema, sus relaciones de interdependencia y su valor para la organización. Conocido el sistema, nos permite introducir las posibles amenazas en los aspectos de disponibilidad, integridad, confidencialidad, autenticidad y trazabilidad, para definir los riesgos potenciales sobre el sistema.

Al conocer los riesgos, se pueden determinar las salvaguardas para la información; además la herramienta PILAR Basic, permite realizar un seguimiento continuo y recurrente al sistema de protección de la Organización, para que de esta manera el sistema pueda afrontar nuevos riesgos y así aumentar la confianza del mismo.

CAPÍTULO 2

PLANIFICACIÓN Y ANÁLISIS DE RIESGOS.

2.1 PLANIFICACIÓN.

2.1.1 OBJETIVOS.

Para realizar el Control de Riesgos a los Sistemas de Información (S.I.) del Departamento de Servicio Técnico de Servindurama, necesitamos conocer como se encuentran actualmente los S.I., esto lo podremos saber, mediante la etapa de Planificación, cuyo objetivo principal es establecer y definir el marco general de referencia para el proyecto de Análisis y Gestión de Riesgos.

Dicho proyecto será ejecutado con la herramienta conocida como PILAR Basic, la cual nos permitirá entender los S.I.

Como objetivos complementarios al desarrollar esta etapa, podemos mencionar los siguientes:

- Motivar a la dirección del Departamento de Servicio Técnico.
- Demostrar la oportunidad de realizar un Análisis y Gestión de Riesgo.
- Dar a conocer la voluntad de la Dirección con respecto al proyecto.
- Crear las condiciones necesarias para el buen desarrollo del proyecto.

Como consecuencia lógica, en esta etapa de Planificación se necesita la participación activa de los responsables del Departamento de Servicio Técnico, así como del personal que labora en el mismo, y de esta manera definir los objetivos y estrategias del Departamento dentro del proyecto.

Para realizar la Planificación de Análisis y Gestión de Riesgos, aplicaremos los siguientes pasos[4]:

- Oportunidad de realización.
- Definición de Objetivos.
- Planificación del Proyecto.

[4] MAÑAS J. Antonio, MAGERIT – versión 2, Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. 2006. Ministerio de Administraciones Públicas, España.

- Lanzamiento del Proyecto.

2.1.2 OPORTUNIDAD DE LA REALIZACIÓN.

La Dirección del Departamento de Servicio Técnico, es consciente de los problemas que están relacionados con la Seguridad de los Sistemas de Información, por ende, ha visto factible la realización del proyecto de Análisis y Gestión de Riesgos.

Las personas encargadas del manejo de la Información, no tienen mucho conocimiento de los nuevos problemas de seguridad que implica la utilización de las técnicas electrónicas, informáticas y telemáticas.

Bajo el análisis de entrevistas realizadas al personal del Departamento de Servicio Técnico, hemos observado que no se han presentado incidentes graves con respecto a la seguridad de los Sistemas de Información, lo que si podemos mencionar, es un problema que se presentó durante la época de racionamiento eléctrico que vivió el país, en donde el generador de energía propio de la Empresa, presentó fallas en el momento de su utilización y esto tuvo como consecuencia la paralización de las actividades.

Otro aspecto a considerar es que los cambios de la tecnología usada, han causado únicamente problemas de adaptabilidad a los usuarios, los cuales al comentar este problema, fueron capacitados para el manejo de la nueva tecnología.

Además el Departamento cuenta con planes de contingencia, en donde, se tiene prioridad al respaldo de la información.

2.1.3 DEFINICIÓN DE OBJETIVOS.

El proyecto a realizarse en el Departamento de Servicio Técnico, tiene por objetivo determinar las áreas donde el riesgo sea más elevado.

Conjuntamente con la determinación del objetivo, se establecerá el dominio del proyecto, que, desde el punto de vista de la seguridad del S.I., abarcará los subsistemas de captura y de gestión de datos, en donde se controlará el acceso, la disponibilidad y la integridad de los mismos.

Otro aspecto a considerar será la protección de la información relativa al proyecto, para lo cual se restringirá el acceso a las instalaciones de la Organización.

2.1.4 PLANIFICACIÓN DEL PROYECTO.

En esta actividad de la Planificación, debemos considerar los siguientes aspectos:

- Identificar, por ámbitos a los usuarios afectados.
- Planificar la intervención del usuario en el proyecto.
- Planificar las entrevistas a realizar con los usuarios.

2.1.5 LANZAMIENTO DEL PROYECTO.

Antes del lanzamiento del proyecto de Análisis y Gestión de Riesgos, debemos seleccionar y adaptar los cuestionarios que se utilizarán en la recogida de datos, así como especificar los criterios y las técnicas concretas a emplear en el Análisis y Gestión de Riesgos; y como fin asignar los recursos necesarios para la realización del proyecto.

Para realizar los cuestionarios nos basaremos en la guía de cuestionarios que ofrece MAGERIT[5].

Los cuestionarios a utilizar para la recogida de la información se adaptan con el objeto de identificar correctamente las amenazas, activos, vulnerabilidades impactos, salvaguardas existentes, restricciones; la necesidad de una adaptación siempre existe debido a los problemas de seguridad que puede y debe tratar MAGERIT.

Ver Anexo 1. Cuestionario.

[5] LÓPEZ C. Francisco, AMUDIO G. Miguel, CANDAU Javier, MAÑAS J. Antonio, MAGERIT – Fase de Inicio. 2006. Ministerio de Administraciones Públicas, España.

2.2 ANÁLISIS DE RIESGOS.

Esta Etapa, tiene por objetivo, identificar los activos que integran el Sistema de Información del Departamento de Servicio Técnico, así como también, determinar las amenazas a las que están expuestos dichos activos, determinar si existen salvaguardas para los activos y estimar el impacto si una amenaza llegara a materializarse.

La siguiente figura, recoge lo anteriormente dicho:

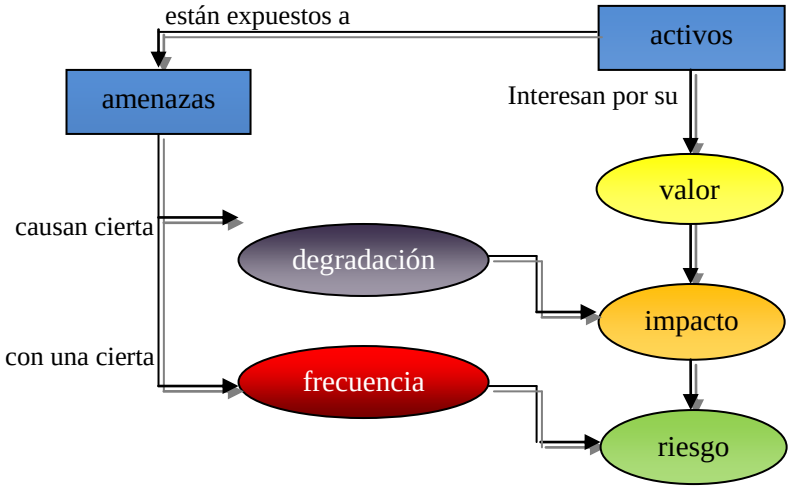


Figura 3: Análisis de Riesgos[6]

Fuente: MAGERIT – Versión 2.

Elaborado por: Autores.

La presente etapa será desarrollada en base a inspecciones físicas realizadas al Departamento, también se considerarán las entrevistas efectuadas, tanto a la Dirección como al personal que labora en dicho Departamento.

[6] MAÑAS J. Antonio, MAGERIT – versión 2, Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. 2006. Ministerio de Administraciones Públicas, España. p. 17.

2.2.1 IDENTIFICACIÓN DE LOS ACTIVOS.

Para realizar un Análisis de Riesgos, es sumamente importante identificar los activos que integran el Sistema de Información, estos activos pueden ser:

- Servicios.
- Aplicaciones Informáticas. (Software)
- Equipos Informáticos (Hardware)
- Soportes de Información
- Equipamiento Auxiliar
- Las Redes de Comunicación
- Las Instalaciones
- Las Personas

2.2.1.1 SERVICIOS.

Los servicios, son aquellos que se pueden prestar por parte de la Organización, a un usuario interno o externo.

Para los usuarios internos, la organización presta los siguientes servicios:

- Diagramas Explosivos.
- Listas de Partes.
- Estadísticas de Daño.

Para los usuarios externos, el Departamento, cuenta con los siguientes servicios:

- Overhaul de producto. (Reparación y Limpieza)
- Asesoría telefónica de instalación.
- Préstamo de producto. (Daño del producto)
- Venta de garantía extendida.
- Llamadas sin costo.

2.2.1.2 APLICACIONES INFORMÁTICAS.

Se considera como aplicaciones informáticas, al software que posee la Organización para manejar los datos.

Entre las aplicaciones que ostenta la Organización tenemos las siguientes:

- Módulo de ventas.
- Módulo de partes y piezas.
- Módulo Customer Service Management System.
- Módulo de préstamo. (producto)
- Módulo de diagramas explosivos.

2.2.1.3 EQUIPOS INFORMÁTICOS.

Equipo Informático también conocido como Hardware, es aquel que permite hospedar datos, programas y servicios.

Dentro del Equipo Informático que posee el Departamento, tenemos lo siguiente:

- Servidor IBM.
- 5 Notebooks marca Hewlett Packard (hp).
- 6 PC's de escritorio.
- Servidor Virtual.
- Impresora hp.
- Scanner.

2.2.1.4 SOPORTES DE INFORMACIÓN.

Los soportes de Información son aquellos dispositivos que permiten el almacenamiento de datos, en la Organización generalmente se utilizan:

- Memorias USB marca Kingston.
- Discos Formato DVD.
- Discos Formato CD.

2.2.1.5 EQUIPAMIENTO AUXILIAR.

Se considera como equipamiento auxiliar a todos los artefactos que complementan el material informático.

En la Organización se cuenta con el siguiente equipo informático:

- Generador de energía.
- Aire Acondicionado.
- UPS.
- Caja Fuerte.
- Mobiliario.

2.2.1.6 REDES DE COMUNICACIÓN.

Las redes de comunicación, son aquellos dispositivos que permiten el intercambio de datos.

Entre los dispositivos que maneja la organización para el intercambio de datos, tenemos los siguientes:

- Modem HUAWEI.
- Concentrador de red.
- Conmutador.
- Router.
- Firewall propio de la empresa.
- Dispositivo Wireless

2.2.1.7 LAS INSTALACIONES.

Es el lugar físico, donde se encuentran los equipos informáticos y de comunicaciones. Cabe recalcar que el estudio se realiza dentro del Departamento de Servicio Técnico de Servindurama.

2.2.1.8 LAS PERSONAS.

Es el personal que maneja los elementos antes mencionados.

Dentro del personal de la Organización, podemos citar a los siguientes:

- Ing. Sebastián Vega. Gerente de Servicio Técnico.
- Ing. Mauricio Alvear. Jefe de Servicio Técnico.
- Ing. Paúl Auquilla. Coordinador de línea café.
- Ing. Gustavo Burbano.
- Tec. Oswaldo Cevallos.

- Srta. María José Carrión.
- Sra. Fabiola Rubín.

Una vez identificados los activos, procederemos a agruparlos en cinco capas o niveles que nos permitirán realizar el respectivo Análisis de Riesgos, esto lo realizaremos considerando el modelo MAGERIT[7].

Por lo tanto, las cinco capas a considerar, serán los siguientes:

- Capa 1. **Entorno:**
    - Equipamiento y suministros: Equipos, energía y climatización.
    - Personal: Dirección y operación.
    - Otros: Instalaciones y mobiliario.
- Capa 2. **Sistema de Información:**
    - Aplicaciones: Software.
    - Comunicaciones
    - Soportes de Información: USB, discos.
- Capa 3. **Información:**
    - Captura de datos.
    - Gestión de datos
- Capa 4. **Funciones de la Organización:**
    - Objetivos.
    - Bienes y servicios producidos.
- Capa 5. **Otros:**
    - Credibilidad.
    - Buena imagen.
    - Conocimiento acumulado.

[7] MAÑAS J. Antonio, MAGERIT – versión 2, Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. 2006. Ministerio de Administraciones Públicas, España. p. 18.

2.2.2 IDENTIFICACIÓN DE LOS MECANISMOS DE SALVAGUARDA EXISTENTES.

Una vez agrupados los activos en capas, es importante identificar los mecanismos de salvaguarda implantados en aquellos activos, describiendo las dimensiones de seguridad que estos ofrecen (Autenticidad, Confidencialidad, Integridad, Disponibilidad, A-C-I-D).

En el Anexo 2 podemos observar los mecanismos de salvaguarda implementados para cada activo.

2.2.3 IDENTIFICACIÓN DE LAS AMENAZAS.

Después de haber identificado los mecanismos de salvaguarda**,** se debe identificar las amenazas que sufren los activos del sistema, puesto que cada amenaza puede desencadenar muchas más.

Es necesario identificar la amenaza y establecer su origen, de esta manera se llega a conocer su capacidad y oportunidad de acción, así como su motivación en el caso de amenazas intencionadas.

En el Anexo 3, podemos observar las diferentes amenazas a las que están expuestos nuestros activos.

2.2.4 IDENTIFICACION DE VULNERABILIDADES.

Luego de haber identificado las amenazas en los activos, nuestra próxima actividad para el Análisis de Riesgos es la identificación de las vulnerabilidades.

