UNIVERSIDAD POLITÉCNICA SALESIANA
SEDE GUAYAQUIL

CARRERA: INGENIERÍA DE SISTEMAS

Tesis previa a la obtención del título de: INGENIERO DE SISTEMAS

TEMA:

DIAGNÓSTICO DE LAS VULNERABILIDADES INFORMÁTICAS EN LOS SISTEMAS DE INFORMACIÓN PARA PROPONER SOLUCIONES DE SEGURIDAD A LA RECTIFICADORA GABRIEL MOSQUERA S.A.

AUTOR/A (S):

KAREN ANDREA PINTADO CUJI

CESAR LUIS HURTADO VALERO

DIRECTOR/A:

MSIG. NELSON MORA SALTOS

Guayaquil, abril del 2015

DECLARATORIA DE RESPONSABILIDAD

Nosotros Karen Pintado Cuji y Cesar Hurtado Valero autorizamos a la Universidad Politécnica Salesiana la publicación total o parcial de este trabajo de grado y su reproducción sin fines de lucro.

Además declaramos que los conceptos y análisis desarrollados y las conclusiones del presente trabajo son de exclusiva responsabilidad de los autores.

Guayaquil, 01 de abril del 2015

_____ _____

Karen Andrea Pintado Cuji
C.I. 0921971073

Cesar Luis Hurtado Valero
C.I. 0926031626

DEDICATORIA

Dedico esta tesis a mi familia, profesores y amigos.

Karen Pintado Cuji

DEDICATORIA

Dedico esta tesis a mi familia pero en especial a mi abuelita Emilia Delgado, mis padres Patricia Valero y Marcos Hurtado.

Cesar Hurtado Valero

AGRADECIMIENTO

A Dios Todopoderoso, San Juan Bosco patrono de los salesianos, mi familia y profesores que acompañaron mi formación personal y académica

A la Sra. Amada Mosquera que me permitió realizar el estudio en la empresa RECTIGAMOS S.A.

Al Ingeniero Nelson Mora mi tutor de tesis que estuvo pendiente ayudándome con las mejores recomendaciones para el desarrollo de la tesis.

A la Universidad Politécnica Salesiana mi más profundo agradecimiento por haberme dado la oportunidad de autofinanciarme la carrera y permitirme gozar de oportunidades únicas como estudiante.

Karen Pintado Cuji

AGRADECIMIENTO

Agradezco primero a Dios por darme las fuerzas necesarias para nunca desmayar y perseverar por alcanzar esta meta.

A mis padres y abuelita por estar presentes en todos los momentos importantes de mi vida.

A los docentes que supieron impartir sus conocimientos con dedicación y paciencia gracias totales: Danny Barona, Ricardo Naranjo, Teddy Negrete, Darío Huilcapi, Joe Llerena, Juan Andrade, Raúl Tingo, Raúl Álvarez.

En especial a mi tutor Msig. Nelson Mora por estar presente y guiarme a lo largo de este camino con toda la paciencia y predisposición para despejar todas mis dudas.

Cesar Hurtado Valero

INDICE

CAPÍTULO I 3
DISEÑO DE LA INVESTIGACIÓN 3
1. Planteamiento del problema 3
1.1 Antecedentes 3
1.1.1. Procesos del negocio 5
1.1.2. Sistema de información de la empresa. 6
1.2. Enunciado del problema 24
1.3 Formulación del Problema 24
1.4. Objetivos 25
1.4.1 Objetivo general 25
1.4.2 Objetivos específicos 25
1.5. Justificación 25
CAPITULO II 27
MARCO DE REFERENCIA DE LA INVESTIGACIÓN 27
2.1. Marco teórico 27
2.1.1. Introducción a la Seguridad 27
2.1.2. Auditoria Informática 29
2.1.3. Sistema Informático 29
2.1.4. Bugs (error de software) 29
2.1.5. Vulnerabilidad Informática 30
2.1.6. Concepto de Amenaza 30
2.2. Marco Conceptual 30
2.3. Hipótesis. 31
2.4 Matriz causa y efecto 32
2.5. Variables e indicadores 33
2.5.1 Variables independientes 33
2.5.2 Variables dependientes 33
2.6. Población y muestra 33
2.6.1. Población 33
2.6.2 Muestra 34
CAPITULO III 35
MARCO METODOLÓGICO 35
3.1. Tipo de investigación 35

3.1.1. Investigación exploratoria 35
3.1.2. Investigación descriptiva 35
3.1.3. Investigación explicativa 35
3.1.4. Investigación de campo 35
3.1.5. Investigación no experimental 36
3.2. Métodos de investigación 36
3.2.1. Método inductivo – deductivo 36
3.2.2. Método observativo 36
3.2.3. Método Sistémico 36
3.3. Fuentes 37
3.3.1. Fuentes Primarias 37
3.3.2. Fuentes Secundarias 38
3.4. Técnicas de recolección de datos 38
CAPITULO IV 39
ANÁLISIS Y RESULTADOS DEL PROYECTO 39
4.1. Metodología para el análisis y evaluación de riesgos en las TI 39
4.2. Evaluación con NESSUS 40
4.3. Evaluación de riesgos con MSAT 42
4.3.1. Resultados obtenidos de la evaluación con MSAT 43
4.3.1.1. Infraestructura 44
4.3.1.2. Aplicaciones 50
4.3.1.3. Operaciones 56
4.3.1.4. PERSONAL 62
4.3.2. Análisis general de la evaluación realizada con MSAT 67
4.4. Método OCTAVE-S 69
4.4.1. Proceso de OCTAVE –S 69
4.4.2. Fases de OCTAVE –S 70
4.4.3. Resultados de OCTAVE –S 73
4.5. Análisis comparativo de los resultados obtenidos 114
CAPITULO V 116
CONCLUSIONES Y RECOMENDACIONES 116
5.1. Conclusiones 116
5.2. Recomendaciones 117

CAPITULO VI 119
PROPUESTA 119
6.1. Datos informativos 119
6.2. Antecedentes de la propuesta 120
6.3. Justificación de la propuesta 120
6.4. Objetivos de la propuesta 121
6.4.1. Objetivo General 121
6.4.2. Objetivo Específicos 121
6.5. Análisis de Factibilidad 122
6.6. Plan de seguridad 123
6.7. Plan de seguridad de MSAT 124
6.7.1. ÁREA: INFRAESTRUCTURA 124
6.7.1.1 Defensa del Perímetro 125
6.7.1.2. Autenticación 126
6.7.1.3. Gestión y control 129
6.7.2. ÁREA: APLICACIONES 130
6.7.2.1 Implementación y uso 131
6.7.2.2. Diseño de aplicaciones 132
6.7.2.3. Almacenamiento y comunicación de datos 133
6.7.3 ÁREA: OPERACIONES 133
6.7.3.1. Entorno 134
6.7.3.2 Directiva de seguridad 134
6.7.3.3 Gestiones de actualizaciones y revisión 135
6.7.3.4. Copias de seguridad y revisión 136
6.7.4. ÁREA: PERSONAL 136
6.7.4.1. Requisitos y evaluaciones 137
6.7.4.2. Directiva y procedimientos 137
6.7.4.3 Formación y conocimiento 138

INDICE DE TABLAS

Tabla 1: Historia, visión y misión de RECTIGAMOS S.A. 4
Tabla 2: Datos de Servidores de RECTIGAMOS S.A. 8
Tabla 3: Matriz Causa y efecto 32
Tabla 4: Departamentos de Rectigamos 33
Tabla 5: Simbología 34
Tabla 6: Evaluación de Riesgos MSAT 43
Tabla 7: Defensa del perímetro 44
Tabla 8: Resultados del Análisis de la defensa del perímetro 45
Tabla 9: Riesgos de autenticación 47
Tabla 10: Resultado de los riesgos de autenticación encontrados 47
Tabla 11: Riesgos de Gestión y control 48
Tabla 12: Resultados del análisis de los riesgos de gestión y control 49
Tabla 13: Sub-sección implementación y uso 51
Tabla 14: Resultados del análisis de implementación y uso de aplicaciones 51
Tabla 15: Diseño de aplicaciones 54
Tabla 16: Resultado del análisis del diseño de aplicaciones 54
Tabla 17: Almacenamiento y comunicación de datos 55
Tabla 18: Entorno de Operaciones 57
Tabla 19: Directivas de seguridad 58
Tabla 20: Resultado del análisis de la directiva de seguridad 58
Tabla 21: Gestión de actualizaciones y revisiones 59
Tabla 22: Resultados del análisis en la gestión de actualizaciones y revisiones 59
Tabla 23: Copias de Seguridad y recuperación 61
Tabla 24: Resultados del análisis en las copias de seguridad y recuperación 61
Tabla 25: Sección de Personal 63
Tabla 26: Resultados del análisis en la sección de personal 63
Tabla 27: Directivas y procedimientos 64
Tabla 28: Resultados del análisis de la directiva y procedimientos 64
Tabla 29: Formación y conocimiento 65
Tabla 30: Resultados del análisis de la formación y conocimiento 65
Tabla 31: Nivel de prioridad para resolución de problemas según MSAT 68
Tabla 32: Identificación de los Activos 79
Tabla 33: Miembros del equipo de Análisis 79

Tabla 34: Área de Infraestructura 124
Tabla 35: Área de Aplicaciones 130
Tabla 36: Área de Operaciones 133
Tabla 37: Área de Personal 136

INDICE DE GRÁFICOS

Figura 1: Diagrama de red 7
Figura 2: Ubicación del acceso directo al Sistema Contable VISUAL FAC..... 10
Figura 3: Ingreso al Sistema VISUAL FAC 10
Figura 4: Módulo de Facturación..... 11
Figura 5: Reporte de Ordenes 11
Figura 6: Módulo de Facturación ‐ Procesos de facturación..... 12
Figura 7: Módulo de Compras 12
Figura 9: Modulo de compras ‐ Listado de retenciones 13
Figura 8: Módulo Compras ‐ Listar Compras 13
Figura 10: Módulo de Compras ‐ Solicitudes de compra..... 14
Figura 11: Módulo de Cuentas por cobrar ‐ Listado de Cuentas por cobrar vigentes..... 14
Figura 12: Módulo de Cuentas por cobrar ‐ Reportes..... 15
Figura 13: Cancelación de cuentas por cobrar..... 15
Figura 14: Modulo de Contabilidad..... 16
Figura 15: Libro Diario..... 16
Figura 17: Libro Mayor 17
Figura 16: Reportes contables y Financieros 17
Figura 19: Ventas de Producto..... 18
Figura 18: Reporte de Ventas..... 18
Figura 20: Formularios SRI 19
Figura 21: Anexos Transaccional Simplificado y de REOC 19
Figura 22: Formularios SRI 20
Figura 23: Módulo de Nómina..... 20
Figura 24: Módulo de Auditoría 21
Figura 25: Módulo de Caja 21
Figura 26: Reporte de Ventas..... 22
Figura 27: Cierre de caja..... 22
Figura 28: Módulo de Inventario 23
Figura 29: Inventario ‐ Reportes 23
Figura 30: Kardex 24
Figura 31: Componentes de la herramienta NESSUS..... 40
Figura 32: Escaneo web desde Nessus..... 41
Figura 33: Análisis de riesgos MSAT..... 42

Figura 34: Procesos, actividades y pasos de la fase 1, Metodología Octave-S 71
Figura 35: Procesos, actividades y pasos de la fase 2, Metodología Octave-S 72
Figura 36: Procesos, actividades y pasos de la fase 3, Metodología Octave-S 73
Figura 37: Actividades y pasos del proceso S1, Metodología Octave-S 80
Figura 38: Actividades y pasos del proceso S2, Metodología Octave-S 92
Figura 39: Actividades y pasos del proceso S3, Metodología Octave-S 111

RESUMEN

En el presente proyecto de tesis se realiza el diagnóstico de las vulnerabilidades informáticas en los Sistemas de Información para proponer soluciones de Seguridad a la empresa RECTIGAMOS S.A. Las soluciones serán descritas en la propuesta técnica que se elabora como resultado a los informes y estudios realizados, este documento básicamente recoge claramente las políticas de seguridad y las responsabilidades de cada uno de los participantes en el proceso informático, así como las medidas y procedimientos que permitan prevenir, detectar y responder a las amenazas presentes en la empresa.

Frente a la necesidad de proteger los sistemas que manejan información delicada y sensible de la empresa RECTIGAMOS S.A., los autores del presente proyecto proponen llevar a cabo una evaluación de los riesgos y desarrollar un plan de mitigación de los mismos, utilizando las metodologías MSAT y OCTAVE -S. Se escogieron estas herramientas debido a que están basadas en las mejores prácticas de seguridad comúnmente aceptadas, es decir, estándares como las normas ISO 27001, 17799 y NIST-800.x. Estas metodologías son diseñadas especialmente para instituciones con menos de 100 empleados y cuya red de datos cuenta con recursos limitados.

ABSTRACT

In this thesis project it is realized the diagnosis of the computer vulnerabilities in the Security Information Systems to propose solutions to the company RECTIGAMOS S.A. The solutions will be described in the technical proposal made as a result of the reports and studies, this paper basically clearly stated security policies and responsibilities of each participants in the information process and the measures and procedures to prevent, detect and respond to threats within the enterprise.

Due to the need to protect the systems that handle delicate and sensitive company information RECTIGAMOS S.A., the authors of this project proposed to carry out a risk assessment and develop a plan to mitigate them, using the MSAT methodologies and OCTAVE -S. These tools were chosen because they are based on best security practices commonly accepted, standards such as ISO 27001, 17799 and NIST-800.x standards. These methodologies are designed especially for institutions with fewer than 100 employees and whose data network with limited resources.

INTRODUCCIÓN

La mayoría de las empresas reconocen la función primordial que la tecnología de la información desempeña en sus modelos de negocio; la administración de la seguridad de sus infraestructuras, y el valor que ofrecen, se ha convertido en una preocupación fundamental para los departamentos de TI, y es por esto que se ha implementado el análisis de la gestión de riesgos, que realizada de una manera eficiente puede garantizar efectos económicos muy importantes para cualquier organización, convirtiéndose en una herramienta para la toma de decisiones.