MAGERIT evalúa la vulnerabilidad como la frecuencia de ocurrencia de la amenaza sobre el activo correspondiente[8].

Para poder valorar la vulnerabilidad, MAGERIT recomienda realizar un análisis subjetivo, en donde deberá tomarse en consideración la frecuencia de ocurrencia de la amenaza.

[8] MAÑAS J. Antonio, MAGERIT: Análisis y Gestión de Riesgos. 2010. Ministerio de Administraciones Públicas, España, p.27.

Para realizar la identificación de la Vulnerabilidad, la clasificamos en tres tipos:

- **Vulnerabilidad Intrínseca**, es aquella que no incluye ninguna salvaguarda.
- **Vulnerabilidad Efectiva**, es la que resulta de la aplicación de las salvaguardas existentes.
- **Vulnerabilidad Residual**, es la que resulta de aplicar las salvaguardas complementarias, aconsejadas como resultado del Análisis y Gestión de Riesgos.

Podemos observar en el Anexo 4, los diferentes niveles de vulnerabilidad a los que están expuestos los activos.

2.2.5 IDENTIFICACIÓN DE IMPACTOS.

Esta actividad, tiene por objetivo conocer el alcance del daño producido en el dominio, como consecuencia de la materialización de una amenaza sobre el activo.

El impacto, nos permite observar la gravedad de una agresión, es decir cómo se ve degradado nuestro activo y cómo esta agresión afecta las dimensiones de seguridad en la Organización (ACID).

El Anexo 5, nos muestra los activos y sus amenazas asociadas, así como el impacto de la materialización de las amenazas y las consecuencias que pueden producir dichos impactos.

2.2.5.1 TIPIFICAR IMPACTOS.

Una vez identificados los impactos y sus consecuencias, se debe clasificar a los impactos por el tipo de consecuencias que las amenazas pueden ocasionar en los activos impactados.

Por lo tanto tendremos:

- **Impactos con consecuencias cuantitativas:**
  - N1: Pérdidas Económicas.
  - N2: Pérdidas Inmateriales.

- N3: Responsabilidad Legal, Civil o Penal.

- **Impacto con consecuencias cualitativas orgánicas:**
  - L1: Pérdida de fondos patrimoniales.
  - L2: Incumplimiento de obligaciones legales.
  - L3: Perturbación o situación embarazosa.
  - L4: Daño a las personas.
- **Impactos con consecuencias cualitativas funcionales:**
  - SA: Autenticación.
  - SC: Confidencialidad.
  - SI: Integridad.
  - SD. Disponibilidad.

En el Anexo 6, podemos observar la clasificación de los impactos, según lo mencionado anteriormente; MAGERIT[9] recomienda realizar una valoración subjetiva de los impactos, en donde se calificará el daño hecho al sistema una vez que se produce el impacto ya sea de una manera directa o indirecta.

Los impactos están evaluados bajo el siguiente criterio:

Muy Bajo, Bajo, Medio, Alto, Muy Alto, Crítico.

2.2.6. EVALUACIÓN DEL RIESGO.

La información que obtuvimos anteriormente sobre la vulnerabilidad y el impacto, nos permiten establecer y estimar el riesgo.

El riesgo resulta de relacionar los distintos niveles de vulnerabilidad (puestos en filas), con los niveles de impacto (puestos en columnas).

En la siguiente tabla se relacionan los niveles de vulnerabilidad y los de impacto, en donde se observará que cuando el Impacto es Crítico, el riesgo alcanzará su máxima expresión, caso contrario, cuando el Impacto es Bajo o Muy Bajo, la consideración del riesgo para los valores más bajos de vulnerabilidad es mínimo o incluso inexistente.

[9] MAÑAS J. Antonio, MAGERIT: Análisis y Gestión de Riesgos. 2010. Ministerio de Administraciones Públicas, España, p.35.

De acuerdo a las recomendaciones de MAGERIT, se puede observar que el nivel de impacto influye más que la vulnerabilidad en la valoración final del Riesgo[10].

		VULNERABILIDAD						
		Muy Baja	**Baja**	**Media Baja**	**Media**	**Media Alta**	**Alta**	**Muy Alta**
IMPACTO	**Muy Bajo**	-	-	-	Mínimo	Mínimo	Mínimo	Mínimo
	Bajo	-	Mínimo	Bajo	Bajo	Bajo	Medio	Medio
	Medio	Mínimo	Bajo	Medio	Medio	Medio	Alto	Alto
	Alto	Medio	Medio	Medio	Alto	Alto	Alto	Alto
	Muy Alto	Alto	Alto	Alto	Muy Alto	Muy Alto	Máximo	Máximo
	Crítico	Máximo	Máximo	Máximo	Máximo	Máximo	Máximo	Máximo

Tabla 2: Determinación del nivel de Riesgo.

Fuente: MAGERIT – versión 2.
Elaborado por: Autores.

Una vez obtenido el valor de riesgo correspondiente a cada nivel de impacto y de vulnerabilidad, se debe realizar la evaluación del riesgo efectivo que existe en los activos de la Organización.

En el anexo 7, podemos observar la relación existente entre la vulnerabilidad y el impacto y como esto determina el riesgo para cada uno de los activos de la Organización.

[10] MAÑAS J. Antonio, MAGERIT: Análisis y Gestión de Riesgos. 2010. Ministerio de Administraciones Públicas, España, p. 36.

CAPÍTULO 3

GESTIÓN DEL RIESGO.

Esta etapa tiene como objetivo, identificar y seleccionar las funciones de salvaguarda apropiadas que nos permitan reducir el riesgo a un nivel aceptable, considerando los siguientes aspectos:

- Fortalecer salvaguardas existentes.
- Implementar nuevas salvaguardas.

Esta etapa será desarrollada en base a la información obtenida en el capítulo 2, en lo que respecta a la descripción de los componentes de riesgo, como los activos, mecanismos de salvaguarda existentes, amenazas, vulnerabilidades e impactos.

3.1 IDENTIFICACIÓN Y ESTIMACIÓN DE FUNCIONES Y SERVICIOS DE SALVAGUARDA.

3.1.1 IDENTIFICACIÓN DE FUNCIONES Y SERVICIOS DE SALVAGUARDA.

Esta tarea servirá para identificar funciones y servicios de salvaguarda que permitan reducir el nivel de riesgo en la Organización.

Las funciones y servicios de salvaguarda se determinarán según la agrupación de activos/amenazas donde se detecta mayor riesgo.[11] Al implementar la nueva salvaguarda, se tomará en consideración el tipo de activo que se quiere proteger, el tipo de amenaza, la dimensión de seguridad (ACID) y la consecuencia de aplicar la nueva salvaguarda.

En el Anexo 8 podemos observar lo anteriormente dicho.

3.1.2 ESTIMACIÓN DE EFECTIVIDAD DE FUNCIONES Y SERVICIOS DE SALVAGUARDA.

A partir de la información que proporciona el Anexo 8, se procede a estimar la efectividad de las nuevas funciones y servicios de salvaguarda.

[11] VER ANEXO 5.

El Anexo 9, nos muestra los pares activos/amenazas, el impacto, y las nuevas funciones de salvaguarda, así como la efectividad de aplicar dichas funciones.

3.2 REEVALUACIÓN DEL RIESGO.

En esta tarea se procede a aplicar las funciones y servicios de salvaguarda seleccionados anteriormente para reducir la frecuencia de ocurrencia de una amenaza y la reducción del impacto.

Los nuevos niveles de vulnerabilidad y de impacto se identifican y evalúan rehaciendo los procedimientos que se vieron en el Capítulo 2 "Identificación de Vulnerabilidades" e "Identificación de Impactos".

A partir de estos nuevos niveles de vulnerabilidad y de impacto, se podrá calcular el riesgo efectivo que resulta de la aplicación de las nuevas salvaguardas.

En el Anexo 10 se puede observar, que la aplicación de nuevas salvaguardas tiende a reducir el nivel de riesgo producido por las amenazas y los impactos; es decir, se puede observar el nivel de riesgo intrínseco y el nuevo nivel de riesgo efectivo que resulta de la aplicación de las nuevas salvaguardas. Cabe recalcar que estas salvaguardas son adicionales a las que la Organización aplica comúnmente en su Sistema de Información.

Vale la pena recordar que los impactos están valorados de una manera subjetiva, en donde se considera el daño que puede provocar el impacto dentro del Sistema.

CAPÍTULO 4

CONCLUSIONES Y RECOMENDACIONES.

4.1 CONCLUSIONES.

- Al realizar el Análisis y Gestión de Riesgos a los S.I. de la Organización, se observó que el impacto es el elemento que determina el nivel de riesgo, debido a que si un impacto llegara a materializarse, este afectaría gravemente a la Organización, por lo que, se vuelve importante su análisis y gestión.

- El Departamento de Servicio Técnico de Servindurama, es consciente del riesgo que implica el manejo de Sistemas de Información, por lo que, la Dirección de la Organización a partir del presente trabajo, realizó la implementación de mecanismos de salvaguarda que les permitirá proteger su información, tomando conciencia de los riesgos que se pueden producir con el avance de la tecnología.

- La herramienta PILAR Basic, sirvió de gran ayuda para entender que los Sistemas de Información están expuestos a amenazas que pueden afectar significativamente las operaciones de la Organización, ya que ésta posee una interfaz amigable para el usuario en el momento de su aplicación.

- El apoyo, tanto de la Dirección como del personal que labora en la Organización, fue fundamental para la elaboración del Proyecto, ya que ellos fueron quienes nos facilitaron la información que nos permitió conocer como se encontraban los Sistemas de Información dentro de la Organización.

4.2 RECOMENDACIONES.

- Al realizar la reevaluación del riesgo (Anexo 10), observamos que en el componente Servidor IBM, el nivel de riesgo resultante de la aplicación de nuevas salvaguardas (riesgo medio), es un valor muy alto para un equipo primordial en el funcionamiento de los S.I., por lo tanto, sugerimos a la Organización, implementar un servidor alterno que entre en funcionamiento en el momento que el servidor principal presente algún desperfecto, de esta manera el nivel de riesgo en dicho componente disminuirá.

- A los estudiantes interesados en realizar un Proyecto de Análisis y Gestión de Riesgos dentro de una Organización, sugerimos, mantener reuniones periódicas, con la Dirección, con los encargados del manejo de la información y con el personal que labora dentro de la Organización, para que de esta manera puedan obtener resultados ajustados a la realidad.

- A las Organizaciones que utilicen Tecnologías de Información, sugerimos, realizar por lo menos, una vez al año, un Análisis y Gestión de Riesgos a sus S.I., porque así, podrán conocer las fortalezas y debilidades de sus Sistemas y en el caso de presentarse debilidades, implementar mecanismos que permitan fortalecer sus Sistemas de Información.

BIBLIOGRAFIA.

- MAÑAS, José Antonio, MAGERIT: Análisis y Gestión de Riesgos. 2010. Ministerio de Administraciones Públicas, España.

- MAÑAS, José Antonio, MAGERIT – versión 2, Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. 2006. Ministerio de Administraciones Públicas, España.

- LÓPEZ C. Francisco, AMUDIO G. Miguel, CANDAU Javier, MAÑAS J. Antonio, MAGERIT – Fase de Inicio. 2006. Ministerio de Administraciones Públicas, España.

- LÓPEZ C. Francisco, AMUDIO G. Miguel, CANDAU. Javier, MAÑAS J. Antonio, MAGERIT – Catálogo de Elementos. 2006. Ministerio de Administraciones Públicas, España.

- MÉNDEZ B. Andrés, MAÑAS José Antonio. MANUAL DE USUARIO PILAR BASIC versión 4.4. 2010. Ministerio de Administraciones Públicas, España.

- FERNÁNDEZ J. Manuel. Parámetros Fundamentales para la implantación de un Sistema de Gestión de Seguridad de la Información. 2006. Grupo Nexus Consultores y Auditores.

Páginas Web:

http://publicaciones.administración.es

http://www.indurama.com/index.php?option=com_content&view=article&id=12&Itemid =14

http://www.ar-tools.com/index.html?tools/pilar_basic/download.htm

http://www.ar-tools.com/index.html?tools/pilar/first_time/

http://www.ar-tools.com/doc/help_es/index.html

http://www.ar-tools.com/doc/man-pilarbasic.pdf (STIC 470)

ANEXOS

ANEXO 1.

CUESTIONARIO REALIZADO AL JEFE NACIONAL DEL DEPARTAMENTO DE SERVICIO TÉCNICO DE SERVINDURAMA.

OBJETIVOS DEL CICLO DE VIDA.

¿Manejan Sistemas de Información y de Comunicación?

Si el sistema que utilizamos es el software de J.D. Edwards ERP del cliente Web, es un sistema de menús basado en HTML que ofrece la posibilidad de navegar por los menús del software de J.D. Edwards e iniciar una versión HTML de las aplicaciones de J.D. Edwards.

¿Qué tan confiables son los Sistemas de Información que operan?

Totalmente confiables ya que se operan en un ambiente web con un servidor de respaldos automatizados garantizando la recuperación de información al momento que se requiera.

¿Qué incidentes han existido con respecto a la seguridad de los Sistemas de Información?

No han existido inconvenientes graves, alguno que recuerdo fue por un problema del suministro de energía eléctrica, se presentó problemas en el motor propio con el que cuenta la empresa y finalmente la batería del UPS se agotó.