Para esto se ha diseñado algunas metodologías que conducen de una forma útil al estudio, ofreciendo a las organizaciones una guía de procedimientos para la implementación y desarrollo y la minimización de los riesgos.

Existe una gran variedad de metodologías, muchas de ellas con reconocimiento internacional, pero todas son distintas. La presente investigación se orientó en la búsqueda de un modelo metodológico para realizar el proceso de análisis de riesgos en los Sistemas de Información, que son manejados por la empresa RECTIGAMOS S.A., con el fin de asegurar el activo fundamental de sus sistemas como lo es la información, permitiendo identificar las amenazas y vulnerabilidades a las que se encuentra expuesto, valorando el impacto que generaría en la institución dicha materialización y estableciendo los controles necesarios para mitigar el riesgo.

De igual manera, se tiene como guía la metodologías para el análisis de riesgos a OCTAVE.

En este sentido, el trabajo de investigación se estructura en seis (VI) capítulos de la siguiente manera:

Capítulo I: El planteamiento del problema de investigación, en el cual se define de forma clara y precisa tanto la formulación del problema como los objetivos de la investigación, justificación, importancia y alcance.

Capítulo II: Denominado marco teórico, contentivo de los antecedentes investigativos, bases teóricas, formulación de hipótesis y señalamiento de variables en relación con el objeto de estudio.

Capítulo III: Llamado marco metodológico, donde se describe la metodología usada, el tipo de investigación, población y muestra, operacionalización de variables e indicadores y los instrumentos de recolección de datos, validez y confiabilidad del plan de procesamiento de la información.

Capítulo IV: Corresponde al análisis de la interpretación de datos mediante la verificación de las hipótesis obteniendo los correspondientes resultados del estudio.

Capítulo V: En este capítulo se expresan las conclusiones a las que se llegó conforme a los objetivos planteados, así como también, aquellas recomendaciones pertinentes de la investigación.

Capítulo VI: Plantea la propuesta acerca del análisis de factibilidad, fundamentación, modelo operativo y su respectiva administración.

Finalmente, se presenta las referencias bibliográficas y los anexos.

CAPÍTULO I

DISEÑO DE LA INVESTIGACIÓN

1. Planteamiento del problema

En la actualidad la seguridad de la información es un punto clave de análisis, puesto que las condiciones van cambiando a lo largo del tiempo en función de las nuevas tecnologías, lo que ha permitido fijar nuevos horizontes dando como resultado, la aparición de nuevas amenazas tecnológicas que pudieran poner en riesgo los activos de información.

Gestionar los riesgos eficientemente constituye hoy en día una preocupación de la alta gerencia, según afirma Bernens (1997): "la grieta pequeña más grande en la armadura corporativa es la dirección de riesgos". La gestión de riesgos se facilita cuando las entidades desarrollan sus actividades sobre la base de sistemas de control para la seguridad acorde con las exigencias actuales.

De lo antes expuesto, surge la necesidad de realizar un diagnóstico de las vulnerabilidades informáticas en los Sistemas de Información para proponer soluciones de seguridad a la empresa Rectificadora Gabriel Mosquera S.A.

Por lo que es preciso, que los responsables de la seguridad de la información en conjunto con la directiva de la empresa, tomen conciencia y deban contrarrestar los riesgos a los que están sometidos sus activos principales.

1.1 Antecedentes

La empresa Rectificadora Gabriel Mosquera S.A. presta servicios de rectificación, a la medida del cliente, caracterizándose por una alta calidad y diferenciación en la prestación.

Sustenta su prestigio e imagen institucional en la alta calidad y confiabilidad de sus repuestos y servicios, manteniendo una permanente actualización en su área.

Tabla 1: Historia, visión y misión de RECTIFICADORA GABRIEL MOSQUERA S.A.

Historia
El gestor para que se constituya esta empresa es el Ing. Gabriel Mosquera Prieto, quien en los años 50 inició sus conocimientos con el Maestro el Sr. Víctor Mosquera Alvarado, en Huancavilca y Chimborazo de la ciudad de Guayaquil. Comenzó su actividad comercial el 15 de noviembre de 1971, dedicándose a la prestación de servicios en cuanto tiene relación al mantenimiento y reparación de todo tipo motores de vehículos. En el año de 1984, entra en una etapa de auge en relación a importaciones; ya que se vió en la necesidad de no solamente brindar servicios sino vender el producto, como son los repuestos automotrices, para finalizar la obra eficazmente. En el año de 1988 y 1998 se formaron dos nuevas instituciones bajo los nombres comerciales de RECTIGAMOS RECTIFICADORA ING. GABRIEL MOSQUERA S.A. e IMPORGAMOS S.A., ubicadas en la Av. De las Américas y Cosme Renella. Loa principales proveedores, entre los principales se encuentran: FADECYA, cuyo producto son las camisas de cilindros provenientes de Argentina; AUTOPARTS de Inglaterra, que provee chapas de bancada y de bielas. De Japón como son los rines marcas NPR y las Junta normalmente llamadas empaques originarios de España cuyo representante es AJUSA; y así una innumerable gama de productos que complementan para abastecer los servicios y productos que requieren nuestros clientes y también nuestro stock.

Misión	
	Prestar servicios de Rectificación, a la medida del cliente, caracterizados por una alta calidad y diferenciación en la prestación. Sustentar el prestigio e imagen institucional en la alta calidad y confiabilidad de los Repuestos y Servicios, manteniendo una permanente actualización en el área.
Visión	
	Continuar con los objetivos en la rectificación de partes y piezas de máquinas a nivel nacional y en la comercialización de repuestos de calidad.

Elaborado por: Amada Mosquera- Gerente General RECTIGAMOS S.A.

Para efectos del desarrollo del presente documento se utilizará el término RECTIGAMOS S. A. para denominar a la empresa Rectificadora Gabriel Mosquera S.A.

Los servicios que ofrece RECTIGAMOS S.A. son:

- ✓ Rectificar Cigueñal
- ✓ Rectificar y Encamisar Cilindros, Brazos de Biela, Asientos de Válvula
- ✓ Instalar Pistones en Bielas
- ✓ Instalar Guías de Válvula
- ✓ Instalar Bujes Barras de Leva
- ✓ Cepillar, Mandrilar, Espichar
- ✓ Prueba Hidrostática
- ✓ Pista del Retenedor del Cigueñal
- ✓ Comprobar Cabezote

1.1.1. Procesos del negocio

El objetivo de conocer los procesos de negocio delicados, y su información sensible ayudará a seleccionar las herramientas adecuadas para realizar el análisis de riesgos.

En la empresa actualmente trabajan aproximadamente 40 empleados, divididos en 2 áreas: Gerencia Financiera con sus sub-áreas: Contabilidad, Tesorería y caja, Gerencia Operaciones y Administración con sus sub-áreas: Operaciones, Administración y Sistemas.

Las aplicaciones más importantes que utiliza en sus procesos de negocio son, el sistema contable, la intranet, correo electrónico, y la página web. La empresa a través de su página web provee toda la información necesaria para acceder a sus servicios. La intranet se la usa para acceder a información y aplicaciones que la empresa utiliza.

Los activos más importantes que forman parte de la infraestructura de red interna de RECTIGAMOS S.A. son el sistema contable, servidor de Base de Datos y Servidor de Correo. El sistema contable automatiza los procesos del negocio y permite la obtención de información necesaria para la gestión empresarial y la toma de decisiones. Para la administración del Servidor de correo electrónico se utilizan los programas Mailscanner y Sendmail, y como cliente de correo electrónico se usa Outlook el cual está instalado en todas las estaciones de trabajo de RECTIGAMOS S.A.

El Servidor de Base de Datos almacena la información que se procesa en el sistema contable, que se considera sensible ya que es información delicada como la contabilidad de la empresa. También se consideran sensibles correos electrónicos que tienen información importante como confirmaciones de contratos o datos de proveedores.

1.1.2. Sistema de información de la empresa.

En este apartado se describen las herramientas y aplicaciones más importantes que usa la empresa en sus procesos de negocio, para poder brindar los servicios a sus clientes. Además se presenta el diagrama y la descripción de la red de la empresa

Topología de Red

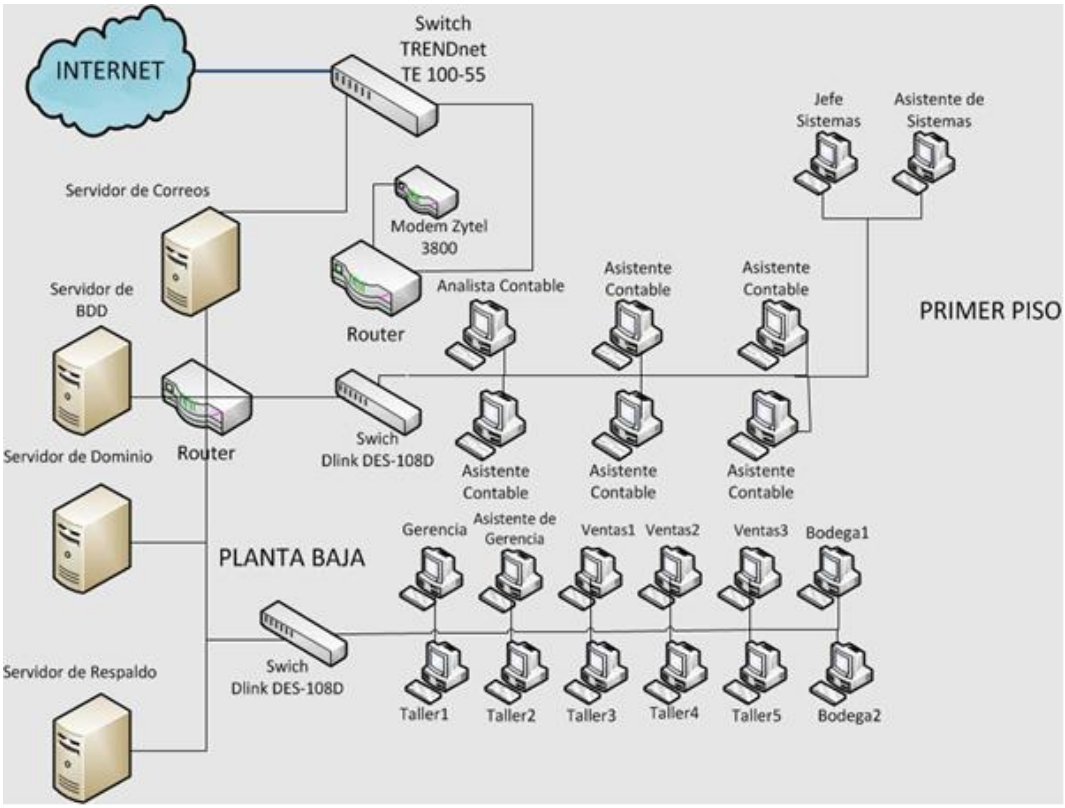


Figura 1: Diagrama de red
Fuente: Los Autores

La topología actual de red de RECTIGAMOS S.A. es de Tipo Estrella y Bus. Como se puede ver en la figura 1, la parte que comprende la topología tipo bus está compuesta por los switches Dlink DES-108D y todas las estaciones de trabajo. Los equipos que se encuentran en la planta baja están conectados a uno de los switches y los equipos que están ubicados en el primer piso se conectan al otro switch.

En cuanto a la parte que comprende la topología de tipo estrella está compuesta por el Router como nodo central y los equipos que confluyen a este son: el servidor de correo, servidor de base de datos, servidor de respaldo, servidor de dominio y los switches Dlink DES-108D. En el Servidor de Correo se encuentra instalado y activado el firewall, por tal motivo es éste el único equipo que está conectado al Switch TRENDnet TE100-55, medio por el cual pasan todos los paquetes de internet y adicionalmente es el único punto de salida a internet con IP fija.

El proveedor de servicio de internet proporciona un dispositivo Modem Zytel 3800 series, el cual está conectado al Router Cisco 1700 series, y este a su vez está conectado al Switch TRENDnet TE100-55.

El cableado de la red en la empresa es estructurado y es del tipo UTP categoría 5e. En cuanto al software, las estaciones de trabajo tienen instalado Windows XP y Windows 7. La información de cada uno de los servidores se encuentra en la tabla 1 que se muestra a continuación.

Tabla 2: Datos de Servidores de RECTIGAMOS S.A.

Servidor	Procesador	Velocidad (GHZ)	RAM	SO	Disco
BDD	Intel Xeon	3,6	4 GB	Windows 2003 R2	1 TB
Correo	Procesador Intel® E3110	3	4 GB	Centos	500 GB
Respaldo	Procesador Intel® E3110	3	4 GB	Windows 2003 R2	500 GB
Dominio	Intel Xeon	3,6	4 GB	Windows 2003 R2	100 GB

Elaborado por: Los Autores

Herramientas y aplicaciones utilizadas en RECTIGAMOS S.A.

En este apartado se presenta una breve descripción de las herramientas y aplicaciones que utiliza la empresa en sus procesos de negocio.

Intranet: La intranet es el medio por el cual personal autorizado de la empresa accede a las aplicaciones y documentos alojadas en los diferentes servidores.

El Gerente General es el encargado de crear los usuarios y proporcionar los permisos adecuados para cada miembro del personal. La intranet además ayuda a compartir recursos, utilizar los servicios de correo electrónico y almacenamientos de datos, y compartir de forma segura información privada como las fichas de candidatos, información contable de la empresa, datos de los accionistas etc.

Sistema de Información: Es un software multiusuario llamado VISUAL FAC que consta de 10 módulos, que automatizan los procesos de negocio de RECTIGAMOS S.A. y permite la obtención de información necesaria para la gestión y toma de decisiones.

Los módulos con los que cuenta el sistema son los siguientes:

- Ventas
- Compras
- Cuentas por Cobrar
- Contabilidad
- Reportes
- Anexos
- Nómina
- Auditoria
- Inventario

A continuación se hace una descripción de cada módulo del Sistema de información:

Ingreso

En esta ventana se visualiza el acceso al sistema contable VISUAL FAC de la empresa.

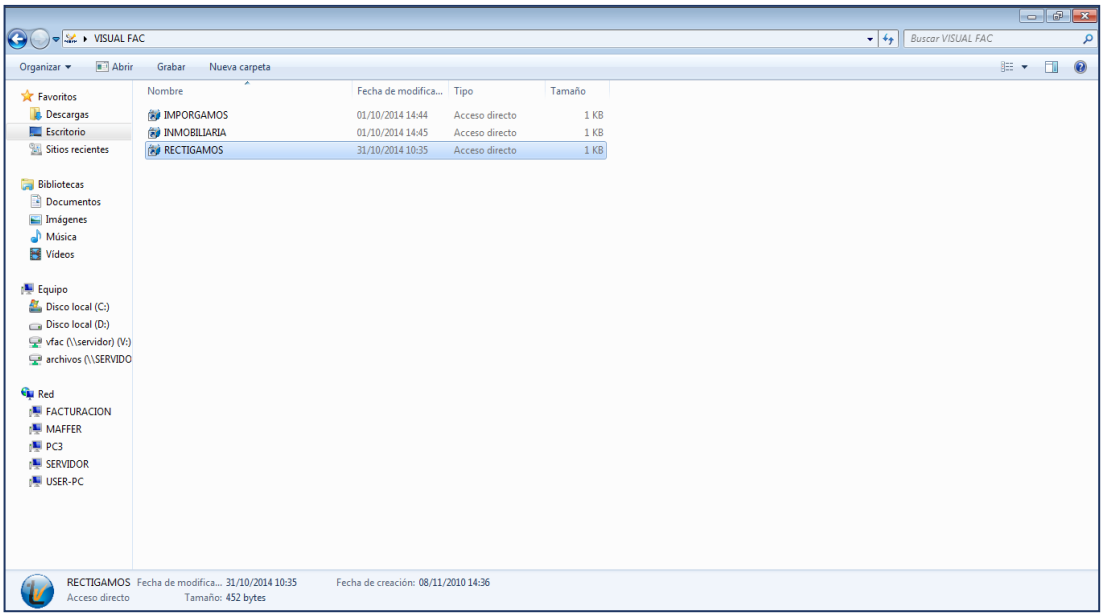


Figura 2: Ubicación del acceso directo al Sistema Contable VISUAL FAC
Fuente: Los Autores

Para poder ingresar al sistema, se debe tener un usuario y una contraseña.

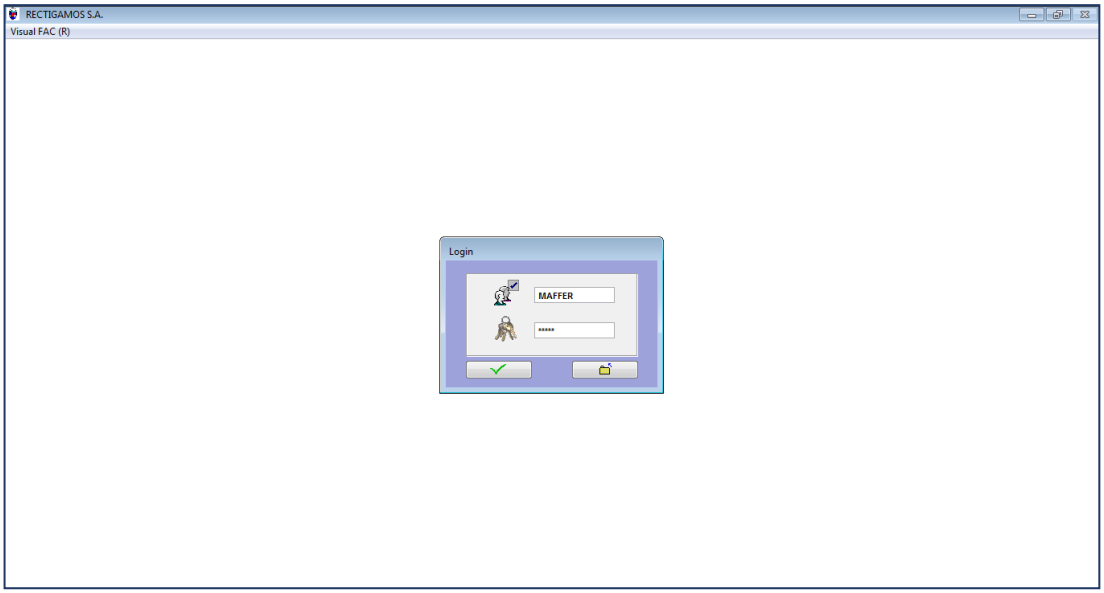


Figura 3: Ingreso al Sistema VISUAL FAC
Fuente: Los Autores

Facturación

En el módulo de facturación se realiza la emisión de facturas por el servicio prestado a los clientes.

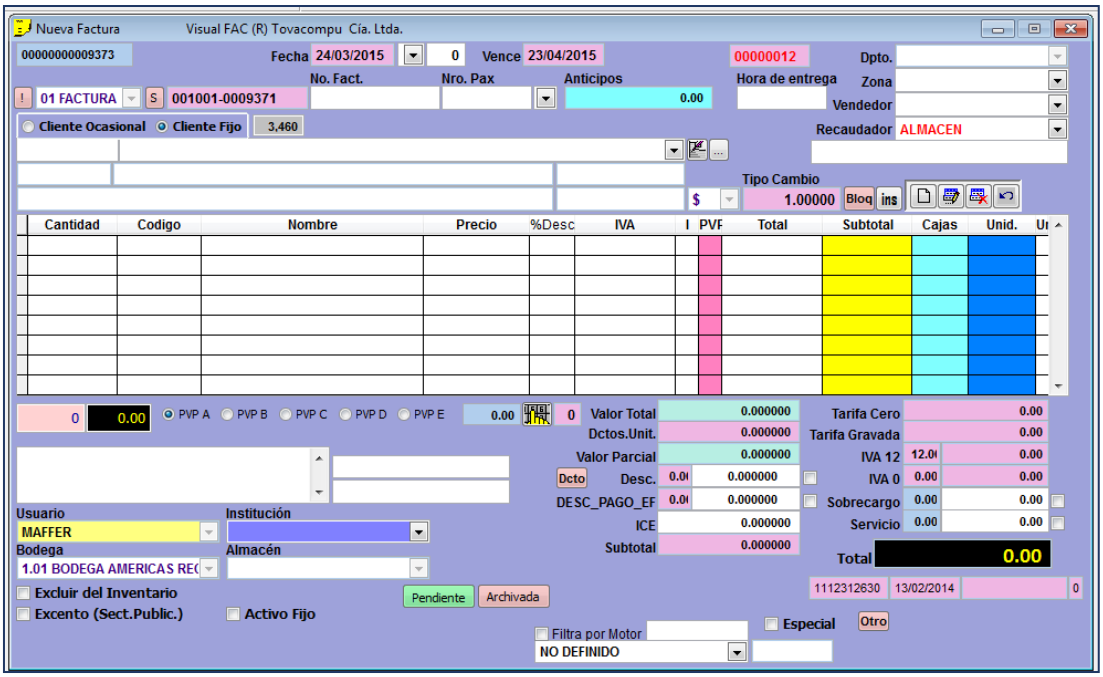


Figura 4: Módulo de Facturación
Fuente: Los Autores

También permite generar un reporte de órdenes de las transacciones por fecha, permitiendo imprimirlo y generarlo en formato PDF, Excel, o enviarlo por e-mail.

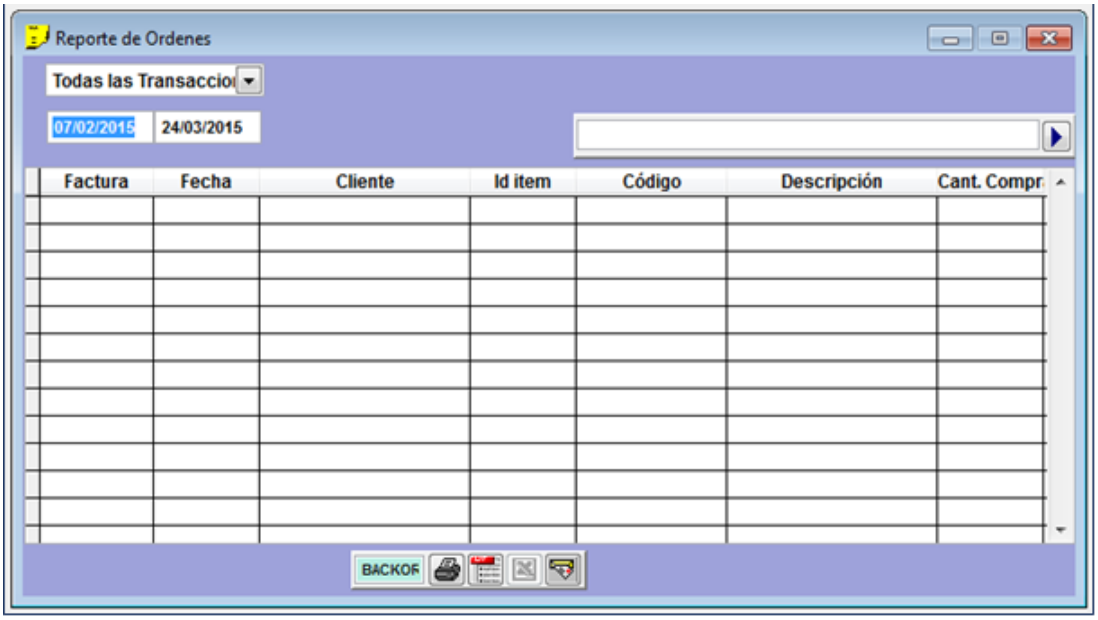


Figura 5: Reporte de Ordenes
Fuente: Los Autores

En los procesos de facturación se realizan los descuentos especiales, descuentos por temporadas y promociones a los clientes.

Figura 6: Módulo de Facturación – Procesos de facturación
Fuente: Los autores

Compras

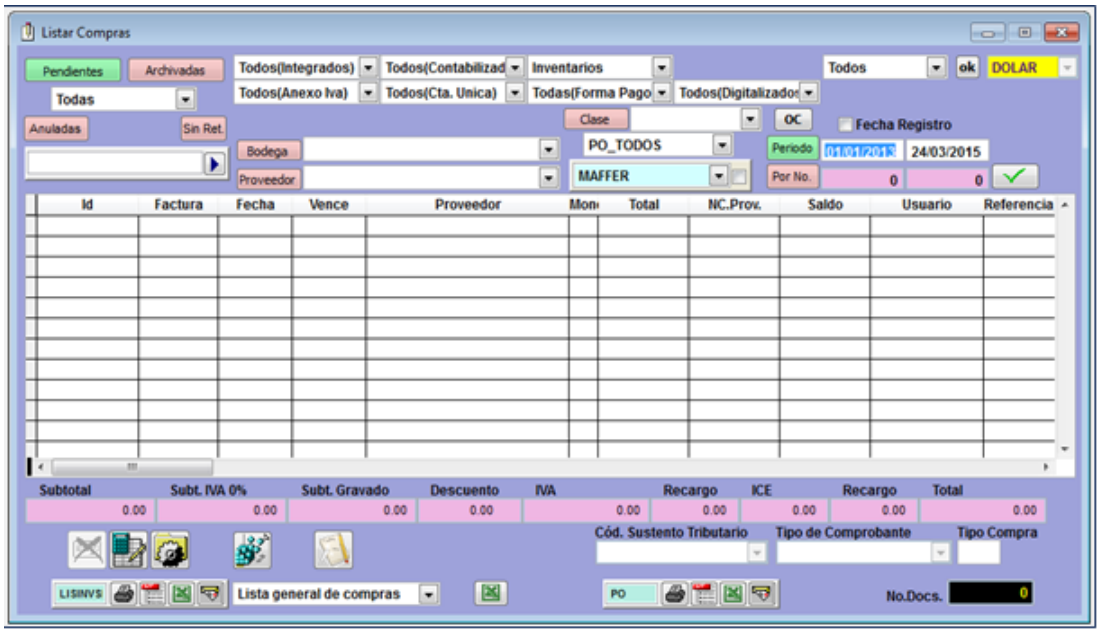


Figura 7: Módulo de Compras
Fuente: Los Autores

En este módulo se puede listar las compras, retenciones y las solicitudes realizadas durante el periodo contable.