¿Son conscientes de los problemas que implican la utilización de las técnicas electrónicas, informáticas y telemáticas?

Por supuesto que sí, existe un plan de capacitación para todo el personal dependiendo de su función y responsabilidad para actualizar el conocimiento de los involucrados.

¿Han existido problemas por el cambio de la Tecnología usada?

Únicamente problemas de adaptabilidad por parte del usuario (mal uso, falta de conocimiento).

¿Se han realizado Proyectos de Seguridad?

Se cuenta con planes de seguridad, planes de contingencia en casa, planes de respaldo de la información, etc.

¿Cuál es la finalidad de la Unidad encargada en el manejo de la Información en el Departamento de Servicio Técnico?

La finalidad es la de garantizar que la información obtenida es oportuna, fiable y veraz, ya que ésta se utiliza para retroalimentar a clientes internos y externos los mismos que a raíz de esta información toman decisiones, acciones preventivas y acciones correctivas enfocados en una mejora continua de nuestros productos.

DOMINIO.

¿Qué medios utilizan para la captura de datos?

La captura de datos se realiza mediante el sistema de información CSMS JD Edwards (Customer Service Management System) que es un módulo de servicio el mismo que permite el ingreso de datos relacionados con el cliente, con el producto y con el daño que presenta el artefacto.

¿Se han identificado los riesgos críticos para el desarrollo exitoso del proyecto?

No.

¿Se prevé una forma de tratarlos?

No.

¿Es factible para su Organización llevar adelante el proyecto?

Si.

ÁMBITO DEL SISTEMA.

¿Existe alguna área que necesite mayor atención en el análisis?

El área que necesita mayor atención es el ingreso de datos ya que de esta información depende el éxito de la atención que brinda Servicio Técnico a sus clientes.

TECNOLOGÍA.

¿Ha existido problemas por el cambio de la de la Tecnología usada?

El mayor inconveniente que se presenta cuando existe un cambio de software o tecnología es el rechazo al cambio por parte del usuario, sin embargo este inconveniente se supera con capacitación y difusión de las ventajas existente.

¿Satisface la arquitectura actual de tecnología las necesidades de los usuarios?

Si satisface, sin embargo los requerimientos de los clientes finales cada vez son más exigentes que nos obligan a actualizar constantemente nuestra tecnología para brindar el servicio que nos proponemos como objetivo.

¿Puede usar de forma apropiada la tecnología sobre la que está construido el servicio para el usuario?

Si, por supuesto, ya que contamos con manuales de procedimientos que cuentan con certificación ISO.

¿Puede ser eficiente?

Si, al adquirir o desarrollar un software una de las expectativas a cubrir es el de la eficiencia.

¿Puede explotar los recursos existentes?

Sí, porque el sistema es flexible y permite la parametrización de acuerdo a las necesidades que se presenten.

¿Puede ser fiable y tolerante a fallos?

Estamos expuestos a un margen bajo de error por parte del usuario, a nivel de software estamos expuestos a fallas, sin embargo existe un plan de respaldo continuo de información.

¿Será robusta y flexible al cambio?

Es flexible, sin embargo se tiene que analizar el impacto que éste puede provocar, ya que al ser un sistema integral un cambio puede afectar el comportamiento del software.

¿Evolucionará fácilmente si se añaden requisitos?

Si, puede evolucionar ya que como comenté anteriormente el sistema es parametrizable y con el análisis previo de factibilidad que debe existir se puede adaptar a los requisitos existentes.

MITIGAR RIESGOS CRÍTICOS.

¿Se han identificado todos los riesgos críticos?

No, ya que existen riesgos que no se pueden identificar, inclusive hay riesgos que se los conoce únicamente cuando éstos se presentan.

¿Se han mitigado los riesgos identificados o existe un plan para mitigarlos?

Si, el Departamento de Sistemas de la Organización es el responsable de desarrollar los planes de mitigación de riesgos y un plan de contingencia en caso de que ocurran.

Fuente: Jefe de Servicio Técnico.
Elaborado por: Autores.

ANEXO 2.

MECANISMOS DE SALVAGUARDAS IMPLEMENTADOS.

Capa	Activo	Salvaguarda	Dimensión
Entorno	Servidor IBM	- Protección del Equipo dentro de la Organización. - Mantenimiento.	- Confidencialidad.
Entorno	Servidor Virtual	- Protección del Equipo dentro de la Organización.	- Confidencialidad. - Autenticidad.
Entorno	PC’s	- Acceso Limitado. - Mantenimiento Permanente.	- Autenticidad. - Confidencialidad.
Entorno	Impresora Hp	- Acceso Limitado. - Mantenimiento.	- Disponibilidad.
Entorno	Notebook’s Hp	- Protección del Equipo dentro de la Organización. - Mantenimiento permanente.	- Autenticidad. - Confidencialidad.
Entorno	Scanner.	- Acceso Limitado. - Mantenimiento.	- Disponibilidad.
Entorno	Mobiliario.	- Acceso Limitado.	- Confidencial. - Disponibilidad.
Sistema de Información	Aplicación de captura de datos.	- Identificación por Usuario y Password. - Respaldo de datos.	- Autenticidad. - Integridad. - Disponibilidad

Capa	Activo	Salvaguarda	Dimensión
Sistema de Información	Aplicación de Gestión de datos.	- Identificación por Usuario y Password. - Respaldo de Datos. - Almacenamiento permanente de datos.	- Autenticidad. - Integridad. - Confidencialidad. - Disponibilidad.
Sistema de Información	Sistema de Base de datos.	- Acceso a los datos únicamente a través del Sistema.	- Confidencialidad. - Disponibilidad. - Integridad.
Información - Captura	Identidad del Usuario Interno.	- Identificación por Usuario y Password.	- Autenticidad. - Integridad.
Información - Captura	Datos capturados durante sesión.	- Identificación por Usuario y Password.	- Autenticación.
Información - Captura	Datos de apoyo durante sesión.	- Identificación por Usuario y Password.	- Integridad.
Información – Gestión	Datos almacenados durante sesión.	- Identificación por Usuario y Password.	- Confidencialidad.
Información – Gestión	Documentos impresos para ser enviados.	- Limitación de acceso a las Instalaciones.	- Confidencialidad. - Disponibilidad.
Información – Gestión	Documentos Recibidos	- Limitación de acceso a las Instalaciones.	- Confidencialidad. - Disponibilidad.

Capa	Activo	Salvaguarda	Dimensión
Funciones de la Organización	Administración de permisos.	- Identificación por Usuario y Password.	- Confidencialidad.
Funciones de la Organización	Transferencia de datos.	- Transferencia entre dos o más dispositivos. Falla en la transferencia de los datos.	- Integridad. - Confidencialidad.
Funciones de la Organización	Relaciones entre Datos.	- Definición correcta del Modelo de Datos. - Limitación del acceso al sistema.	- Disponibilidad. - Integridad.

Fuente: MAGERIT: Análisis y Gestión de Riesgos
Elaborado por: Autores.

ANEXO 3.

AMENAZAS CORRESPONDIENTES A CADA ACTIVO.

Capa	Activo	Amenaza	Origen
Entorno	Servidor IBM	- Ataque físico. - Avería.	- Intención de causar daño a la Organización. - Mal uso o infortunio.
Entorno	Servidor Virtual	- Avería del servidor.	- Infortunio.
Entorno	PC’s	- Robo. - Ataque físico. - Avería.	- Intención de acceder en los datos. - Intención de invalidar los datos. - Mal uso o infortunio
Entorno	Impresora Hp	- Ataque Físico. - Avería.	- Intención de retrasar la actividad de la Organización. - Mal uso o infortunio.
Entorno	Notebook’s Hp	- Robo. - Ataque Físico. - Avería.	- Intención de acceder a los datos. - Intención de Invalidar los datos. - Mal uso o infortunio.
Entorno	Scanner	- Ataque Físico. -Avería.	- Intención de retrasar la actividad de la Organización. - Mal uso o infortunio.
Entorno	Mobiliario.	-Robo. - Ataque Físico.	- Intención de acceder a la documentación. - Intención de retrasar la actividad de la Organización.

Capa	Activo	Amenaza	Origen
Sistema de Información	Aplicación de captura de datos.	- Suplantación de identidad. - Introducción de datos incorrectos. - Descarga de datos en destino inapropiado.	- Intención de actuar con impunidad. - Intención de invalidar la actividad de la Organización, o error. - Intención de acceder a los datos y hacer que la Organización los pierda.
Sistema de Información	Aplicación de Gestión de datos.	- Suplantación de identidad. - Introducción de datos incorrectos. - Borrado de datos.	- Intención de acceder a información a la cual no se tiene permiso. - Intención de invalidar la actividad de la Organización, o error. - Intención de invalidar la actividad de la Organización.
Sistema de Información	Sistema de Base de datos.	- Acceso no permitido. - Modificación de datos malintencionada.	- Intención de acceder a los datos. - Intención de invalidar la actividad de la Organización.
Información – Captura	Identidad del Usuario Interno.	- Suplantación de identidad.	- Intención de actuar con impunidad.
Información – Captura	Datos capturados durante sesión.	- Suplantación de identidad.	- Intención de actuar con impunidad.
Información - Captura	Datos de apoyo durante sesión.	- Introducción de datos incorrectos.	- Intención de invalidar la actividad de la Organización, o error.
Información – Gestión	Datos almacenados durante sesión.	- Suplantación de identidad.	- Intención de acceder a información a la cual no se tiene permiso.

Capa	Activo	Amenaza	Origen
Información – Gestión	Documentos impresos para ser enviados.	-Robo. - Destrucción.	- Intención de acceder a la documentación. - Intención de retrasar la actividad de la Organización.
Información – Gestión	Documentos Recibidos	-Robo. - Destrucción.	- Intención de acceder a la documentación. - Intención de retrasar la actividad de la Organización.
Funciones de la Organización	Administración de permisos.	- Suplantación de identidad.	- Intención de obtener más permisos de los estipulados.
Funciones de la Organización	Transferencia de datos.	- Acceso no permitido a la información. -Error en la comunicación	- Intención de acceder a la información. - Intención de retrasar la actividad de la organización, o fallo técnico.
Funciones de la Organización	Relaciones entre Datos.	-Error en la definición del modelo de Datos. -Accedo no permitido a la Base de Datos.	-Mala aplicación de la metodología de desarrollo. -Intención de invalidar la actividad de la Organización.

Fuente: MAGERIT: Análisis y Gestión de Riesgos
Elaborado por: Autores.

ANEXO 4.

VULNERABILIDADES CORRESPONDIENTES A CADA ACTIVO.

CAPA	ACTIVOS	AMENAZAS	SALVAGUARDAS	VULNERABILIDADES		
				INTRÍNSECA	EFECTIVA	RESIDUAL
Entorno	Servidor IBM	- Ataque físico. - Avería.	- Protección del Equipo dentro de la Organización. - Mantenimiento	-Muy baja. -Muy baja.	-Casi nula. -Se reduce en gran medida.	
Entorno	Servidor Virtual	- Avería del servidor.	- Protección del Equipo dentro de la Organización.	-Muy baja.	-Se reduce en gran medida.	
Entorno	PC’s	- Robo. - Ataque físico. - Avería.	- Acceso Limitado. - Acceso Limitado. - Mantenimiento Permanente.	-Muy baja. -Muy baja. -Media	-Se reduce en gran medida. - Casi nula. -Se reduce en gran medida.	
Entorno	Impresora Hp	- Ataque Físico. - Avería.	-Acceso Limitado. -Mantenimiento	-Muy baja. -Media.	-Casi nula. -Se reduce en gran medida.	

CAPA	ACTIVOS	AMENAZAS	SALVAGUARDAS	VULNERABILIDADES		
				INTRÍNSECA	EFECTIVA	RESIDUAL
Entorno	Notebook's Hp	- Robo. - Ataque Físico. - Avería.	-Protección del Equipo dentro de la Organización. -Protección del Equipo dentro de la Organización. - Mantenimiento permanente.	-Muy baja. -Muy baja. -Media	-Se reduce en gran medida. - Casi nula. - Se reduce en gran medida.	
Entorno	Scanner	- Ataque Físico. -Avería.	-Acceso Limitado. -Mantenimiento.	-Muy baja. -Media.	- Casi nula. -Se reduce en gran medida.	
Entorno	Mobiliario.	-Robo. - Ataque Físico.	- Acceso Limitado. - Acceso Limitado.	- Muy baja. - Muy baja.	- Casi nula. - Casi nula.	
Sistema de Información	Aplicación de captura de datos.	- Suplantación de identidad. - Introducción de datos incorrectos. - Descarga de datos en destino inapropiado.	- Identificación por Usuario y Password. - Respaldo de datos. - Reconocimiento de destino.	-Media -Alta. -Media-Alta	- Se reduce en gran medida. - Se reduce al mínimo. - Se reduce al mínimo.	- Se propone al usuario la elección cuidada de contraseñas.