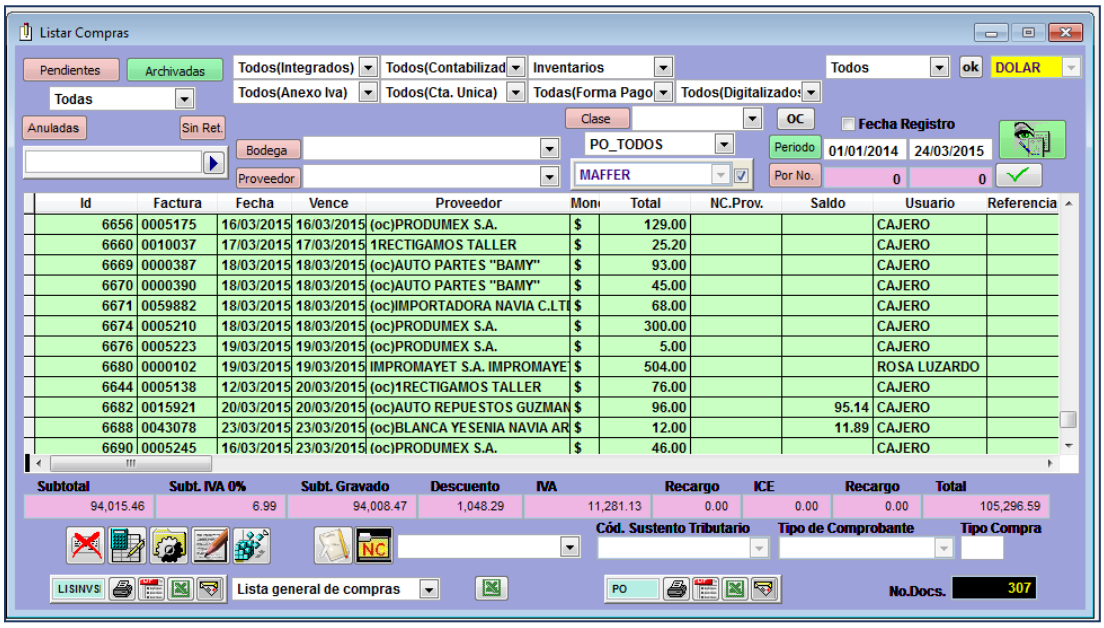


Figura 9: Módulo Compras – Listar Compras
Fuente: Los autores

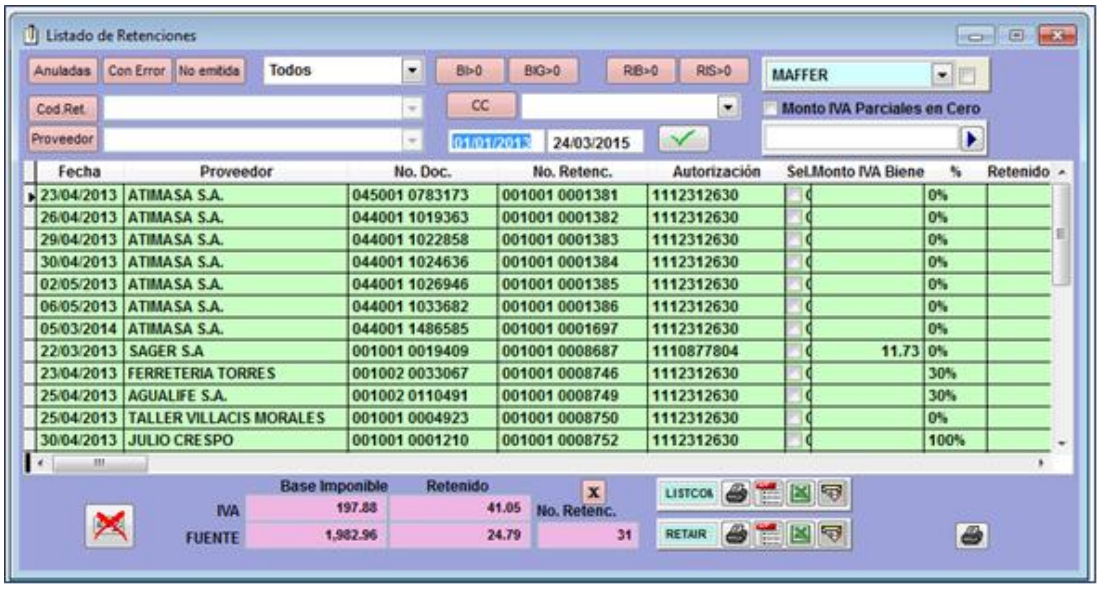


Figura 8: Modulo de compras – Listado de retenciones
Fuente: Los Autores

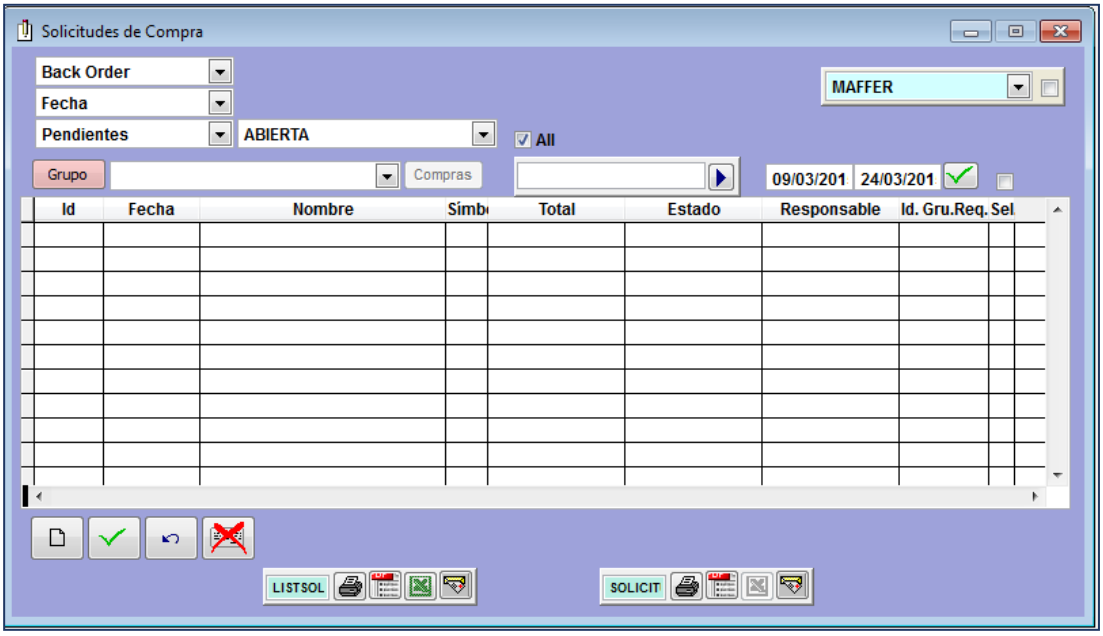


Figura 10: Módulo de Compras – Solicitudes de compra
Fuente: Los Autores

Cuentas por cobrar

En este módulo se listan las cuentas por cobrar vigentes

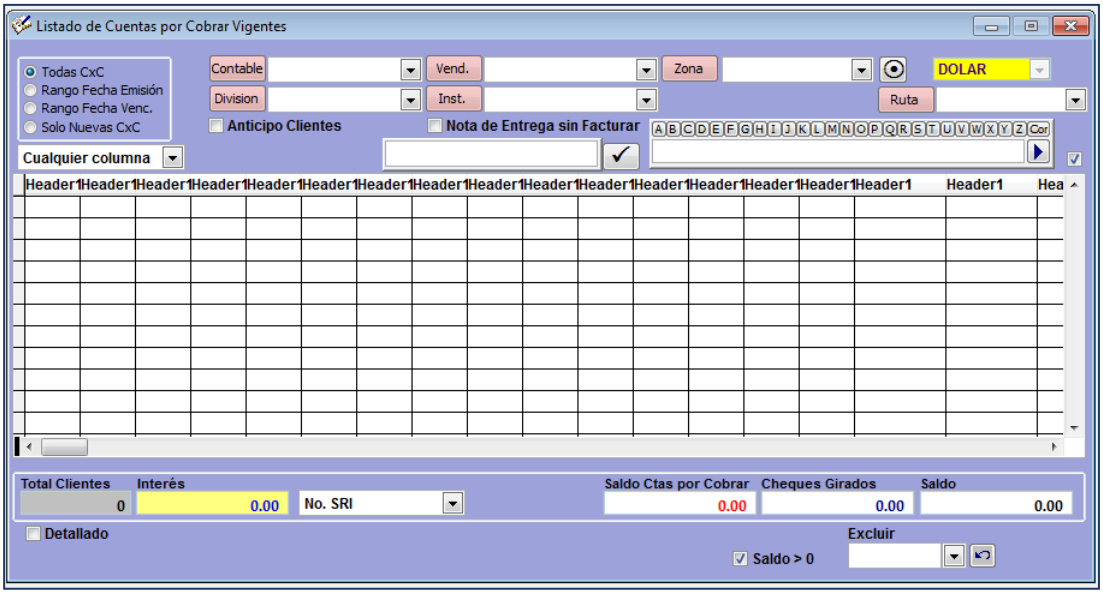


Figura 11: Módulo de Cuentas por cobrar – Listado de Cuentas por cobrar vigentes
Fuente: Los Autores

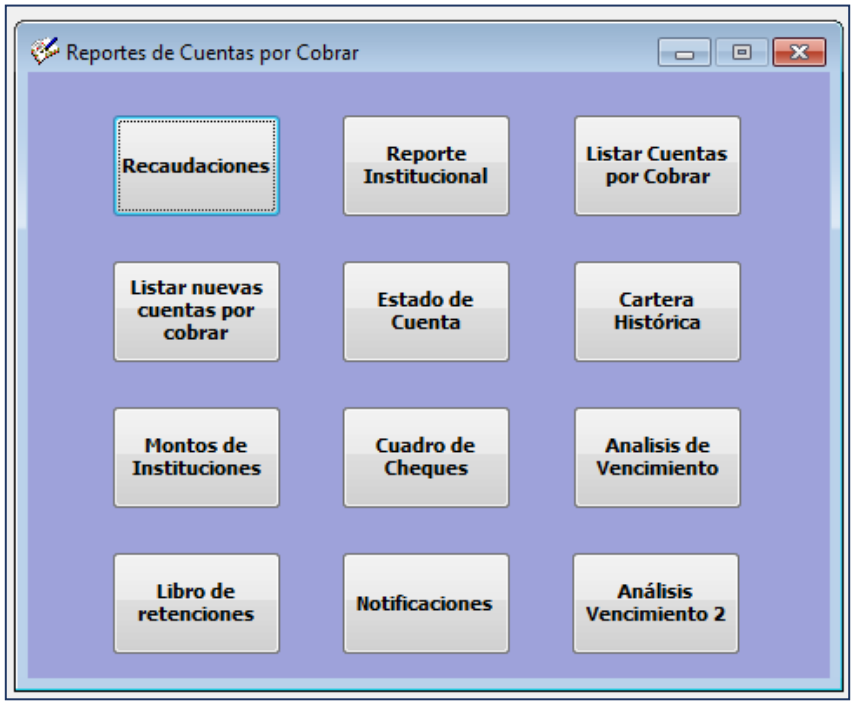


Figura 12: Módulo de Cuentas por cobrar – Reportes
Fuente: Los Autores

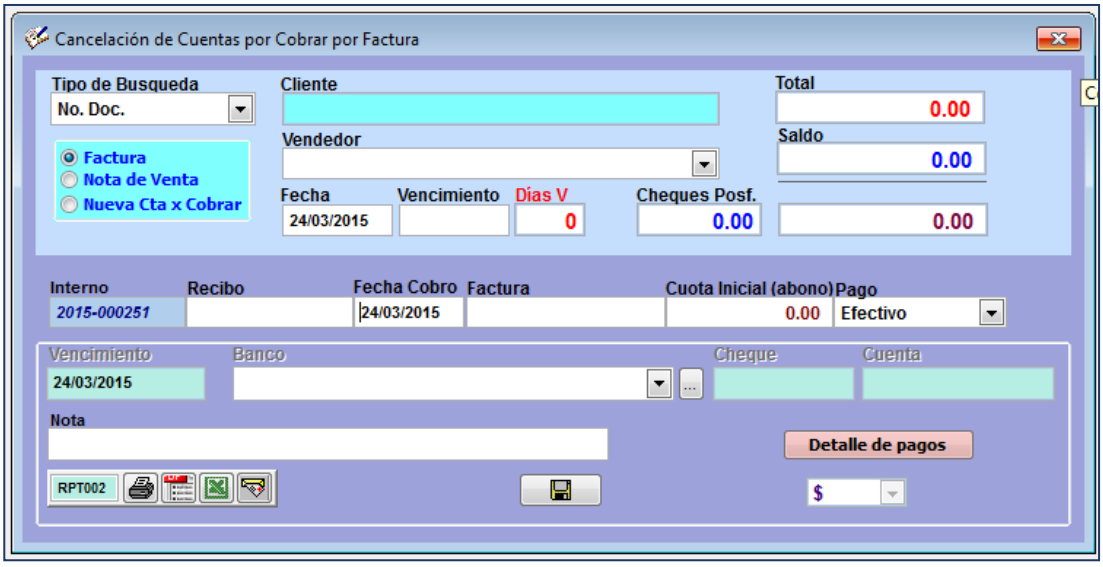


Figura 13: Cancelación de cuentas por cobrar
Fuente: Los Autores

Contabilidad

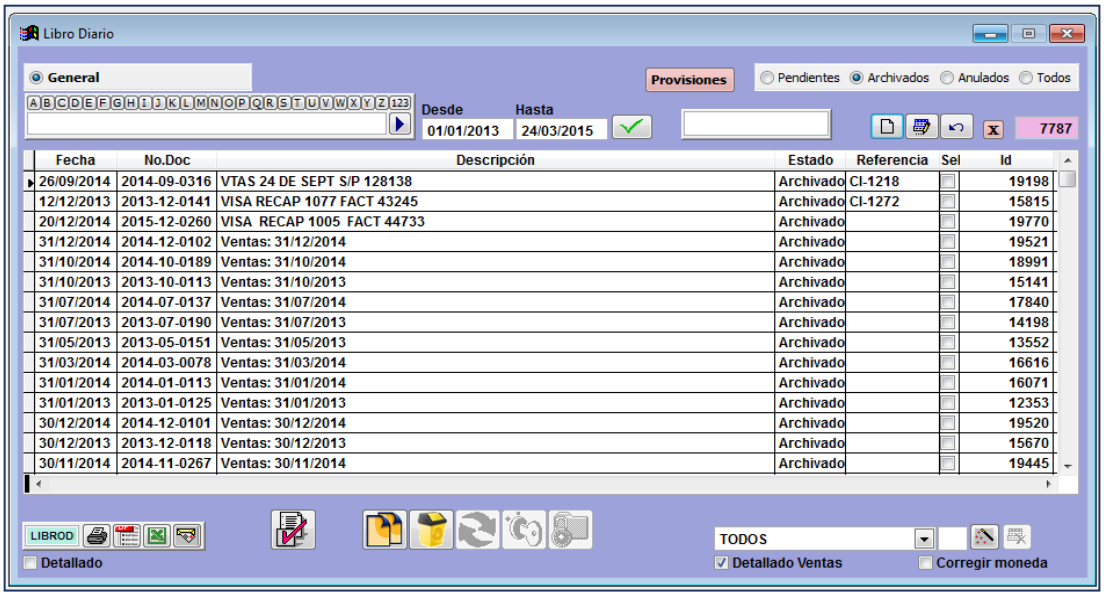


Figura 14: Modulo de Contabilidad
Fuente: Los Autores

En esta opción el sistema permite generar reportes contables y financieros.

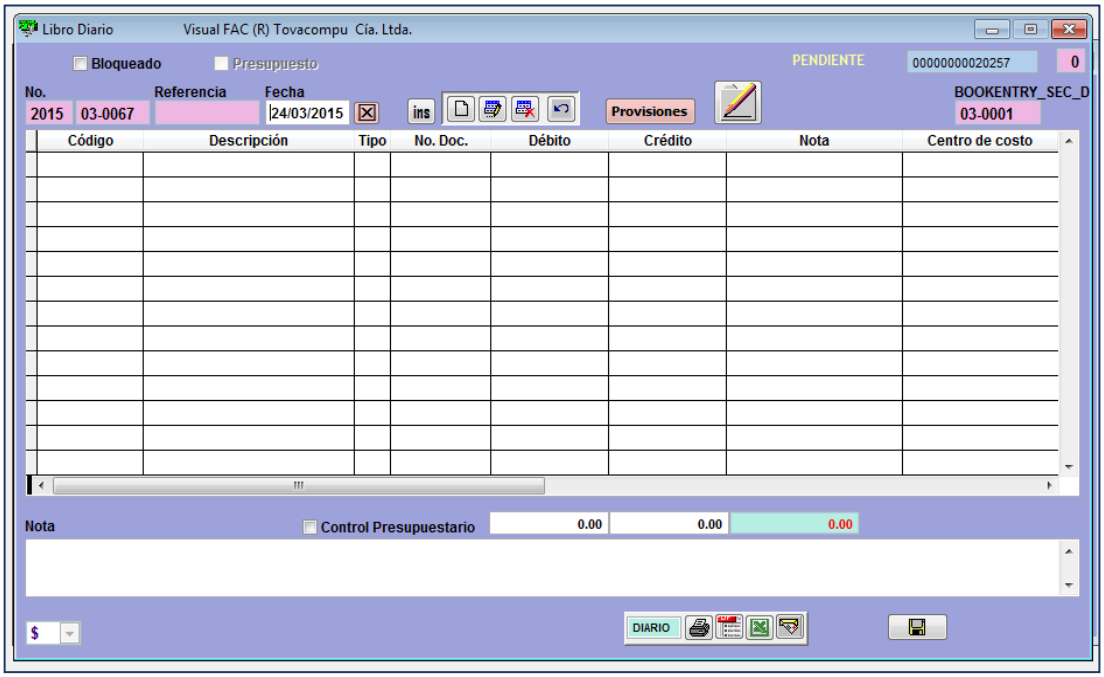


Figura 15: Libro Diario
Fuente: Los Autores

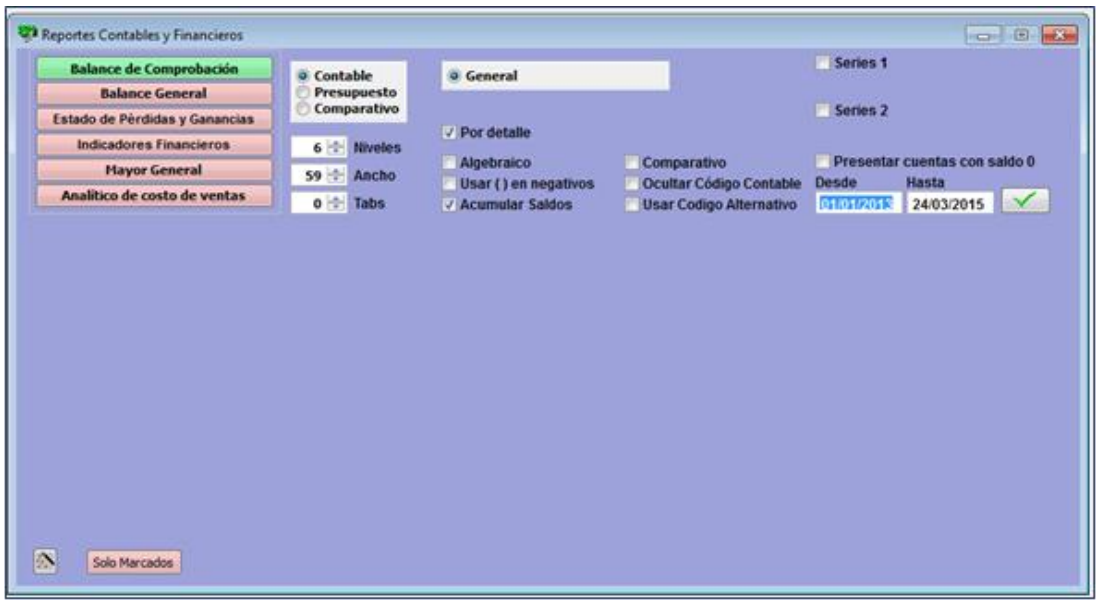


Figura 17: Reportes contables y Financieros
Fuente: Los Autores

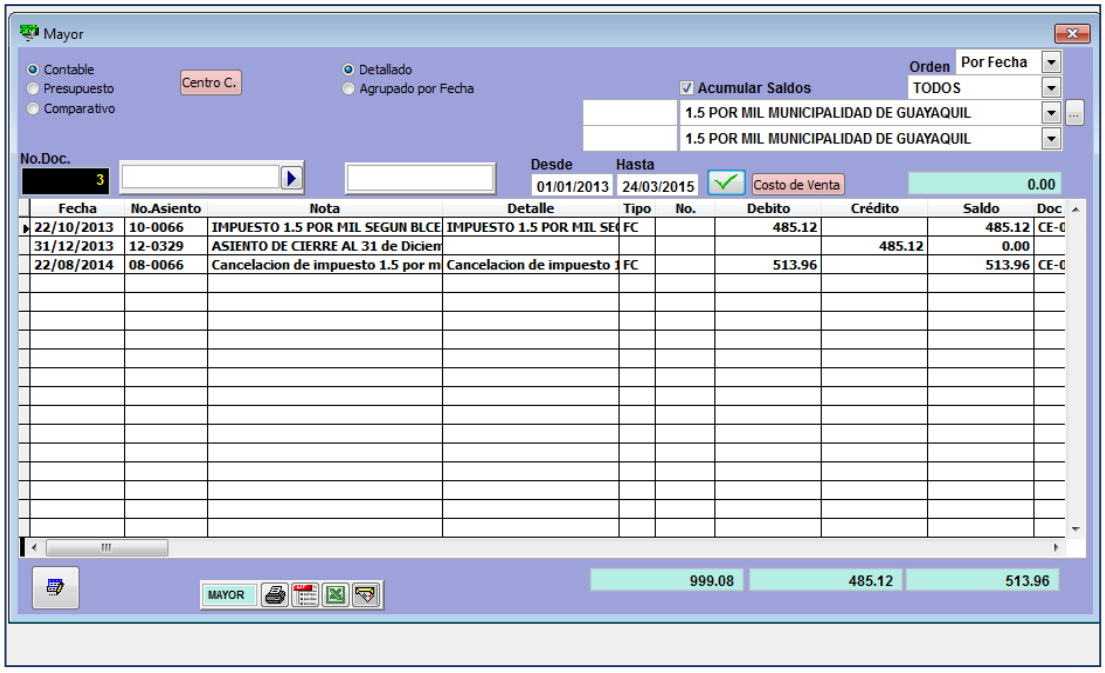


Figura 16: Libro Mayor
Fuente: Los Autores

Reportes

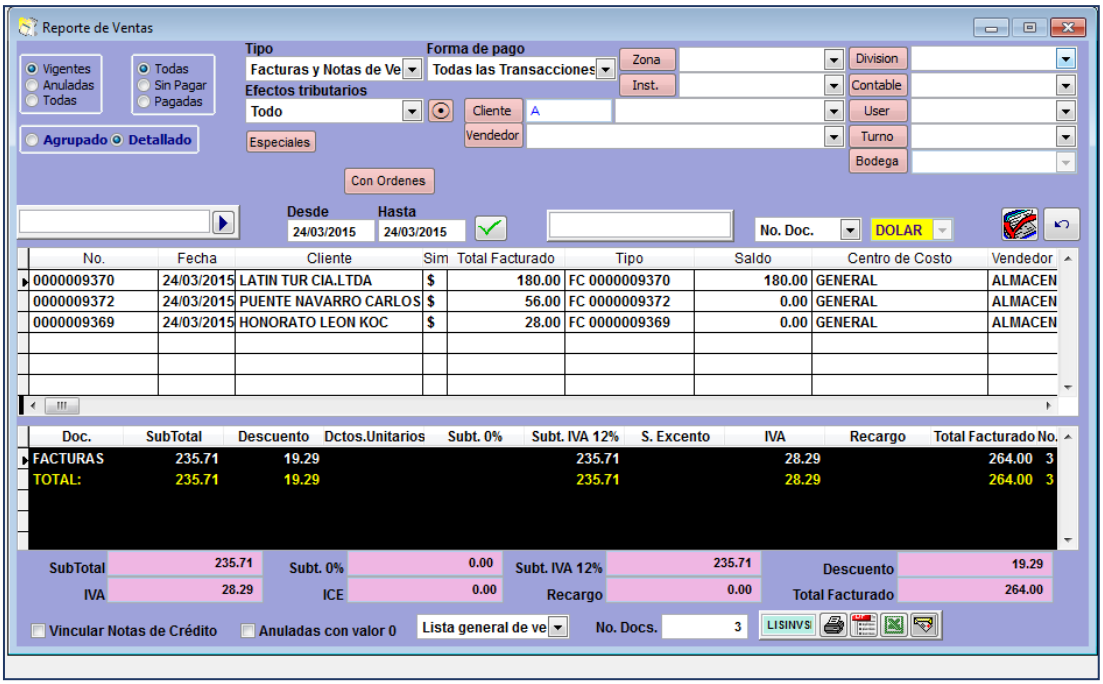


Figura 19: Reporte de Ventas
Fuentes: Los Autores

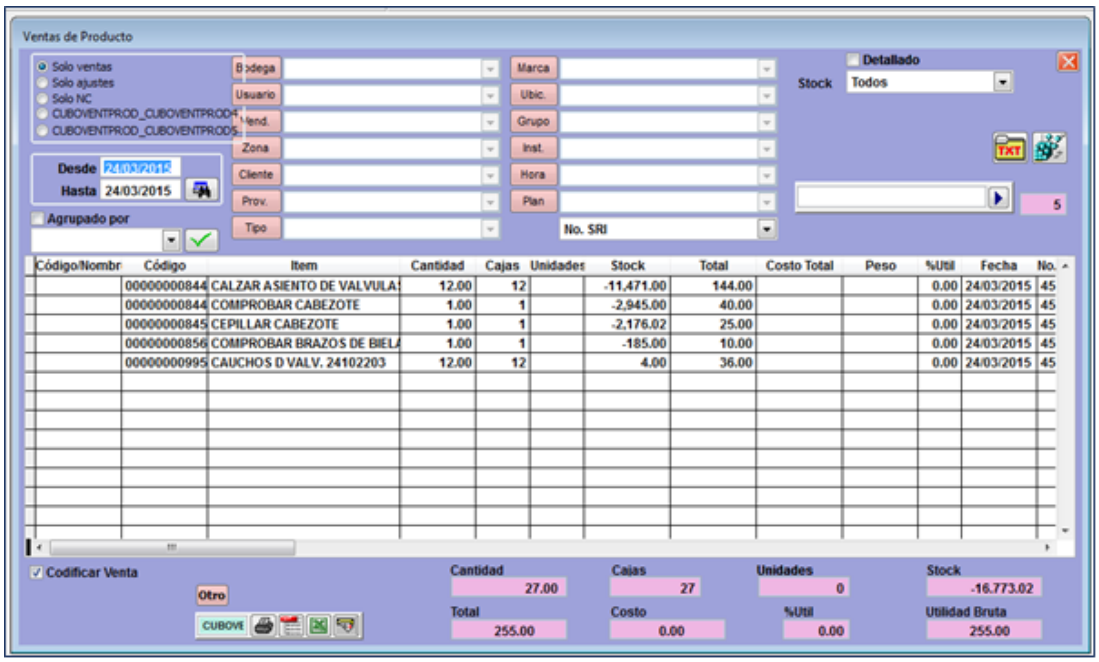
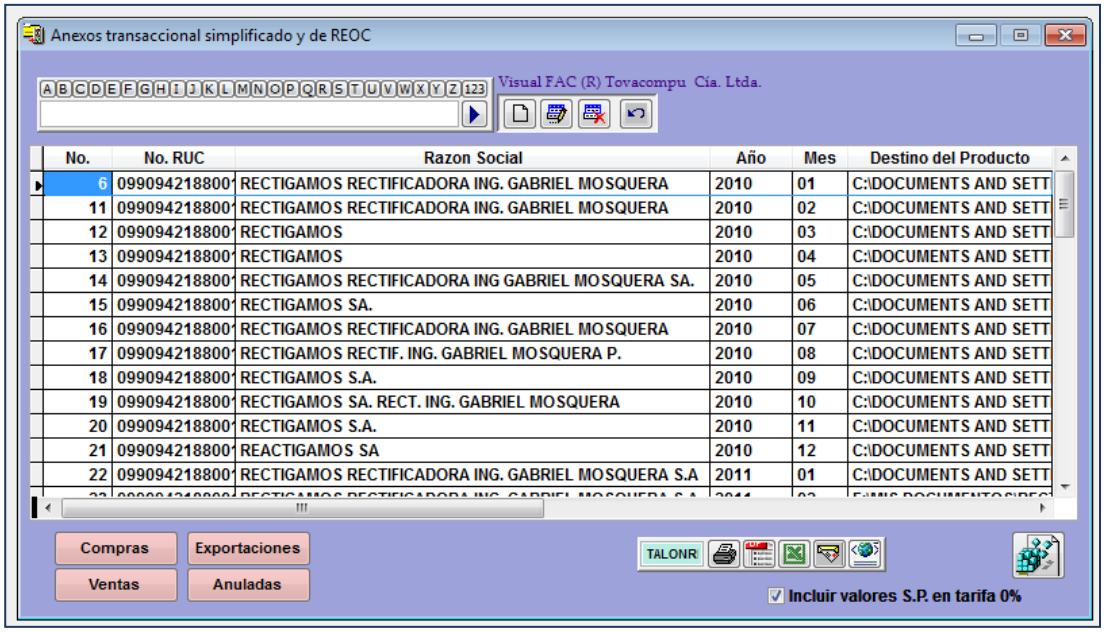