CAPA	ACTIVOS	AMENAZAS	SALVAGUARDAS	VULNERABILIDADES		
				INTRÍNSECA	EFECTIVA	RESIDUAL
Sistema de Información	Aplicación de Gestión de datos.	- Suplantación de identidad. - Introducción de datos incorrectos. - Borrado de datos.	- Identificación por Usuario y Password. - Respaldo de Datos. - Almacenamiento permanente de datos.	-Media-baja -Media Alta. - Media.	-Se reduce en gran medida. -Se reduce al mínimo. -Se reduce al mínimo.	-Se propone al usuario la elección cuidada de contraseñas. -Se propone el uso de la papelera de reciclaje.
Sistema de Información	Sistema de Base de datos.	- Acceso no permitido. - Modificación malintencionada de datos.	- Acceso a los datos únicamente a través del sistema.	- Muy alta. - Media –baja.	- Se reduce aunque no lo suficiente. -Se reduce en gran medida.	-Se propone el bloqueo a la base de datos.
Información - Captura	Identidad del Usuario Interno.	- Suplantación de identidad	- Identificación por Usuario y Password.	- Media.	-Se reduce en gran medida.	-Responsabilidad del usuario de cuidar su contraseña.
Información - Captura	Datos capturados durante sesión.	- Suplantación de identidad.	- Identificación por Usuario y Password.	- Media	- Se reduce en gran medida.	- Se recomienda al usuario cuidar su contraseña.
Información - Captura	Datos de apoyo durante sesión.	- Introducción de datos incorrectos.	- Identificación por Usuario y Password.	- Media	-Se reduce en gran medida.	

CAPA	ACTIVOS	AMENAZAS	SALVAGUARDAS	VULNERABILIDADES		
				INTRÍNSECA	EFECTIVA	RESIDUAL
Información - Gestión	Datos almacenados durante sesión.	- Suplantación de identidad.	- Identificación por Usuario y Password.	- Media	- Se reduce en gran medida.	-Será responsabilidad de los usuarios no difundir las contraseñas.
Información - Gestión	Documentos impresos para ser enviados.	- Robo. -Destrucción.	- Limitación de acceso a las Instalaciones.	- Media-Alta	-Se reduce al mínimo.	
Información - Gestión	Documentos Recibidos	-Robo. - Destrucción.	- Limitación de acceso a las Instalaciones.	- Media-Alta	-Se reduce al mínimo.	
Funciones de la Organización	Administración de permisos.	- Suplantación de identidad.	- Identificación por Usuario y Password.	- Media-Alta	- Se reduce en gran medida.	- Será responsabilidad de los usuarios no difundir las contraseñas.
Funciones de la Organización	Transferencia de datos.	- Acceso no permitido a la comunicación. -Error en la comunicación	-Transferencia entre dos o más dispositivos. -Señales de dispositivos listos.	-Alta -Media	- Se reduce totalmente. -Se reduce su efecto totalmente.	

CAPA	ACTIVOS	AMENAZAS	SALVAGUARDAS	VULNERABILIDADES		
				INTRÍNSECA	EFECTIVA	RESIDUAL
Funciones de la Organización	Relaciones entre Datos.	-Error en la definición del modelo de Datos. -Acceso no permitido a la base de Datos.	- Definición correcta del Modelo de Datos. -Limitación del acceso al sistema.	-Media- Alta -Muy alta.	-Se reduce todo lo posible. -Se reduce aunque no lo suficiente.	- -Se propone el bloqueo a la base de datos.

Fuente: MAGERIT: Análisis y Gestión de Riesgos.
Elaborado por: Autores.

ANEXO 5.

IDENTIFICACIÓN DE IMPACTOS.

CAPA	ACTIVOS	AMENAZAS	IMPACTO	CONSECUENCIAS
Entorno	Servidor IBM	- Ataque físico. - Avería.	- Reducción de Disponibilidad.	-Paralización Total de las Actividades.
Entorno	Servidor Virtual	- Avería del servidor.	- Reducción de Confidencialidad.	-Paralización Parcial de las Actividades.
Entorno	PC’s	- Robo. - Ataque físico. - Avería.	- Reducción de Confidencialidad. - Reducción de Autenticidad. - Reducción de Disponibilidad. - Reducción de Confidencialidad.	- Pérdida del destino de datos. - Suplantación de Identidad. - Pérdida del destino de datos. - Pérdida del destino de datos.
Entorno	Impresora Hp	- Ataque Físico. - Avería.	- Reducción de Disponibilidad.	- Pérdida de la representación de datos.

CAPA	ACTIVOS	AMENAZAS	IMPACTO	CONSECUENCIAS
Entorno	Notebook's Hp	- Robo. - Ataque Físico. - Avería.	- Reducción de Confidencialidad. - Reducción de Autenticidad. - Reducción de Disponibilidad. - Reducción de Confidencialidad.	- Pérdida del destino de datos. - Suplantación de Identidad. - Pérdida del destino de datos. - Pérdida del destino de datos.
Entorno	Scanner	- Ataque Físico. - Avería.	- Reducción de Disponibilidad.	- Pérdida de la representación de datos.
Entorno	Mobiliario.	- Robo. - Ataque Físico.	- Reducción de Confidencialidad. - Reducción de Disponibilidad. - Reducción de Disponibilidad.	- Robo de Documentos importantes para la Organización. - Destrucción parcial o total de Documentos.
Sistema de Información	Aplicación de captura de datos.	- Suplantación de identidad. - Introducción de datos incorrectos. - Descarga de datos en destino inapropiado.	- Reducción de Autenticidad. - Reducción de Integridad. - Reducción de disponibilidad.	- - Introducción de datos incorrectos en la B.D. - Pérdida de datos.

CAPA	ACTIVOS	AMENAZAS	IMPACTO	CONSECUENCIAS
Sistema de Información	Aplicación de Gestión de datos.	- Suplantación de identidad. - Introducción de datos incorrectos. - Borrado de datos.	- Reducción de Confidencialidad. - Reducción de Autenticidad. - Reducción de Integridad. - Reducción de Integridad. - Reducción de Disponibilidad.	- Acceso a datos personales. - Cambios en los permisos - Borrado de datos. - Introducción de datos incorrectos en la B.D. - Introducción de datos incorrectos en la B.D. - Pérdida parcial o total de los datos.
Sistema de Información	Sistema de Base de datos.	- Acceso no permitido. - Modificación de datos malintencionada.	- Reducción de la Confidencialidad. - Reducción de Integridad. - Reducción de Disponibilidad.	- Acceso a datos personales. - Suplantación de identidad. - Modificación Malintencionada de datos. - Introducción de datos incorrectos.
Información – Captura	Identidad del Usuario Interno.	- Suplantación de identidad.	- Reducción de Autenticación.	- Introducción de datos incorrectos al subsistema.
Información – Captura	Datos capturados durante sesión.	- Suplantación de identidad.	- Reducción de Autenticidad.	- Introducción de datos incorrectos al subsistema.
Información - Captura	Datos de apoyo durante sesión.	- Introducción de datos incorrectos.	- Reducción de Integridad.	- Introducción de datos incorrectos al subsistema.

CAPA	ACTIVOS	AMENAZAS	IMPACTO	CONSECUENCIAS
Información – Gestión	Datos almacenados durante sesión.	- Suplantación de identidad.	- Reducción de Autenticidad. - Reducción de Confidencialidad. - Reducción de Integridad. - Reducción de Disponibilidad.	- Acceso a datos personales. - Cambio en los permisos. - Introducción de datos incorrectos al subsistema. - Borrado de datos
Información – Gestión	Documentos impresos para ser enviados.	-Robo. -Destrucción.	- Reducción de Confidencialidad. - Reducción de Disponibilidad.	Necesidad de volver a producirlos.
Información – Gestión	Documentos Recibidos	-Robo. - Destrucción.	- Reducción de Confidencialidad. - Reducción de Disponibilidad.	Necesidad de volver a producirlos.
Funciones de la Organización	Administración de permisos.	- Suplantación de identidad.	- Reducción de Autenticidad. - Reducción de Confidencialidad.	- Suplantación de Identidad.
Funciones de la Organización	Transferencia de datos.	- Acceso no permitido a la comunicación. -Error en la comunicación	- Reducción de Confidencialidad. - Reducción de Integridad.	- Error en la comunicación. - Necesidad de repetir la transferencia.

CAPA	ACTIVOS	AMENAZAS	IMPACTO	CONSECUENCIAS
Funciones de la Organización	Relaciones entre Datos.	- Error en la definición del modelo de Datos. - Accedo no permitido a la base de Datos.	- Reducción de Integridad. - Reducción de Disponibilidad. - Reducción de Confidencialidad. - Reducción de Integridad. - Reducción de Disponibilidad.	- Necesidad de rediseñar el modelo de datos. - Acceso no permitido a la Base de Datos.

Fuente: MAGERIT: Análisis y Gestión de Riesgos.
Elaborado por: Autores.

ANEXO 6.

TIPIFICACIÓN DE IMPACTOS.

ACTIVOS	AMENAZAS	IMPACTO	CONSECUENCIAS			Valoración
			Cuantitativas	Cualitativas Orgánicas	Cualitativas Funcionales	
Servidor IBM	- Ataque físico. - Avería.	- Reducción de Disponibilidad.	N1, N2	L1, L3	SD	Crítico.
Servidor Virtual	- Avería del servidor.	- Reducción de Confidencialidad.	N1, N2	L3	SD	Crítico.
PC's	- Robo.	- Reducción de Confidencialidad. - Reducción de Autenticidad.	N1, N2, N3	L2	SC, SD	Crítico.
	- Ataque físico.	- Reducción de Disponibilidad.	N1, N2	L2, L4	SD	Muy Alto.
	- Avería.	- Reducción de Confidencialidad.	N1, N2	L2	SD	Muy Alto.
Impresora Hp	- Ataque Físico. - Avería.	- Reducción de Disponibilidad.	N1	L4	SD	Alto.

ACTIVOS	AMENAZAS	IMPACTO	CONSECUENCIAS			Valoración
			Cuantitativas	Cualitativas Orgánicas	Cualitativas Funcionales	
Notebook's Hp	- Robo.	- Reducción de Confidencialidad. - Reducción de Autenticidad.	N1, N2, N3	L2	SC, SD	Crítico.
	- Ataque Físico.	- Reducción de Disponibilidad.	N1, N2	L2, L4	SD	Muy Alto.
	- Avería.	- Reducción de Confidencialidad.	N1, N2	L2	SD	Muy Alto.
Scanner	- Ataque Físico. - Avería.	- Reducción de Disponibilidad.	N1	L4	SD	Alto.
Mobiliario.	-Robo.	- Reducción de Confidencialidad. - Reducción de Disponibilidad.	N1	L2	SC,SD	Alto.
	- Ataque Físico.	- Reducción de Disponibilidad.	N1	L2, L4	SD	Alto.
Aplicación de captura de datos.	- Suplantación de identidad.	- Reducción de Autenticidad.	N2	L2	SA	Muy Alto.
	- Introducción de datos incorrectos.	- Reducción de Integridad.	N2	L2	SI	Muy Alto.
	- Descarga de datos en destino inapropiado.	- Reducción de disponibilidad.	N2	-	SD	Alto.

ACTIVOS	AMENAZAS	IMPACTO	CONSECUENCIAS			Valoración
			Cuantitativas	Cualitativas Orgánicas	Cualitativas Funcionales	
Aplicación de Gestión de datos.	- Suplantación de identidad.	- Reducción de Confidencialidad. - Reducción de Autenticidad.	N2, N3	L2	SC, SA	Crítico.
	- Introducción de datos incorrectos.	- Reducción de Integridad.	N2, N3	L2	SI	Crítico.
	- Borrado de datos.	- Reducción de Integridad. - Reducción de Disponibilidad.	N2, N3	L2	SI, SD	Crítico.
Sistema de Base de datos.	- Acceso no permitido.	- Reducción de la Confidencialidad.	N2, N3	L2	SC	Crítico.
	- Modificación de datos malintencionada.	- Reducción de Integridad. - Reducción de Disponibilidad.	N2, N3	L2	SI, SD	Crítico.
Identidad del Usuario Interno.	- Suplantación de identidad	- Reducción de Autenticación.	N2	L2	SA	Muy Alto.
Datos capturados durante sesión.	- Suplantación de identidad.	- Reducción de Autenticidad.	N2	L2	SA	Muy Alto.

ACTIVOS	AMENAZAS	IMPACTO	CONSECUENCIAS			Valoración
			Cuantitativas	Cualitativas Orgánicas	Cualitativas Funcionales	
Datos de apoyo durante sesión.	- Introducción de datos incorrectos.	- Reducción de Integridad.	N2	L2	SI	Muy Alto.
Datos almacenados durante sesión.	- Suplantación de identidad.	- Reducción de Autenticidad. - Reducción de Confidencialidad. - Reducción de Integridad. - Reducción de Disponibilidad	N2, N3	L2	SA, SC, SI, SD	Crítico.
Documentos impresos para ser enviados.	-Robo. -Destrucción.	- Reducción de Confidencialidad. - Reducción de Disponibilidad.	N2	L2	SC, SD	Alto. Medio.
Documentos Recibidos	-Robo. - Destrucción.	- Reducción de Confidencialidad. - Reducción de Disponibilidad.	N2	L2	SC, SD	Alto. Medio.
Administración de permisos.	- Suplantación de identidad.	- Reducción de Autenticidad. - Reducción de Confidencialidad.	N2, N3	L2	SA, SC	Crítico.