Figura 18: Ventas de Producto
Fuente: Los Autores

Anexos SRI

En este módulo se realizan los formularios y anexos que se presentan al SRI

Figura 20: Formularios SRI
Fuentes: Los Autores



No.	No. RUC	Razon Social	Año	Mes	Destino del Producto
6	0990942188001	RECTIGAMOS RECTIFICADORA ING. GABRIEL MOSQUERA	2010	01	C:\DOCUMENTS AND SETT
11	0990942188001	RECTIGAMOS RECTIFICADORA ING. GABRIEL MOSQUERA	2010	02	C:\DOCUMENTS AND SETT
12	0990942188001	RECTIGAMOS	2010	03	C:\DOCUMENTS AND SETT
13	0990942188001	RECTIGAMOS	2010	04	C:\DOCUMENTS AND SETT
14	0990942188001	RECTIGAMOS RECTIFICADORA ING GABRIEL MOSQUERA SA.	2010	05	C:\DOCUMENTS AND SETT
15	0990942188001	RECTIGAMOS SA.	2010	06	C:\DOCUMENTS AND SETT
16	0990942188001	RECTIGAMOS RECTIFICADORA ING. GABRIEL MOSQUERA	2010	07	C:\DOCUMENTS AND SETT
17	0990942188001	RECTIGAMOS RECTIF. ING. GABRIEL MOSQUERA P.	2010	08	C:\DOCUMENTS AND SETT
18	0990942188001	RECTIGAMOS S.A.	2010	09	C:\DOCUMENTS AND SETT
19	0990942188001	RECTIGAMOS SA. RECT. ING. GABRIEL MOSQUERA	2010	10	C:\DOCUMENTS AND SETT
20	0990942188001	RECTIGAMOS S.A.	2010	11	C:\DOCUMENTS AND SETT
21	0990942188001	REACTIGAMOS SA	2010	12	C:\DOCUMENTS AND SETT
22	0990942188001	RECTIGAMOS RECTIFICADORA ING. GABRIEL MOSQUERA S.A	2011	01	C:\DOCUMENTS AND SETT

Figura 21: Anexos Transaccional Simplificado y de REOC
Fuente: Los Autores

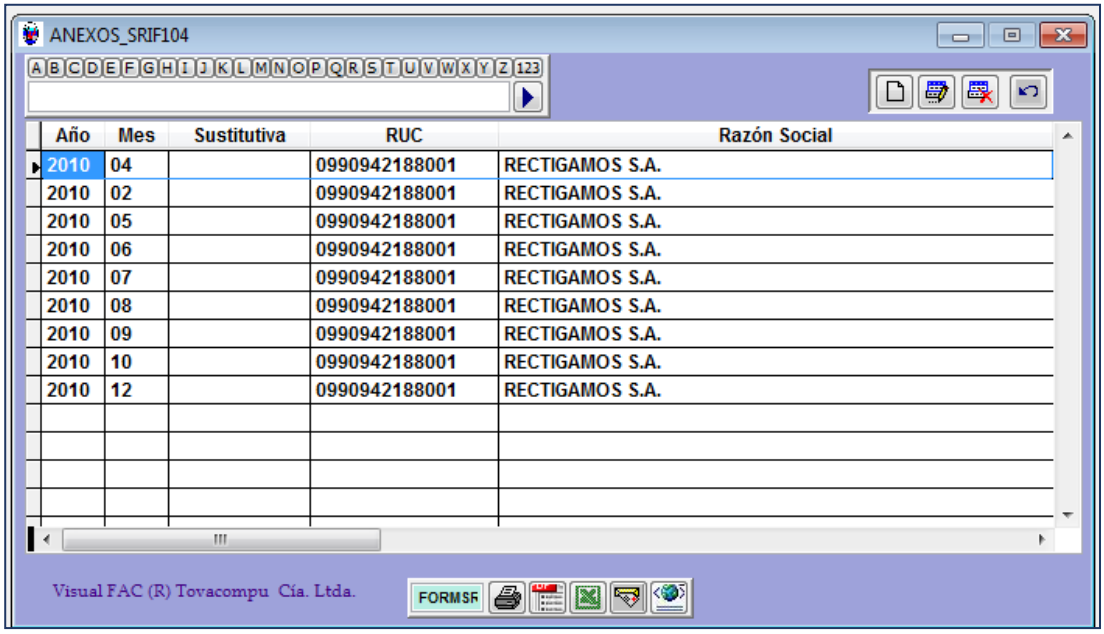


Figura 22: Formularios SRI
Fuentes: Los Autores

Nómina

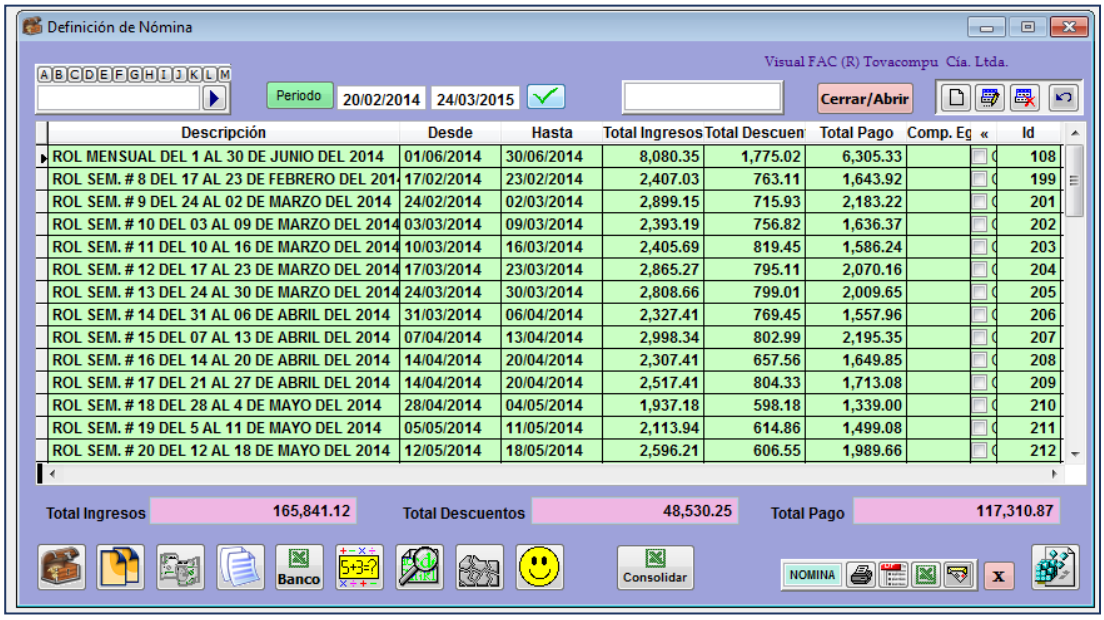


Figura 23: Módulo de Nómina
Fuente: Los Autores

Auditoria

Figura 24: Módulo de Auditoría
Fuente: Los Autores

Caja

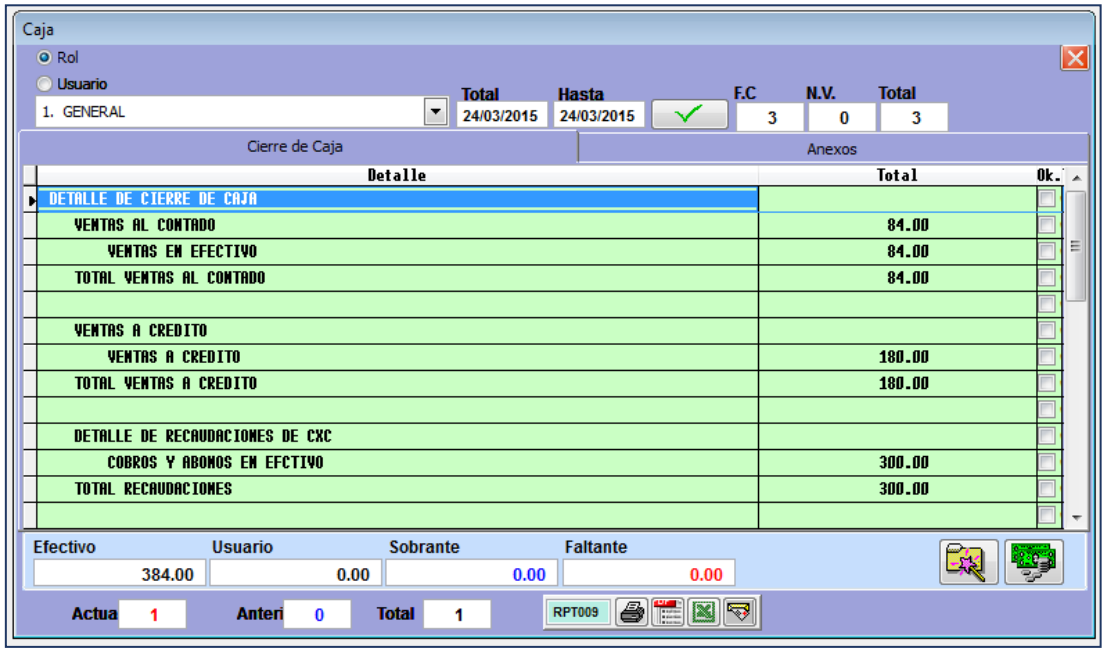


Figura 25: Módulo de Caja
Fuente: Los Autores

En la imagen a continuación se muestra el diseñador de informes con el reporte de ventas.

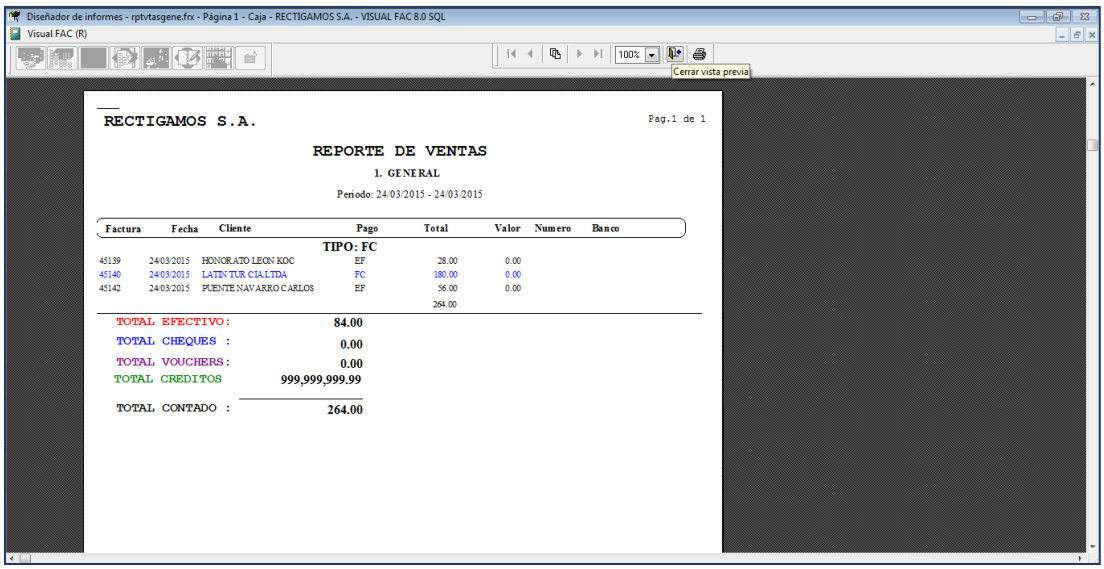


Figura 26: Reporte de Ventas
Fuente: Los Autores

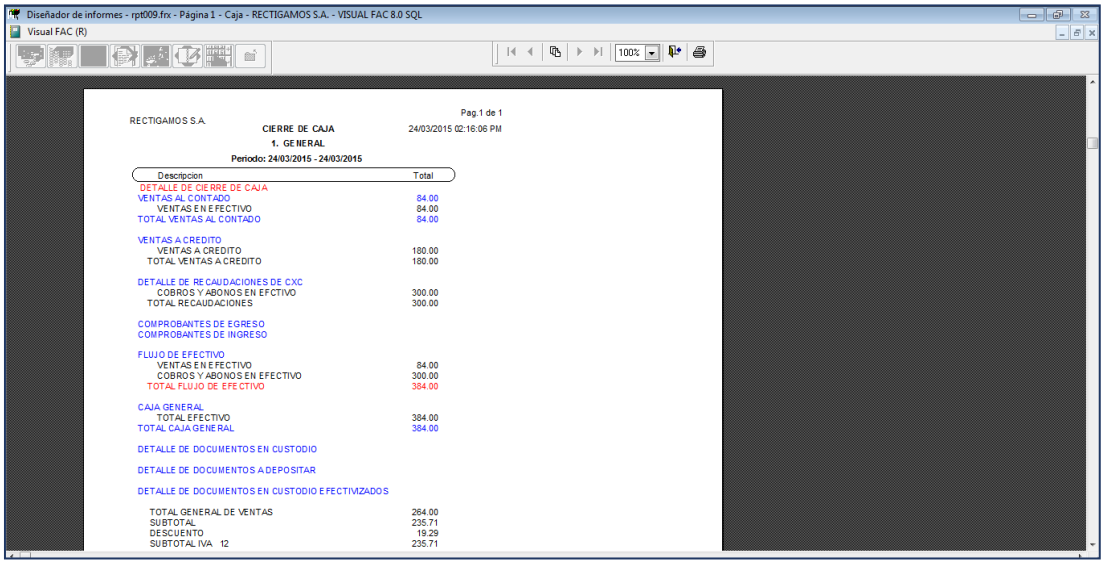


Figura 27: Cierre de caja
Fuente: Los Autores

Inventario

En el módulo de inventario se muestra las diferentes opciones para mantener actualizado el estado de los bienes en bodega.

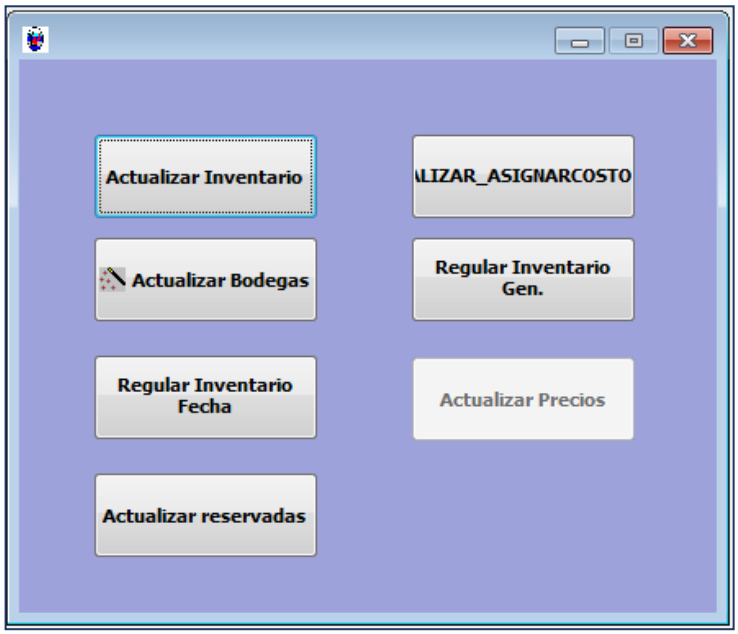


Figura 28: Módulo de Inventario
Fuente: Los Autores

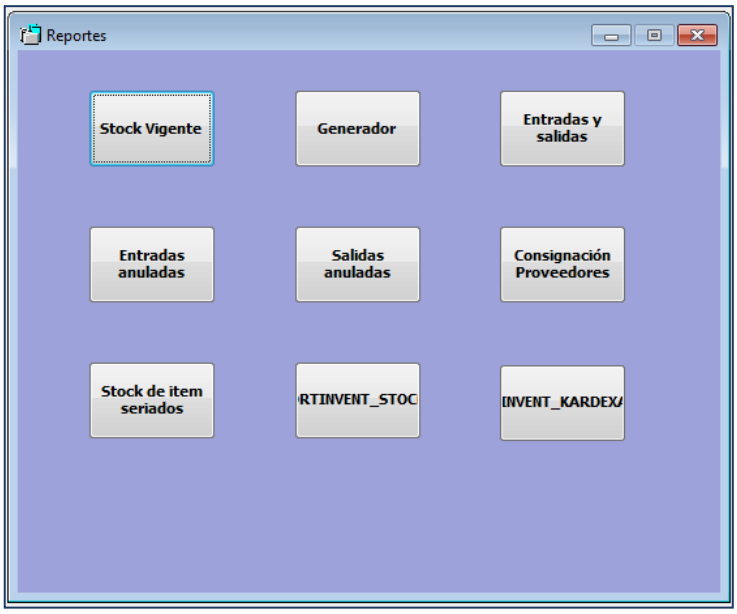


Figura 29: Inventario – Reportes
Fuente: Los Autores

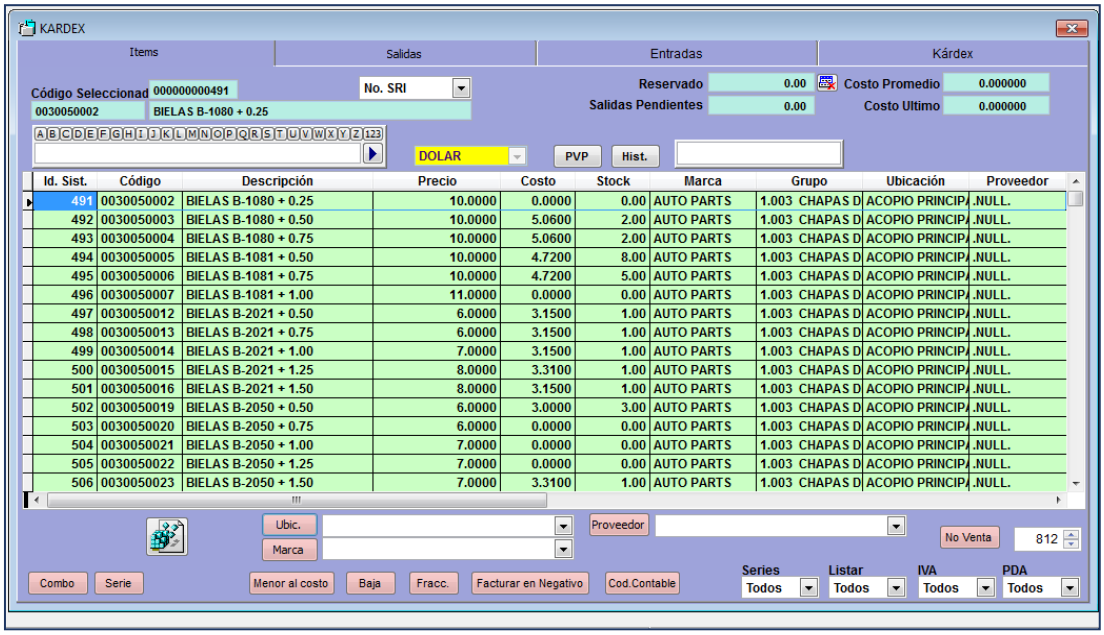


Figura 30: Kardex
Fuente: Los Autores

Herramientas ofimática: En RECTIGAMOS S.A. los miembros de personal utilizan Microsoft Word y Excel 2010 para realizar sus tareas e informes.

Cliente de Correo: Como aplicación utilizan Outlook que es un cliente de correo electrónico de Microsoft. Se encuentra instalado en todas las computadoras de la empresa porque es un medio importante de comunicación interna y externa.

1.2. Enunciado del problema

Diagnóstico de las vulnerabilidades informáticas en los Sistemas de Información para proponer soluciones de Seguridad a la empresa RECTIGAMOS S.A.

1.3 Formulación del Problema

Para el desarrollo de la tesis se tendrá que considerar los siguientes aspectos:

¿Por qué los procesos actuales de seguridad informática y de la información no son los adecuados para la empresa?

¿Por qué el sistema de gestión actual de la seguridad de la información que tiene implementado la empresa no es eficiente?

¿Por qué la no estandarización en los Sistemas de Información provoca riesgos de seguridad?

¿Cuáles son los factores que inciden para que se presenten fallos e interrupciones en la infraestructura?

1.4. Objetivos

1.4.1 Objetivo general

Identificar los procesos de seguridad físicos y lógicos para la información que están implementados en la empresa de servicios para proceder a evaluar, formular, recomendar y plantear soluciones.

1.4.2 Objetivos específicos

- ✓ Identificar las vulnerabilidades que están presentes y que provocan daños en el esquema de los Sistemas de Información.
- ✓ Proponer políticas y estándares en los sistemas de información evitando así riesgos de seguridad en los datos.
- ✓ Detectar las causas por las cuales los procedimientos están provocando fallos en los Sistemas de Información de la empresa.

1.5. Justificación

La seguridad en los Sistemas de Información se ha convertido hoy en día en el eje principal para fijar la protección ante amenazas a las cuales las empresas se encuentran expuestas en el día a día.

La empresa RECTIGAMOS S.A. al igual que cualquier empresa de servicios usa los sistemas de información para su operatividad, convirtiéndose en un activo fundamental que necesita asegurarse ante las amenazas que pueden afectar su disponibilidad, integridad, confidencialidad y confiabilidad. En este sentido, se deben establecer procedimientos adecuados y controles de seguridad basados en el análisis de riesgos para conocerlos y afrontarlos de manera adecuada, lograr reducir las amenazas hasta alcanzar un nivel asumible por la empresa y disminuir los costos derivados de una racionalización de los recursos.

Con los resultados obtenidos de este proyecto se busca exponer las posibles vulnerabilidades y se espera ofrecer una solución para que la empresa disponga de un método que le permita identificar cuáles son sus activos primordiales, cuáles son las amenazas que afectan a dichos activos, y así determinar cuál es el impacto que tendrá en la empresa si esas amenazas se materializan permitiendo establecer los controles necesarios para mitigar los riesgos encontrados.

De igual manera, se espera que este estudio sirva como base para futuras investigaciones en el área, así como aportar una alternativa para el resto de las empresas u organizaciones con problemática similar.

CAPITULO II

MARCO DE REFERENCIA DE LA INVESTIGACIÓN

2.1. Marco teórico

En este capítulo se realiza una revisión de las herramientas que se utilizan para efectuar la intrusión, su definición sus principales términos y usos, además de especificar los elementos de la seguridad informática, redes, arquitecturas, y protocolos. Se ingresa al ámbito de los intrusos y se los clasifica, detallando los modos de operación.

Para el desarrollo del estudio se realiza en primer lugar un levantamiento de información de los procesos más críticos de la empresa. Para la recopilación de la información se realizan entrevistas con formularios a los usuarios responsables de ejecutar cada proceso esto con el fin de medir el nivel de criticidad. Como herramientas se usarán diferentes programas utilizados para probar la seguridad de la organización.

El alcance del estudio permitirá proponer controles y políticas basados en el análisis de los posibles riesgos a los cuales pueden estar expuestos los equipos de cómputo y sistemas de información.

2.1.1. Introducción a la Seguridad

Cuando se piensa en seguridad, se comienza por tomar en cuenta las cosas personales. Todos tienen objetos que realmente les importan, unos que serían irremplazables y otros que tienen un gran valor sentimental. Todos tienen cosas que no quieren que otras personas se enteren, incluso algunas sin las cuales tampoco podrían vivir. Piense ahora en donde las guarda.

Podría ser en su casa, automóvil, unidad educativa u oficina, en un bolso, cartera o en otros numerosos lugares. Piense en todo lo que podría ocurrirle a sus pertenencias. Puede ser asaltado o encontrarse en un desastre natural por ejemplo un incendio, un terremoto o una inundación. De cualquier manera

desea proteger sus posesiones, sin importar de donde proviene la amenaza. (Wiley, 2012).

De igual manera la seguridad en informática, es el arte de protección del bien invaluable más importante de una organización como lo es la información que necesita ser protegida mediante controles que mitiguen los riesgos que se encuentren en la investigación pertinente.

A continuación se presenta referencia a varios conceptos que ayudarán a entender el tema planteado y determinar las partes de su estudio.

a) Seguridad Informática

Esta disciplina se encargaría de las implementaciones técnicas de la protección de la información, el despliegue de las tecnologías antivirus, firewalls, detección de intrusos, detección de anomalías, correlación de eventos, atención de incidentes, entre otros elementos, que articulados con prácticas de gobierno de tecnología de información establecen la forma de actuar y asegurar las situaciones de fallas parciales o totales, cuando la información es el activo que se encuentra en riesgo. ([Jeimy J. Cano, s.f.)

Existen también diferentes definiciones del término Seguridad Informática. Se considerará la definición ofrecida por el estándar para la seguridad de la información ISO/IEC 27001, que fue aprobado y publicado en octubre de 2005 por la International Organization for Standardization (ISO) y por la comisión International Electrotechnical Commission (IEC).

"La seguridad informática consiste en la implantación de un conjunto de medidas técnicas destinadas a preservar la confidencialidad, la integridad y la disponibilidad de la información, pudiendo, además, abarcar otras propiedades, como la autenticidad, la responsabilidad, la fiabilidad y el no repudio." (Mifsud)

b) Seguridad de la Información

Es la disciplina que habla de los riesgos, de las amenazas, de los análisis de escenarios, de las buenas prácticas y esquemas normativos, que exigen niveles de

aseguramiento de procesos y tecnologías para elevar el nivel de confianza en la creación, uso, almacenamiento, transmisión, recuperación y disposición final de la información. ([Jeimy J. Cano, s.f.)

2.1.2. Auditoria Informática

La auditoría informática es el proceso de recoger, agrupar y evaluar evidencias para determinar si un sistema informatizado salvaguarda los activos, mantiene la integridad de los datos, lleva a cabo eficazmente los fines de la organización y utiliza eficientemente los recursos. (Roldan, s.f.)

2.1.3. Sistema Informático

Un sistema informático es un conjunto de partes que funcionan relacionándose entre sí con un objetivo preciso. Sus partes son: hardware, software y las personas que lo usan. (Alegsa, s.f.)

Para que un sistema se pueda definir como seguro debe estar dotado de las siguientes cuatro características:

Integridad: La información no puede ser modificada por quien no está autorizado

Confidencialidad: La información solo debe ser legible para los autorizados

Disponibilidad: Debe estar disponible cuando se necesita

Irrefutabilidad: (No-Rechazo o No Repudio) Que no se pueda negar la autoría (Samuel, s.f.)

2.1.4. Bugs (error de software)

Se refiere a una debilidad o defecto o error en un sistema informático, el cual lo hace vulnerable a ataques informáticos (virus, ciberdelicuentes, etc.). También se le conoce como agujeros de seguridad. (seguridadpc, s.f.)