ACTIVOS	AMENAZAS	IMPACTO	CONSECUENCIAS			Valoración
			Cuantitativas	Cualitativas Orgánicas	Cualitativas Funcionales	
Transferencia de datos.	- Acceso no permitido a la comunicación. -Error en la comunicación	- Reducción de Confidencialidad. - Reducción de Integridad.	N2	L2	SC, SI	Muy Alto. Medio.
Relaciones entre Datos.	- Error en la definición del modelo de Datos. - Accedo no permitido a la base de Datos.	- Reducción de Integridad. - Reducción de Disponibilidad. - Reducción de Confidencialidad. - Reducción de Integridad. - Reducción de Disponibilidad.	N2 N2, N3	L2 L2	SI, SD SC, SI, SD	Crítico. Crítico.

Fuente: MAGERIT: Análisis y Gestión de Riesgos.
Elaborado por: Autores.

ANEXO 7.

RIESGO EXISTENTE EN LOS ACTIVOS.

CAPA	ACTIVOS	AMENAZAS	SALVAGUARDAS	VULNERABILIDAD		IMPACTO	RIESGO INTRÍNSECO	RIESGO EFECTIVO
				INTRÍNSECA	EFECTIVA			
Entorno	Servidor IBM	- Ataque físico. - Avería.	-Protección del Equipo dentro de la Organización. -Mantenimiento.	- Muy baja en el entorno en que se realiza la actividad. - Muy baja	-Casi nula. -Se reduce en gran medida.	Crítico Crítico	Máximo Máximo	Máximo Máximo
Entorno	Servidor Virtual	Avería del servidor.	- Protección del Equipo dentro de la Organización.	- Muy baja	-Se reduce en gran medida.	Crítico	Máximo	Máximo
Entorno	PC’s	- Robo. - Ataque físico. - Avería.	- Acceso Limitado. - Acceso Limitado. - Mantenimiento Permanente.	- Muy baja. - Muy baja. - Media	-Se reduce en gran medida. - Casi nula. -Se reduce en gran medida.	Crítico Muy Alto Muy Alto	Máximo Alto Muy Alto	Máximo Alto Alto
Entorno	Impresora Hp	- Ataque Físico. - Avería.	- Acceso Limitado. - Mantenimiento.	- Muy baja. - Media.	- Casi nula. -Se reduce en gran medida.	Alto Alto	Medio Alto	Medio Medio

CAPA	ACTIVOS	AMENAZAS	SALVAGUARDAS	VULNERABILIDAD		IMPACTO	RIESGO INTRÍNSECO	RIESGO EFECTIVO
				INTRÍNSECA	EFECTIVA			
Entorno	Notebook's Hp	- Robo. - Ataque físico. - Avería.	- Protección del Equipo dentro de la Organización. - Protección del Equipo dentro de la Organización. - Mantenimiento permanente.	- Muy baja. -Muy baja. -Media	- Se reduce en gran medida. - Casi nula. -Se reduce en gran medida.	Crítico Muy Alto Muy Alto	Máximo Alto Muy Alto	Máximo Alto Alto
Entorno	Scanner	- Ataque Físico. - Avería.	- Acceso Limitado. - Mantenimiento.	-Muy baja. -Media.	-Casi nula. -Se reduce en gran medida.	Alto Alto	Medio Alto	Medio Medio
Entorno	Mobiliario.	-Robo. - Ataque Físico.	- Acceso Limitado. - Acceso Limitado.	-Muy baja. -Muy baja.	-Casi nula. -Casi nula.	Alto Alto	Medio Medio	Medio Medio
Sistema de Información	Aplicación de captura de datos.	- Suplantación de identidad. - Introducción de datos incorrectos. - Descarga de datos en destino inapropiado.	- Identificación por Usuario y Password. - Respaldo de datos. - Reconocimiento de destino.	-Media - Alta. -Media-Alta	-Se reduce en gran medida. - Se reduce al mínimo. -Se reduce al mínimo.	Muy Alto Muy Alto Alto	Muy Alto Máximo Alto	Alto Alto Medio

CAPA	ACTIVOS	AMENAZAS	SALVAGUARDAS	VULNERABILIDAD		IMPACTO	RIESGO INTRÍNSECO	RIESGO EFECTIVO
				INTRÍNSECA	EFECTIVA			
Sistema de Información	Aplicación de Gestión de datos.	- Suplantación de identidad.	- Identificación por Usuario y Password.	-Media-baja	-Se reduce en gran medida.	Crítico	Máximo	Máximo
		- Introducción de datos incorrectos.	- Respaldo de Datos.	-Media Alta.	-Se reduce al mínimo.	Crítico	Máximo	Máximo
		- Borrado de datos.	- Almacenamiento permanente de datos.	-Media.	-Se reduce al mínimo.	Crítico	Máximo	Máximo
Sistema de Información	Sistema de Base de datos.	- Acceso no permitido.	- Acceso a los datos únicamente a través del sistema a través de identificación de usuario y password.	-Muy alta.	- Se reduce aunque no lo suficiente.	Crítico	Máximo	Máximo
		- Modificación de datos malintencionada		-Media –baja.	-Se reduce en gran medida.	Crítico	Máximo	Máximo
Información - Captura	Identidad del Usuario Interno.	- Suplantación de identidad	- Identificación por Usuario y Password.	-Media.	-Se reduce en gran medida.	Muy Alto	Muy Alto	Alto
Información - Captura	Datos capturados durante sesión.	- Suplantación de identidad.	- Identificación por Usuario y Password.	-Media	- Se reduce en gran medida.	Muy Alto	Muy Alto	Alto
Información - Captura	Datos de apoyo durante sesión.	- Introducción de datos incorrectos.	- Identificación por Usuario y Password.	-Media	-Se reduce en gran medida.	Muy Alto	Muy Alto	Alto
Información - Gestión	Datos almacenados durante sesión.	- Suplantación de identidad.	- Identificación por Usuario y Password.	-Media	-Se reduce en gran medida.	Crítico	Máximo	Máximo

CAPA	ACTIVOS	AMENAZAS	SALVAGUARDAS	VULNERABILIDAD		IMPACTO	RIESGO INTRÍNSECO	RIESGO EFECTIVO
				INTRÍNSECA	EFECTIVA			
Información - Gestión	Documentos impresos para ser enviados.	-Robo. - Destrucción.	- Limitación de acceso a las Instalaciones.	-Media-Alta	-Se reduce al mínimo.	Alto Medio	Alto Medio	Medio Mínimo
Información – Gestión	Documentos Recibidos	-Robo. - Destrucción.	- Limitación de acceso a las Instalaciones.	-Media-Alta	-Se reduce al mínimo.	Alto Medio	Alto Medio	Medio Mínimo
Funciones de la Organización	Administración de permisos.	- Suplantación de identidad.	- Identificación por Usuario y Password.	-Media-Alta	Se reduce en gran medida.	Crítico	Máximo	Máximo
Funciones de la Organización	Transferencia de datos.	- Acceso no permitido a la comunicación. -Error en la comunicación	-Transferencia entre dos o más dispositivos. -Señales de dispositivos listos.	-Alta -Media	- Se reduce totalmente. - Se reduce su efecto totalmente.	Muy Alto Medio	Máximo Medio	Alto Mínimo
Funciones de la Organización	Relaciones entre Datos.	-Error en la definición del modelo de Datos. -Acceso no permitido a la base de Datos.	- Definición correcta del Modelo de Datos. -Limitación del acceso al sistema.	-Media- Alta -Muy Alta.	-Se reduce todo lo posible. -Se reduce aunque no lo suficiente.	Crítico Crítico	Máximo Máximo	Máximo Máximo

Fuente: MAGERIT: Análisis y Gestión de Riesgos.
Elaborado por: Autores.

ANEXO 8

IDENTIFICACIÓN DE FUNCIONES Y SERVICIOS DE SALVAGUARDA.

ACTIVOS	AMENAZAS	IMPACTO	SALVAGUARDA	CONSECUENCIAS DE APLICAR LAS SALVAGUARDAS
Servidor IBM	- Ataque físico. - Avería.	- Reducción de Disponibilidad. - Reducción de Disponibilidad.	-Contratar seguro. -Mantenimiento permanente. - Protección Física de los equipos.	-Recuperación de coste. -Aumento de Disponibilidad.
Servidor Virtual	- Avería del servidor.	- Reducción de Confidencialidad.	-Mantenimiento.	-Aumento de Disponibilidad.
PC’s	- Robo. - Ataque físico. - Avería.	- Reducción de Confidencialidad. - Reducción de Autenticidad. - Reducción de Disponibilidad. - Reducción de Confidencialidad.	- Contratar seguro. -Contratar seguro. -Mantenimiento y copias de seguridad.	-Recuperación de coste. -Aumento de Disponibilidad. -Aumento de Disponibilidad.

ACTIVOS	AMENAZAS	IMPACTO	SALVAGUARDA	CONSECUENCIAS DE APLICAR LAS SALVAGUARDAS
Impresora Hp	- Ataque Físico. - Avería.	- Reducción de Disponibilidad.	- Contratar seguro. -Mantenimiento.	-Ahorro de coste. -Aumento de Disponibilidad.
Notebook's Hp	- Robo. - Ataque Físico. - Avería.	- Reducción de Confidencialidad. - Reducción de Autenticidad. - Reducción de Disponibilidad. - Reducción de Confidencialidad.	-Contratar seguro. -Contratar seguro. -Mantenimiento y copias de seguridad.	-Recuperación de coste. - Aumento de Autenticidad. -Aumento de Disponibilidad. -Aumento de Disponibilidad.
Scanner	- Ataque Físico. - Avería.	- Reducción de Disponibilidad.	- Contratar seguro. - Mantenimiento.	-Ahorro de coste. -Aumento de Disponibilidad.
Mobiliario.	- Robo. - Ataque Físico.	- Reducción de Confidencialidad. - Reducción de Disponibilidad. - Reducción de Disponibilidad.	-Contratar seguro. -Contratar seguro.	-Aumento de Disponibilidad. -Aumento de Disponibilidad.

ACTIVOS	AMENAZAS	IMPACTO	SALVAGUARDA	CONSECUENCIAS DE APLICAR LAS SALVAGUARDAS
Aplicación de captura de datos.	- Suplantación de identidad. - Introducción de datos incorrectos. - Descarga de datos en destino inapropiado.	- Reducción de Autenticidad. - Reducción de Integridad. - Reducción de disponibilidad.	- Elección adecuada de contraseñas. - Identificación individualizada de todos los usuarios. -Comprobación de Integridad en la base de datos. -Comprobación de destino.	-Aumento de Autenticidad. -Aumento de Integridad. -Aumento de Disponibilidad.
Aplicación de Gestión de datos.	- Suplantación de identidad. - Introducción de datos incorrectos. - Borrado de datos.	- Reducción de Confidencialidad. - Reducción de Autenticidad. - Reducción de Integridad. - Reducción de Integridad. - Reducción de Disponibilidad.	-Elección adecuada de contraseñas. - Identificación individualizada de todos los usuarios. -Comprobación de Integridad en la base de datos. -Incorporar el uso de la “Papelera de reciclaje.”	-Aumento de Confidencialidad. -Aumento de Autenticidad. -Aumento de Integridad. -Aumento de Integridad. -Aumento de Disponibilidad.

ACTIVOS	AMENAZAS	IMPACTO	SALVAGUARDA	CONSECUENCIAS DE APLICAR LAS SALVAGUARDAS
Sistema de Base de datos.	- Acceso no permitido. - Modificación de datos malintencionada.	- Reducción de la Confidencialidad. - Reducción de Integridad. - Reducción de Disponibilidad.	- Bloquear acceso a la base de datos. - Bloqueo de sesión al dejar desatendidos los equipos.	-Aumento de Confidencialidad. -Aumento de Integridad. -Aumento de Disponibilidad.
Identidad del Usuario Interno.	- Suplantación de identidad.	- Reducción de Autenticación.	- Elección adecuada de contraseñas. - Identificación individualizada de todos los usuarios.	- Aumento de Autenticidad.
Datos capturados durante sesión.	- Suplantación de identidad.	- Reducción de Autenticidad.	- Elección adecuada de contraseñas. - Identificación individualizada de todos los usuarios.	- Aumento de Autenticidad.
Datos de apoyo durante sesión.	- Introducción de datos incorrectos.	- Reducción de Integridad.	-Comprobación de Integridad en la base de datos. - Verificación automática de ortografía.	-Aumento de Integridad.

ACTIVOS	AMENAZAS	IMPACTO	SALVAGUARDA	CONSECUENCIAS DE APLICAR LAS SALVAGUARDAS
Datos almacenados durante sesión.	- Suplantación de identidad.	- Reducción de Autenticidad. - Reducción de Confidencialidad. - Reducción de Integridad. - Reducción de Disponibilidad	- Elección adecuada de contraseñas. - Identificación individualizada de todos los usuarios.	-Aumento de Autenticidad. -Aumento de Confidencialidad. -Aumento de Integridad. -Aumento de Disponibilidad.
Documentos impresos para ser enviados.	-Robo. -Destrucción.	- Reducción de Confidencialidad. - Reducción de Disponibilidad.	-Restaurar copias.	-Aumento de Confidencialidad. -Aumento de Disponibilidad.
Documentos Recibidos	-Robo. - Destrucción.	- Reducción de Confidencialidad. - Reducción de Disponibilidad.	-Restaurar copias.	-Aumento de Confidencialidad. -Aumento de Disponibilidad.
Administración de permisos.	- Suplantación de identidad.	- Reducción de Autenticidad. - Reducción de Confidencialidad.	- Elección adecuada de contraseñas. - Identificación individualizada de todos los usuarios.	-Aumento de Autenticidad. -Aumento de Confidencialidad.

ACTIVOS	AMENAZAS	IMPACTO	SALVAGUARDA	CONSECUENCIAS DE APLICAR LAS SALVAGUARDAS
Transferencia de datos.	- Acceso no permitido a la comunicación. -Error en la comunicación	- Reducción de Confidencialidad. - Reducción de Integridad.	-Comprobación de origen. - Inclusión de cláusulas de confidencialidad. -Tratamiento de transacción.	-Aumento de Confidencialidad. -Aumento de Integridad.
Relaciones entre Datos.	- Error en la definición del modelo de Datos. - Accedo no permitido a la base de Datos.	- Reducción de Integridad. - Reducción de Disponibilidad. - Reducción de Confidencialidad. - Reducción de Integridad. - Reducción de Disponibilidad.	-Formación en desarrollo de software. -Bloquear acceso a la base de datos. - Bloqueo de sesión al dejar desatendidos los equipos.	-Aumento de Integridad. -Aumento de Disponibilidad. -Aumento de Confidencialidad. -Aumento de Integridad. -Aumento de Disponibilidad.

Fuente: MAGERIT: Análisis y Gestión de Riesgos.
Elaborado por: Autores.

ANEXO 9.

ESTIMACION EFECTIVA DE FUNCIONES Y SERVICIOS DE SALVAGUARDA.

ACTIVOS	AMENAZAS	IMPACTO	Valoración Intrinseca (Impacto)	SALVAGUARDA	Valoración Efectiva (Impacto)
Servidor IBM	- Ataque físico. - Avería.	- Reducción de Disponibilidad.	-Crítico. -Crítico.	-Contratar seguro. -Mantenimiento	-Alto. -Alto.
Servidor Virtual	- Avería del servidor.	- Reducción de Confidencialidad.	-Crítico.	-Mantenimiento.	-Alto.
PC's	- Robo. - Ataque físico. - Avería.	- Reducción de Confidencialidad. - Reducción de Autenticidad. - Reducción de Disponibilidad. - Reducción de Confidencialidad.	- Crítico. -Muy Alto. -Muy Alto.	- Contratar seguro. - Contratar seguro. -Mantenimiento y copias de seguridad.	- Alto. -Alto. -Alto.
Impresora Hp	- Ataque Físico. - Avería.	- Reducción de Disponibilidad.	- Alto. - Alto.	- Mantenimiento.	- Muy bajo. - Bajo.

ACTIVOS	AMENAZAS	IMPACTO	Valoración Intrinseca (Impacto)	SALVAGUARDA	Valoración Efectiva (Impacto)
Notebook's Hp	- Robo.	- Reducción de Confidencialidad. - Reducción de Autenticidad.	-Crítico.	-Contratar seguro.	- Alto.
	- Ataque Físico.	- Reducción de Disponibilidad.	-Muy Alto.	-Mantenimiento y copias de seguridad.	-Alto.
	- Avería.	- Reducción de Confidencialidad.	-Muy Alto.	-Mantenimiento y copias de seguridad.	-Alto.
Scanner	- Ataque Físico.	- Reducción de Disponibilidad.	-Alto.	- Mantenimiento.	- Muy bajo.
	- Avería.		-Alto.		- Bajo.
Mobiliario.	- Robo.	- Reducción de Confidencialidad. - Reducción de Disponibilidad.	-Alto.	- Restaurar copias.	- Medio.
	- Ataque Físico.	- Reducción de Disponibilidad.	-Alto.	- Contratar seguro.	- Muy bajo.

ACTIVOS	AMENAZAS	IMPACTO	Valoración Intrinseca (Impacto)	SALVAGUARDA	Valoración Efectiva (Impacto)
Aplicación de captura de datos.	- Suplantación de identidad.	- Reducción de Autenticidad.	-Muy alto.	-Elección adecuada de contraseñas.	- Bajo.
	- Introducción de datos incorrectos.	- Reducción de Integridad.	-Muy alto.	-Comprobación de Integridad en la base de datos.	- Muy bajo.
	- Descarga de datos en destino inapropiado.	- Reducción de disponibilidad.	-Alto.	-Comprobación de destino.	- Muy bajo.
Aplicación de Gestión de datos.	- Suplantación de identidad.	- Reducción de Confidencialidad. - Reducción de Autenticidad.	-Crítico.	-Elección adecuada de contraseñas.	- Alto.
	- Introducción de datos incorrectos.	- Reducción de Integridad.	-Crítico.	-Comprobación de Integridad en la base de datos.	- Muy bajo.
	- Borrado de datos.	- Reducción de Integridad. - Reducción de Disponibilidad.	-Crítico.	-Incorporar el uso de “Papelera de reciclaje.”	- Muy bajo.
Sistema de Base de datos.	- Acceso no permitido.	- Reducción de la Confidencialidad. - Reducción de Integridad.	-Crítico.	-Bloquear acceso a la base de datos.	- Alto.
	- Modificación de datos malintencionada.	- Reducción de Disponibilidad.	-Crítico.		- Alto.

ACTIVOS	AMENAZAS	IMPACTO	Valoración Intrinseca (Impacto)	SALVAGUARDA	Valoración Efectiva (Impacto)
Identidad del Usuario Interno.	- Suplantación de identidad.	- Reducción de Autenticación.	-Muy alto.	- Elección adecuada de contraseñas.	- Alto.
Datos capturados durante sesión.	- Suplantación de identidad.	- Reducción de Autenticidad.	-Muy alto.	- Elección adecuada de contraseñas.	- Alto.
Datos de apoyo durante sesión.	- Introducción de datos incorrectos.	- Reducción de Integridad.	-Muy alto.	-Comprobación de Integridad en la base de datos.	- Muy bajo.
Datos almacenados durante sesión.	- Suplantación de identidad.	- Reducción de Autenticidad. - Reducción de Confidencialidad. - Reducción de Integridad. - Reducción de Disponibilidad	-Crítico.	- Elección adecuada de contraseñas.	- Alto.
Documentos impresos para ser enviados.	-Robo. -Destrucción.	- Reducción de Confidencialidad. - Reducción de Disponibilidad.	-Alto -Medio	-Restaurar copias.	- Medio. -Muy bajo.
Documentos Recibidos	-Robo. - Destrucción.	- Reducción de Confidencialidad. - Reducción de Disponibilidad.	-Alto. -Medio.	-Restaurar copias.	-Muy bajo. -Muy bajo.

ACTIVOS	AMENAZAS	IMPACTO	Valoración Intrinseca (Impacto)	SALVAGUARDA	Valoración Efectiva (Impacto)
Administración de permisos.	- Suplantación de identidad.	- Reducción de Autenticidad. - Reducción de Confidencialidad.	-Crítico.	- Elección adecuada de contraseñas.	- Alto.
Transferencia de datos.	- Acceso no permitido a la comunicación. -Error en la comunicación.	- Reducción de Confidencialidad. - Reducción de Integridad.	-Muy alto. -Medio.	-Comprobación de origen. -Tratamiento de transacción.	-Muy bajo. -Muy bajo.
Relaciones entre Datos.	- Error en la definición del modelo de Datos. - Accedo no permitido a la base de Datos.	- Reducción de Integridad. - Reducción de Disponibilidad. - Reducción de Confidencialidad. - Reducción de Integridad. - Reducción de Disponibilidad.	-Crítico. -Crítico.	-Formación en desarrollo de software. -Bloquear acceso a la base de datos.	-Bajo. -Alto.

Fuente: MAGERIT: Análisis y Gestión de Riesgos.
Elaborado por: Autores.

ANEXO 10.

REEVALUACIÓN DEL RIESGO.

CAPA	ACTIVOS	AMENAZAS	SALVAGUARDAS	VULNERABILIDAD		IMPACTO INTRÍNSECO	IMPACTO EFECTIVO	RIESGO INTRÍNSECO	RIESGO EFECTIVO
				INTRÍNSECA	EFECTIVA				
Entorno	Servidor IBM	- Ataque físico. - Avería.	-Protección del Equipo dentro de la Organización. -Mantenimiento Permanente.	- Muy baja. - Muy baja	- Casi nula. -Se reduce en gran medida.	Crítico Crítico	Alto Alto	Máximo Máximo	Medio Medio
Entorno	Servidor Virtual	Avería del servidor.	- Protección del Equipo dentro de la Organización.	- Muy baja	-Se reduce en gran medida.	Crítico	Alto	Máximo	Medio
Entorno	PC’s	- Robo. - Ataque físico. - Avería.	- Acceso Limitado. - Acceso Limitado. - Mantenimiento Permanente.	- Muy baja. - Muy baja. - Media	-Se reduce en gran medida. - Casi nula. -Se reduce en gran medida.	Crítico Muy Alto Muy Alto	Alto Alto Alto	Máximo Alto Muy Alto	Medio Medio Medio
Entorno	Impresora Hp	- Ataque Físico. - Avería.	- Acceso Limitado. - Mantenimiento.	- Muy baja. - Media.	-Casi nula. -Se reduce en gran medida.	Alto Alto	Muy bajo Bajo	Medio Alto	_ Mínimo

CAPA	ACTIVOS	AMENAZAS	SALVAGUARDAS	VULNERABILIDAD		IMPACTO INTRÍNSECO	IMPACTO EFECTIVO	RIESGO INTRÍNSECO	RIESGO EFECTIVO
				INTRÍNSECA	EFECTIVA				
Entorno	Notebook's Hp	- Robo. - Ataque físico. - Avería.	- Protección del Equipo dentro de la Organización. - Protección del Equipo dentro de la Organización. - Mantenimiento permanente.	- Muy baja. - Muy baja. - Media	- Se reduce en gran medida. - Casi nula. - Se reduce en gran medida.	Crítico Muy Alto Muy Alto	Alto Alto Alto	Máximo Alto Muy Alto	Medio Medio Medio
Entorno	Scanner	- Ataque Físico. - Avería.	- Acceso Limitado. - Mantenimiento.	- Muy baja. - Media.	-Casi nula. -Se reduce en gran medida.	Alto Alto	Muy bajo Bajo	Medio Alto	- Mínimo
Entorno	Mobiliario.	-Robo. - Ataque Físico.	- Acceso Limitado. - Acceso Limitado.	-Muy baja. -Muy baja.	-Casi nula. -Casi nula.	Alto Alto	Medio Muy bajo	Medio Medio	Mínimo -
Sistema de Información	Aplicación de captura de datos.	- Suplantación de identidad. - Introducción de datos incorrectos. - Descarga de datos en destino inapropiado.	- Identificación por Usuario y Password. - Respaldo de datos. - Reconocimiento de destino.	-Media - Alta. -Media-Alta	-Se reduce en gran medida. - Se reduce al mínimo. -Se reduce al mínimo.	Muy Alto Muy Alto Alto	Bajo Muy bajo Muy bajo	Muy Alto Máximo Alto	Mínimo - -

CAPA	ACTIVOS	AMENAZAS	SALVAGUARDAS	VULNERABILIDAD		IMPACTO INTRÍNSECO	IMPACTO EFECTIVO	RIESGO INTRÍNSECO	RIESGO EFECTIVO
				INTRÍNSECA	EFECTIVA				
Sistema de Información	Aplicación de Gestión de datos.	- Suplantación de identidad. - Introducción de datos incorrectos. - Borrado de datos.	- Identificación por Usuario y Password. - Respaldo de Datos. - Almacenamiento permanente de datos.	-Media-baja - Media Alta. - Media.	-Se reduce en gran medida. -Se reduce al mínimo. -Se reduce al mínimo.	Crítico Crítico Crítico	Alto Muy bajo Muy bajo	Máximo Máximo Máximo	Medio - -
Sistema de Información	Sistema de Base de datos.	- Acceso no permitido. - Modificación de datos malintencionada	- Acceso a los datos únicamente a través del sistema a través de identificación de usuario y password.	- Muy alta. - Media–baja.	- Se reduce aunque no lo suficiente. -Se reduce en gran medida.	Crítico Crítico	Alto Alto	Máximo Máximo	Medio Medio
Información - Captura	Identidad del Usuario Interno.	- Suplantación de identidad.	- Identificación por Usuario y Password.	- Media.	-Se reduce en gran medida.	Muy Alto	Alto	Muy Alto	Medio
Información - Captura	Datos capturados durante sesión.	- Suplantación de identidad.	- Identificación por Usuario y Password.	- Media	- Se reduce en gran medida.	Muy Alto	Alto	Muy Alto	Medio
Información - Captura	Datos de apoyo durante sesión.	- Introducción de datos incorrectos.	- Identificación por Usuario y Password.	- Media	-Se reduce en gran medida.	Muy Alto	Muy bajo	Muy Alto	-
Información - Gestión	Datos almacenados durante sesión.	- Suplantación de identidad.	- Identificación por Usuario y Password.	- Media	-Se reduce en gran medida.	Crítico	Alto	Máximo	Medio

CAPA	ACTIVOS	AMENAZAS	SALVAGUARDAS	VULNERABILIDAD		IMPACTO INTRÍNSECO	IMPACTO EFECTIVO	RIESGO INTRÍNSECO	RIESGO EFECTIVO
				INTRÍNSECA	EFECTIVA				
Información - Gestión	Documentos impresos para ser enviados.	-Robo. - Destrucción.	- Limitación de acceso a las Instalaciones.	- Media-Alta	-Se reduce al mínimo.	Alto Medio	Medio Muy bajo	Alto Medio	Mínimo -
Información – Gestión	Documentos Recibidos	-Robo. - Destrucción.	- Limitación de acceso a las Instalaciones.	- Media-Alta	-Se reduce al mínimo.	Alto Medio	Muy bajo Muy bajo	Alto Medio	- -
Funciones de la Organización	Administración de permisos.	- Suplantación de identidad.	- Identificación por Usuario y Password.	- Media-Alta	Se reduce en gran medida.	Crítico	Alto	Máximo	Medio
Funciones de la Organización	Transferencia de datos.	- Acceso no permitido a la comunicación. -Error en la comunicación	-Transferencia entre dos o más dispositivos. -Señales de dispositivos listos.	- Alta - Media	- Se reduce totalmente. - Se reduce su efecto totalmente.	Muy Alto Medio	Muy bajo Muy bajo	Máximo Medio	- -
Funciones de la Organización	Relaciones entre Datos.	-Error en la definición del modelo de Datos. -Acceso no permitido a la base de Datos.	- Definición correcta del Modelo de Datos. -Limitación del acceso al sistema.	- Media- Alta - Muy alta.	-Se reduce todo lo posible. -Se reduce aunque no lo suficiente.	Crítico Crítico	Bajo Alto	Máximo Máximo	Mínimo Medio

Fuente: MAGERIT: Análisis y Gestión de Riesgos.
Elaborado por: Autores.

ANEXO 11

Modelo de valor

proyecto: [GS-RI-001] Análisis y Gestión de Riesgos en el Departamento de Servicio Técnico de Servindurama.

1. Datos del proyecto

GS-RI-001	Análisis y Gestión de Riesgos en el Departamento de Servicio Técnico de Servindurama.
descripción	Análisis a los Sistemas de Información.
responsable	Sr. Norman Andrés Alvear Vanegas. y Sr. Santiago Alejandro Plaza Auquilla.
fecha	14 de Febrero del 2011.
biblioteca	[std] Biblioteca INFOSEC (22.1.2009)

Licencia

[edu] Universidad de Cuenca
Cuenca - Ecuador
[... 1.1.2012]

2. Dimensiones

- [D] disponibilidad
- [I] integridad de los datos
- [C] confidencialidad de los datos
- [A] autenticidad de los usuarios y de la información
- [T] trazabilidad del servicio y de los datos

3. Dominios de seguridad

dominio de seguridad	[D]	[I]	[C]	[A]	[T]
[base] Departamento de Servicio Técnico.	A	A	A	A	M

4. Activos

4.1. Capa - [B] Capa de negocio

[SER-EXT-001.01.01] Overhaul del producto.
[SER-EXT-001.01.02] Asesoría Telefónica de instalación.
[SER-EXT-001.01.03] Préstamo del producto.
[SER-EXT-001.01.04] Venta de garantía extendida.
[SER-EXT-001.01.05] Llamadas sin costo.

4.2. Capa - [IS] Servicios internos

[SER-INT-001.02.01] Diagramas explosivos.
[SER-INT-001.02.02] Listas de partes.
[SER-INT-001.02.03] Estadísticas de daño.

4.3. Capa - [E] Equipamiento

[SW] Aplicaciones
- [SW-001.03.01.1] Módulo de Ventas.
- [SW-001.03.01.2] Módulo de Partes y Piezas.
- [SW-001.03.01.3] Módulo Customer Service Management System.
- [SW-001.03.01.4] Módulo de préstamo (producto).
- [SW-001.03.01.5] Módulo de diagramas explosivos.

[HW] Equipos
- [HW-001.03.02.1] Servidor IBM.
- [HW-001.03.02.2] Servidor Virtual.
- [HW-001.03.02.3] PC de escritorio.
- [HW-001.03.02.4] Notebook.
- [HW-001.03.02.5] Impresora.
- [HW-001.03.02.6] Scanner.

[COM] Comunicaciones
[COM-001.03.03.1] Módem.
[COM-001.03.03.2] Concentrador de red.
[COM-001.03.03.3] Conmutador.
[COM-001.03.03.4] Router.
[COM-001.03.03.5] Firewall propio de la Empresa.
[COM-001.03.03.6] Dispositivo Wireless.
[AUX] Elementos auxiliares
[AUX-001.03.04.1] Generador Eléctrico.
[AUX-001.03.04.2] Aire Acondicionado.
[AUX-001.03.04.3] UPS.
[AUX-001.03.04.4] Caja Fuerte.
[AUX-001.03.04.5] Mobiliario.

4.4. Capa - [SS] Servicios subcontratados

4.5. Capa - [L] Instalaciones

[INST-001.05.01] Departamento de Servicio Técnico.

4.6. Capa - [P] Personal

[PER-001.06.01] Ing. Sebastián Vega.
[PER-001.06.02] Ing. Mauricio Alvear.
[PER-001.06.03] Ing. Paúl Auquilla.
[PER-001.06.04] Ing. Gustavo Burbano.
[PER-001.06.05] Tec. Oswaldo Cevallos.
[PER-001.06.06] Srta. María José Carrión.
[PER-001.06.07] Sra. Fabiola Rubín.

5. Activos

5.1. [SER-EXT-001.01.01] Overhaul del producto.

- [S] Servicios
- [S.ext] a usuarios externos (bajo una relación contractual)
- [S.email] correo electrónico
- [S.file] almacenamiento de ficheros
- [S.edi] intercambio electrónico de datos
- [S.dir] servicio de directorio
- [S.idm] gestión de identidades
- [S.other] otros ...

Dominio de seguridad

- [base] Departamento de Servicio Técnico.

Datos

Servicio ofrecido a:	Usuarios Externos.

5.2. [SER-EXT-001.01.02] Asesoría Telefónica de instalación.

- [S] Servicios
- [S.ext] a usuarios externos (bajo una relación contractual)
- [S.edi] intercambio electrónico de datos
- [S.dir] servicio de directorio
- [S.idm] gestión de identidades
- [S.other] otros ...

Dominio de seguridad

- [base] Departamento de Servicio Técnico.

Datos

Servicio ofrecido a:	Usuarios Externos.

5.3. [SER-EXT-001.01.03] Préstamo del producto.

- [S] Servicios
- [S.ext] a usuarios externos (bajo una relación contractual)
- [S.email] correo electrónico
- [S.file] almacenamiento de ficheros
- [S.edi] intercambio electrónico de datos
- [S.idm] gestión de identidades
- [S.other] otros ...

Dominio de seguridad

- [base] Departamento de Servicio Técnico.

Datos

Servicio ofrecido a:	Usuarios Externos.

5.4. [SER-EXT-001.01.04] Venta de garantía extendida.

- [S] Servicios
- [S.ext] a usuarios externos (bajo una relación contractual)
- [S.file] almacenamiento de ficheros
- [S.edi] intercambio electrónico de datos
- [S.ipm] gestión de privilegios
- [S.other] otros ...

Dominio de seguridad

- [base] Departamento de Servicio Técnico.

Datos

Servicio ofrecido a:	usuarios Externos.

5.5. [SER-EXT-001.01.05] Llamadas sin costo.

- [S] Servicios
- [S.ext] a usuarios externos (bajo una relación contractual)
- [S.file] almacenamiento de ficheros
- [S.edi] intercambio electrónico de datos
- [S.idm] gestión de identidades
- [S.other] otros ...

Dominio de seguridad

- [base] Departamento de Servicio Técnico.

Datos

Servicio ofrecido a:	Usuarios Externos.

5.6. [SER-INT-001.02.01] Diagramas explosivos.

- [S] Servicios
- [S.int] interno (usuarios y medios de la propia organización)
- [S.www] world wide web
- [S.email] correo electrónico
- [S.file] almacenamiento de ficheros
- [S.edi] intercambio electrónico de datos
- [S.idm] gestión de identidades
- [S.other] otros ...

Dominio de seguridad

- [base] Departamento de Servicio Técnico.

Datos

Servicio ofrecido a:	Usuarios Internos.

5.7. [SER-INT-001.02.02] Listas de partes.

- [S] Servicios
- [S.int] interno (usuarios y medios de la propia organización)
- [S.www] world wide web
- [S.email] correo electrónico
- [S.file] almacenamiento de ficheros
- [S.edi] intercambio electrónico de datos
- [S.idm] gestión de identidades
- [S.other] otros ...

Dominio de seguridad

- [base] Departamento de Servicio Técnico.

Datos

Servicio ofrecido a:	Usuarios Internos.

5.8. [SER-INT-001.02.03] Estadísticas de daño.

- [S] Servicios
- [S.int] interno (usuarios y medios de la propia organización)
- [S.www] world wide web
- [S.email] correo electrónico
- [S.file] almacenamiento de ficheros
- [S.edi] intercambio electrónico de datos
- [S.idm] gestión de identidades

- [S.other] otros ...

Dominio de seguridad

- [base] Departamento de Servicio Técnico.

Datos

Servicio ofrecido a:	Usuarios Internos.

5.9. [SW.SW-001.03.01.1] Módulo de Ventas.

- [D] Datos / Información
- [D.vr] datos vitales
- [D.biz] datos de interés para el negocio
- [D.com] datos de interés comercial
- [D.int] datos de gestión interna
- [D.keys] claves criptográficas
- [D.multimedia] multimedia
- [D.source] código fuente
- [D.exe] código ejecutable
- [D.conf] datos de configuración
- [D.log] registro de actividad (log)
- [D.test] datos de prueba
- [D.per] datos de carácter personal
- [D.per.A] de nivel alto
- [D.classified] datos clasificados
- [D.classified.C] confidencial
- [D.other] otros ...
- [SW] Aplicaciones (software)
- [SW.sub] desarrollo a medida (subcontratado)
- [SW.std] estándar (off the shelf)

- [SW.std.dbms] sistema de gestión de bases de datos

Dominio de seguridad

- [base] Departamento de Servicio Técnico.

5.10. [SW.SW-001.03.01.2] Módulo de Partes y Piezas.

- [D] Datos / Información
- [D.vr] datos vitales
- [D.biz] datos de interés para el negocio
- [D.com] datos de interés comercial
- [D.int] datos de gestión interna
- [D.keys] claves criptográficas
- [D.multimedia] multimedia
- [D.source] código fuente
- [D.exe] código ejecutable
- [D.conf] datos de configuración
- [D.log] registro de actividad (log)
- [D.test] datos de prueba
- [D.per] datos de carácter personal
- [D.per.A] de nivel alto
- [D.classified] datos clasificados
- [D.classified.C] confidencial
- [D.other] otros ...
- [SW] Aplicaciones (software)
- [SW.sub] desarrollo a medida (subcontratado)
- [SW.std] estándar (off the shelf)
- [SW.std.dbms] sistema de gestión de bases de datos

Dominio de seguridad

- [base] Departamento de Servicio Técnico.

5.11. [SW.SW-001.03.01.3] Módulo Customer Service Management System.

- [D] Datos / Información
- [D.vr] datos vitales
- [D.biz] datos de interés para el negocio
- [D.com] datos de interés comercial
- [D.int] datos de gestión interna
- [D.keys] claves criptográficas
- [D.multimedia] multimedia
- [D.source] código fuente
- [D.exe] código ejecutable
- [D.conf] datos de configuración
- [D.log] registro de actividad (log)
- [D.test] datos de prueba
- [D.per] datos de carácter personal
- [D.per.A] de nivel alto
- [D.classified] datos clasificados
- [D.classified.C] confidencial
- [D.other] otros ...
- [SW] Aplicaciones (software)
- [SW.sub] desarrollo a medida (subcontratado)
- [SW.std] estándar (off the shelf)
- [SW.std.dbms] sistema de gestión de bases de datos

Dominio de seguridad

- [base] Departamento de Servicio Técnico.

5.12. [SW.SW-001.03.01.4] Módulo de préstamo (producto).

- [D] Datos / Información
- [D.vr] datos vitales
- [D.biz] datos de interés para el negocio
- [D.com] datos de interés comercial
- [D.int] datos de gestión interna
- [D.keys] claves criptográficas
- [D.multimedia] multimedia
- [D.source] código fuente
- [D.exe] código ejecutable
- [D.conf] datos de configuración
- [D.log] registro de actividad (log)
- [D.test] datos de prueba
- [D.per] datos de carácter personal
- [D.per.A] de nivel alto
- [D.classified] datos clasificados
- [D.classified.C] confidencial
- [D.other] otros ...
- [SW] Aplicaciones (software)
- [SW.sub] desarrollo a medida (subcontratado)
- [SW.std] estándar (off the shelf)
- [SW.std.dbms] sistema de gestión de bases de datos

Dominio de seguridad

- [base] Departamento de Servicio Técnico.

5.13. [SW.SW-001.03.01.5] Módulo de diagramas explosivos.

- [D] Datos / Información
- [D.vr] datos vitales
- [D.biz] datos de interés para el negocio

- [D.com] datos de interés comercial
- [D.int] datos de gestión interna
- [D.keys] claves criptográficas
- [D.multimedia] multimedia
- [D.source] código fuente
- [D.exe] código ejecutable
- [D.conf] datos de configuración
- [D.log] registro de actividad (log)
- [D.test] datos de prueba
- [D.per] datos de carácter personal
- [D.per.A] de nivel alto
- [D.classified] datos clasificados
- [D.classified.C] confidencial
- [D.other] otros ...
- [SW] Aplicaciones (software)
- [SW.sub] desarrollo a medida (subcontratado)
- [SW.std] estándar (off the shelf)
- [SW.std.dbms] sistema de gestión de bases de datos

Dominio de seguridad

- [base] Departamento de Servicio Técnico.

5.14. [HW.HW-001.03.02.1] Servidor IBM.

- [SW] Aplicaciones (software)
- [SW.std] estándar (off the shelf)
- [SW.std.browser] navegador web
- [SW.std.app] servidor de aplicaciones
- [SW.std.email_server] servidor de correo electrónico
- [SW.std.file] servidor de ficheros

- [SW.std.os] sistema operativo
- [SW.std.os.windows] windows
- [HW] Equipamiento informático (hardware)
- [HW.host] grandes equipos (host)

Dominio de seguridad

- [base] Departamento de Servicio Técnico.

5.15. [HW.HW-001.03.02.2] Servidor Virtual.

- [SW] Aplicaciones (software)
- [SW.std] estándar (off the shelf)
- [SW.std.browser] navegador web
- [SW.std.app] servidor de aplicaciones
- [SW.std.email_server] servidor de correo electrónico
- [SW.std.file] servidor de ficheros
- [SW.std.dbms] sistema de gestión de bases de datos
- [SW.std.os] sistema operativo
- [SW.std.os.windows] windows
- [HW] Equipamiento informático (hardware)
- [HW.vhost] equipos virtuales

Dominio de seguridad

- [base] Departamento de Servicio Técnico.

Datos

Asociado con:	Servidor IBM.

5.16. [HW.HW-001.03.02.3] PC de escritorio.

- [SW] Aplicaciones (software)

- [SW.std] estándar (off the shelf)
- [SW.std.browser] navegador web
- [SW.std.office] ofimática
- [SW.std.av] anti virus
- [SW.std.os] sistema operativo
- [SW.std.os.windows] windows
- [SW.std.other] otros ...
- [HW] Equipamiento informático (hardware)
- [HW.pc] informática personal

Dominio de seguridad

- [base] Departamento de Servicio Técnico.

Datos

Número de PC's en el Dep:	6
Capacidad:	80 GB.
Procesador:	Intel Pentium 4.
Memoria RAM:	256 MB.

5.17. [HW.HW-001.03.02.4] Notebook.

- [SW] Aplicaciones (software)
- [SW.std] estándar (off the shelf)
- [SW.std.browser] navegador web
- [SW.std.office] ofimática
- [SW.std.av] anti virus
- [SW.std.os] sistema operativo
- [SW.std.os.windows] windows

- [HW] Equipamiento informático (hardware)
- [HW.mobile] informática móvil

Dominio de seguridad

- [base] Departamento de Servicio Técnico.

Datos

Número de Notebook's:	5.
Marca:	Hewlett Packard (hp).
Capacidad:	250 GB.
Memoria RAM:	2.0 GB.

5.18. [HW.HW-001.03.02.5] Impresora.

- [SW] Aplicaciones (software)
- [SW.std] estándar (off the shelf)
- [SW.std.other] otros ...
- [HW] Equipamiento informático (hardware)
- [HW.peripheral] periféricos
- [HW.peripheral.print] medios de impresión

Dominio de seguridad

- [base] Departamento de Servicio Técnico.

Datos

Marca:	Hewlett Packard (hp).

5.19. [HW.HW-001.03.02.6] Scanner.

- [SW] Aplicaciones (software)
- [SW.std] estándar (off the shelf)

- [SW.std.other] otros ...
- [HW] Equipamiento informático (hardware)
- [HW.peripheral] periféricos
- [HW.peripheral.scan] escáner

Dominio de seguridad

- [base] Departamento de Servicio Técnico.

Datos

Marca:	Hewlett Packard (hp).

5.20. [COM.COM-001.03.03.1] Módem.

- [HW] Equipamiento informático (hardware)
- [HW.network] soporte de la red
- [HW.network.modem] módem
- [HW.network.wap] punto de acceso wireless
- [COM] Redes de comunicaciones
- [COM.X25] X25 (red de datos)
- [COM.pp] punto a punto
- [COM.radio] red inalámbrica
- [COM.wifi] WiFi
- [COM.LAN] red local
- [COM.Internet] Internet
- [COM.vpn] red privada virtual

Dominio de seguridad

- [base] Departamento de Servicio Técnico.

Datos

Marca:	Huawei.

5.21. [COM.COM-001.03.03.2] Concentrador de red.

- [HW] Equipamiento informático (hardware)
- [HW.network] soporte de la red
- [HW.network.hub] concentrador
- [COM] Redes de comunicaciones
- [COM.pp] punto a punto
- [COM.LAN] red local

Dominio de seguridad

- [base] Departamento de Servicio Técnico.

5.22. [COM.COM-001.03.03.3] Conmutador.

- [HW] Equipamiento informático (hardware)
- [HW.network] soporte de la red
- [HW.network.switch] conmutador
- [COM] Redes de comunicaciones
- [COM.X25] X25 (red de datos)
- [COM.pp] punto a punto
- [COM.LAN] red local
- [COM.Internet] Internet
- [COM.vpn] red privada virtual

Dominio de seguridad

- [base] Departamento de Servicio Técnico.

5.23. [COM.COM-001.03.03.4] Router.

- [HW] Equipamiento informático (hardware)
- [HW.network] soporte de la red
- [HW.network.router] encaminador
- [COM] Redes de comunicaciones
- [COM.ISDN] RDSI (red digital)
- [COM.pp] punto a punto
- [COM.radio] red inalámbrica
- [COM.LAN] red local
- [COM.Internet] Internet
- [COM.vpn] red privada virtual

Dominio de seguridad

- [base] Departamento de Servicio Técnico.

5.24. [COM.COM-001.03.03.5] Firewall propio de la Empresa.

- [HW] Equipamiento informático (hardware)
- [HW.network] soporte de la red
- [HW.network.firewall] cortafuegos
- [COM] Redes de comunicaciones
- [COM.X25] X25 (red de datos)
- [COM.pp] punto a punto
- [COM.radio] red inalámbrica
- [COM.wifi] WiFi
- [COM.LAN] red local
- [COM.VLAN] LAN virtual
- [COM.Internet] Internet
- [COM.vpn] red privada virtual

Dominio de seguridad

- [base] Departamento de Servicio Técnico.

5.25. [COM.COM-001.03.03.6] Dispositivo Wireless.

- [HW] Equipamiento informático (hardware)
- [HW.network] soporte de la red
- [HW.network.wap] punto de acceso wireless
- [COM] Redes de comunicaciones
- [COM.X25] X25 (red de datos)
- [COM.radio] red inalámbrica
- [COM.wifi] WiFi
- [COM.Internet] Internet
- [COM.vpn] red privada virtual

Dominio de seguridad

- [base] Departamento de Servicio Técnico.

5.26. [AUX.AUX-001.03.04.1] Generador Eléctrico.

- [AUX] Equipamiento auxiliar
- [AUX.gen] generadores eléctricos

Dominio de seguridad

- [base] Departamento de Servicio Técnico.

5.27. [AUX.AUX-001.03.04.2] Aire Acondicionado.

- [AUX] Equipamiento auxiliar
- [AUX.ac] equipos de climatización

Dominio de seguridad

- [base] Departamento de Servicio Técnico.

5.28. [AUX.AUX-001.03.04.3] UPS.

- [AUX] Equipamiento auxiliar
- [AUX.ups] sai - sistemas de alimentación ininterrumpida

Dominio de seguridad

- [base] Departamento de Servicio Técnico.

5.29. [AUX.AUX-001.03.04.4] Caja Fuerte.

- [AUX] Equipamiento auxiliar
- [AUX.safe] cajas fuertes

Dominio de seguridad

- [base] Departamento de Servicio Técnico.

5.30. [AUX.AUX-001.03.04.5] Mobiliario.

- [AUX] Equipamiento auxiliar
- [AUX.furniture] mobiliario

Dominio de seguridad

- [base] Departamento de Servicio Técnico.

5.31. [INST-001.05.01] Departamento de Servicio Técnico.

- [L] Instalaciones
- [L.local] local

Dominio de seguridad

- [base] Departamento de Servicio Técnico.

5.32. [PER-001.06.01] Ing. Sebastián Vega.

- [P] Personal
- [P.adm] administradores de sistemas

Dominio de seguridad

- [base] Departamento de Servicio Técnico.

5.33. [PER-001.06.02] Ing. Mauricio Alvear.

- [P] Personal
- [P.adm] administradores de sistemas

Dominio de seguridad

- [base] Departamento de Servicio Técnico.

5.34. [PER-001.06.03] Ing. Paúl Auquilla.

- [P] Personal
- [P.dba] administradores de BBDD

Dominio de seguridad

- [base] Departamento de Servicio Técnico.

5.35. [PER-001.06.04] Ing. Gustavo Burbano.

- [P] Personal
- [P.ui] usuarios internos

Dominio de seguridad

- [base] Departamento de Servicio Técnico.

5.36. [PER-001.06.05] Tec. Oswaldo Cevallos.

- [P] Personal
- [P.sub] subcontratas

Dominio de seguridad

- [base] Departamento de Servicio Técnico.

5.37. [PER-001.06.06] Srta. María José Carrión.

- [P] Personal
- [P.op] operadores

Dominio de seguridad

- [base] Departamento de Servicio Técnico.

5.38. [PER-001.06.07] Sra. Fabiola Rubín.

- [P] Personal
- [P.ue] usuarios externos

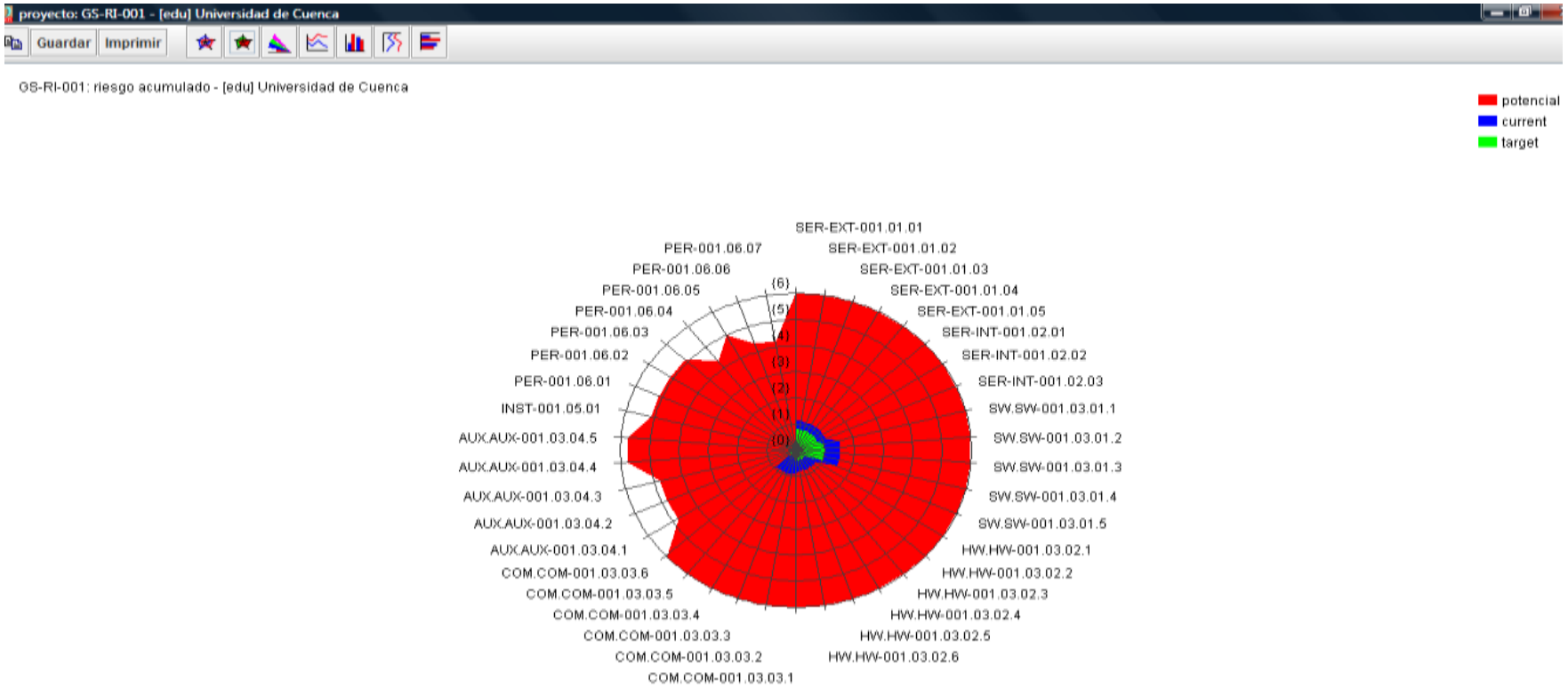
Dominio de seguridad

- [base] Departamento de Servicio Técnico.

Fuente: PILAR Basic 4.4.3
Elaborado por: Autores.

ANEXO 12

RIESGO ACUMULADO.



Fuente: PILAR Basic 4.4.3
Elaborado por: Autores.