2.1.5. Vulnerabilidad Informática

Se refiere a una debilidad en un sistema informático permitiendo a un atacante violar el control de acceso y a la confidencialidad de datos y aplicaciones.

Las vulnerabilidades son el resultado de fallos (bugs) en el diseño o desarrollo o a las propias limitaciones del sistema. Cabe mencionar que no existe sistema 100% seguro. (seguridadpc, s.f.)

2.1.6. Concepto de Amenaza

Se puede definir como amenaza a todo elemento o acción capaz de atentar contra la seguridad de la información. Las amenazas surgen a partir de la existencia de vulnerabilidades, es decir que una amenaza sólo puede existir si existe una vulnerabilidad que pueda ser aprovechada, e independientemente de que se comprometa o no la seguridad de un sistema de información. (seguridadinformatica, s.f.)

Tipos de amenazas

Las amenazas pueden clasificarse en dos tipos:

- Intencionales, en caso de que deliberadamente se intente producir un daño (por ejemplo el robo de información aplicando la técnica de trashing, la propagación de código malicioso y las técnicas de ingeniería social).
- No intencionales, en donde se producen acciones u omisiones de acciones que si bien no buscan explotar una vulnerabilidad, ponen en riesgo los activos de información y pueden producir un daño (por ejemplo las amenazas relacionadas con fenómenos naturales) (seguridadinformatica, s.f.)

2.2. Marco Conceptual

Exploit

Es un programa de prueba de concepto que puede estar en código fuente para compilar (fuente.c) o formato binario tipo .exe. Sirve para aprovechar o demostrar

una vulnerabilidad en una aplicación y puede estar en escrita en varios lenguajes de programación. (Tori)

Script Kiddies

Es aquella persona que, sin conocimiento alguno de protocolos, sistemas operativos, ni seguridad de la información, se vale de una herramienta o técnicas ajenas para cometer intrusiones en internet u otras redes, o al menos intentarlo. (Tori, pág. 41)

2.3. Hipótesis

2.3.1. Hipótesis General

Al evaluar los Sistemas de Información aplicando metodologías y técnicas que utilizaría un intruso para violar la seguridad de un sistema informático se conocerá cuáles son las condiciones de la seguridad informática

2.3.2. Hipótesis Particulares

- El esquema actual no se rige bajo ningún estándar internacional, lo cual produce impactos negativos de seguridad.
- Al no estar estandarizado los Sistemas de Información los mecanismos de control preventivos y correctivos no brindan las garantías necesarias por lo que se generan fallos, interrupciones y fugas de información.
- La gestión de procesos mal implementados y la falta de monitoreo de eventos externos generan interrupciones en los servicios informáticos de la infraestructura del Sistema de Gestión de los Sistemas de Información volviéndolos deficientes.

2.4 Matriz causa y efecto

Tabla 3: Matriz Causa y efecto

Problema General	Objetivo General	Hipótesis General
¿Por qué los procesos actuales de seguridad informática y de la información no son los adecuados para la empresa?	Identificar los procesos de seguridad físicos y lógicos para la información que están implementados en la empresa para proceder a evaluar, formular, recomendar y plantear soluciones.	Al evaluar los Sistemas de Información aplicando metodologías y técnicas que utilizaría un intruso para violar la seguridad de un sistema informático se conocerá cuáles son las condiciones de la seguridad informática
Problemas Específicos	**Objetivos Específicos**	**Hipótesis Particulares**
¿Por qué el sistema de gestión actual de la seguridad de la información que tiene implementado la empresa no es eficiente?	Identificar las vulnerabilidades que están presentes y que provocan daños en el esquema de los Sistemas de Información	El esquema actual no se rige bajo ningún estándar internacional, lo cual produce impactos negativos de seguridad.
¿Por qué la no estandarización en los Sistemas de Información provoca riesgos de seguridad?	Proponer políticas y estándares en los sistemas de información, evitando así riesgos de seguridad en los datos	Al no estar estandarizado los Sistemas de Información los mecanismos de control preventivos y correctivos no brindan las garantías necesarias por lo que se generan fallos, interrupciones y fugas de información.
¿Cuáles son los factores que inciden para que se presenten fallos e interrupciones en la infraestructura tecnológica?	Detectar las causas por las cuales los procedimientos están provocando fallos en los Sistemas de Gestión de los Sistemas de Información de la empresa.	La gestión de procesos mal implementados y la falta de monitoreo de eventos externos generan interrupciones en los servicios informáticos de la infraestructura del Sistema de Gestión de los Sistemas de Información volviéndolos deficientes.

Elaborado por: Los Autores

2.5. Variables e indicadores

2.5.1 Variables independientes

El estudio de las vulnerabilidades por medio de la herramienta MSAT

2.5.2 Variables dependientes

Mitigación de los riesgos, reducción de vulnerabilidades.

2.6. Población y muestra

2.6.1. Población

El Personal del Departamento de TI, quienes tienen la información y conocen los procesos actuales dentro de la organización.

La empresa RECTIGAMOS S.A. se encuentra integrada por los siguientes elementos destacados en la Tabla 3.

Tabla 4: Departamentos de Rectigamos

DEPARTAMENTOS	NÚMERO DE PERSONAL
GERENCIA	2
CONTABILIDAD	9
VENTAS	3
TALLER	5
BODEGA	2
SISTEMAS	2
TOTAL PERSONAL	23

Elaborado por: Los Autores

El estudio que se ha realizado, está dirigido a toda el área que tienen que ver con el departamento de TI y que utilizan los sistemas informáticos, correo e internet.

El número involucrados con los servicios del departamento de TI es 23 personas

2.6.2 Muestra

El Departamento de Sistemas está conformado por 2 personas que cumplen con funciones específicas en la administración de los Sistemas de Información.

El Marco Muestral utilizado en el diseño de la muestra corresponde a la totalidad área o departamentos de la empresa RECTIGAMOS S.A. que utilizan los servicios informáticos del departamento de TI por lo tanto el muestreo será por cuotas y dirigido, a la unidad final de muestreo: El administrador o quien lo represente de cada departamento, de manera tal que los instrumentos de interés estén en los parámetros representados apropiadamente.

Tamaño de la muestra

Para establecer el tamaño de la muestra se calcula mediante la siguiente expresión matemática de manera probabilística:

$$n = \frac{Z^2 PQN}{\frac{(N-1)\,E^2}{K^2} + Z^2 PQ}$$

De donde:

Tabla 5: Simbología

n	Tamaño de la muestra
PQ	Constante de varianza de la población (0.50)
N	Tamaño de la población
E	Error máximo admisible (al 1% = 0.01; 2 % = 0.02; 3% = 0.03, etc.). A mayor error probable, menor tamaño de la muestra y viceversa.
K	Coeficiente de corrección del error.

Elaborado por: Los Autores

Usuarios que utilizan los servicios básicos del departamento de TI son 23

22 empleados de la empresa corresponden a la muestra de los seleccionados al azar.

CAPITULO III

MARCO METODOLÓGICO

3.1. Tipo de investigación

3.1.1. Investigación exploratoria

Se realiza ante la falta de información o de organización del problema que se quiere investigar. Un estudio cualitativo es un muy buen ejemplo de estudio exploratorio, ya que se puede obtener un análisis preliminar de la situación. Entre los métodos más usados se encuentran: la observación y la entrevista. (Namakforoosh, 2005).

Se utiliza este método porque facilita la información para obtener un conocimiento más amplio respecto al problema del estudio de riesgo, incidentes, amenazas etc. que ocurren en la empresa.

3.1.2. Investigación descriptiva

El estudio describe todos los procesos y errores que son causados al momento de efectuar actividades en las cuales son incurridas grandes cantidades de datos y la forma que afecta directa e indirectamente en el progreso de las actividades desarrolladas diariamente en la empresa.

3.1.3. Investigación explicativa

Es explicativa porque determina cuáles son las causas que desde un principio han ocasionado problemas, los cuales deben tener soluciones inmediatas para mejoras en el campo de trabajo.

3.1.4. Investigación de campo

Es de campo porque se basa en la observación de los acontecimientos y en los testimonios de las personas que laboran en el departamento y realizan a diario estos procedimientos para de esta manera encontrar soluciones viables a la realidad.

3.1.5. Investigación no experimental

Es no experimental porque el objeto de estudio es observado en su contexto natural, en su realidad día a día sin realizarle cambios, analizándolos como se efectúan naturalmente en su ambiente en el que estos ocurren.

3.2. Métodos de investigación

De acuerdo al análisis de la investigación y acciones correctivas que van a ser presentadas para la evaluación en lo que respecta a la seguridad informática, se utiliza los siguientes métodos de investigación:

3.2.1. Método inductivo – deductivo

De nuestras ideas y conjeturas permite obtener una conclusión, para llegar a resultados con acciones correctivas asegurando el cumplimiento de lo propuesto.

3.2.2. Método observativo

Utilizado para la detección visual de fallas de seguridad física que implique riesgos de la seguridad informática.

3.2.3. Método Sistémico

Utilizado para determinar las vulnerabilidades en los Sistemas informáticos y en los Sistemas de Información de la empresa se realizó el análisis en 3 etapas, las mismas que se detallan a continuación

Etapa 1 – Reconocimiento

El reconocimiento se refiere a la fase preparatoria donde se obtiene toda la información necesaria del objetivo de estudio. Esta fase también puede incluir el escaneo de la red de manera interna o externa.

Esta fase incluye la Ingeniería Social, busca que tipo de sistema operativo y aplicaciones, cuales son los puertos que están abiertos, donde están localizados los routers, cuales son los host (terminales, computadoras) más accesibles, busca en las bases de datos del Internet (Whois) información como direcciones de Internet (IP),

nombres de dominios, información de contacto, servidores de email y toda la información que se pueda extraer de los DNS. En esta fase se analiza toda la información que se ha obtenido para lanzar los ataques con mayor precisión.

Etapa 2 – Escaneo

En esta fase se utiliza toda la información que se obtuvo en la Fase del reconocimiento. En esta fase se buscan más vulnerabilidades que permitan el acceso al sistema.

Etapa 3 – Ganar Acceso

Esta es una de las fases más importantes existe la penetración al sistema, en esta punto se explota las vulnerabilidades que se encontraron en la fase 2. La explotación puede ocurrir localmente, Los factores que ayudan a tener una penetración exitosa al sistema dependen de cómo es la arquitectura del sistema y de cómo está configurado el sistema, una configuración de seguridad simple significa un acceso más fácil al sistema, otro factor a tener en cuenta es el nivel de destrezas, habilidades y conocimientos sobre seguridad informática y redes que tenga el nivel de acceso que obtuvo al principio de la penetración.

3.3. Fuentes

3.3.1. Fuentes Primarias

Las fuentes utilizadas fueron las siguientes:

a) Entrevista con personal encargado de la supervisión de los procesos
b) Entrevista con personal encargado de contabilidad
c) Entrevista con personal encargado del área de sistemas
d) Cuestionario de preguntas para la investigación dirigidos a: Gerencia, Departamento Contable, Taller, Sistemas y Bodega

3.3.2. Fuentes Secundarias

Dentro de las fuentes de información secundaria que se utilizaron se encuentran:

a) Manual de normas y procedimientos basados en estándares internacionales 27001

b) Libros relacionados con el tema de estudio, trabajos de graduación, publicaciones en internet escritos en publicaciones, revistas periódicos, etc.

3.4. Técnicas de recolección de datos

Las técnicas de la siguiente encuesta fueron realizadas al jefe o personal encargado de los diferentes procesos críticos de la empresa industrial.

En el capítulo 4 se detalla los nombres de los procesos críticos, los nombres de los diferentes tipos de amenazas y vulnerabilidades sobre las cuales fueron evaluados los activos.

Los cuestionarios de preguntas de cada proceso se encuentran en el anexo A del presente proyecto.

CAPITULO IV

ANÁLISIS Y RESULTADOS DEL PROYECTO

4.1. Metodología para el análisis y evaluación de riesgos en las TI

Una evaluación efectiva de riesgos en la seguridad de la información considera tanto los temas organizacionales como los técnicos, examina cómo los usuarios emplean la infraestructura diariamente en su entorno. Además es una práctica fundamental porque genera una visión para la empresa acerca de los riesgos, proporcionando una base para futuras mejoras.

Toda empresa u organización tiene como gran reto administrar estos riesgos porque de lo contrario le puede generar altos costos. En consecuencia se debe contar con una metodología, para el análisis y gestión de riesgos pues de lo contrario los resultados y conclusiones no son confiables y difícilmente serán de valor para la entidad.

El análisis de los riesgos se puede determinar siguiendo algunos pasos pautados:

- Determinar los activos relevantes para la organización.
- Determinar a qué amenazas están expuestos aquellos activos.
- Estimar el impacto, definido como daño sobre el activo derivado de la materialización de la amenaza.
- Determinar qué controles hay dispuestos y qué tan eficaces son frente al riesgo.
- Estimar el riesgo, definido como el impacto en relación a la probabilidad de ocurrencia de la amenaza.

El desafío más importante es entender la interrelación que tiene el proceso de negocio con los riesgos de los activos de TI que son necesarios para que los mismos funcionen correctamente. Para ello es necesario ver el modelo de negocio y cómo los activos interactuarán con cada uno de los procesos.

Se recomienda subdividir los procesos de la organización y buscar las diferentes dependencias que hay entre esos procesos y los activos; esto puede depender de más de una aplicación y, a su vez, una aplicación puede depender de más de un equipo,

con lo cual los riesgos de un activo naturalmente repercuten en los activos que son dependientes y éstos a su vez de los procesos de negocio.

En consecuencia, surge la necesidad de crear estándares para el análisis y gestión de riesgos, conocidos como frameworks o marcos de trabajo, entre los cuales está NESSUS y OCTAVE (Operationally Critical Threat, Asset and Vulnerability Evaluation)

4.2. Evaluación con NESSUS

La herramienta NESSUS, permite la configuración de opciones como políticas que se pueden especificar de acuerdo a los requerimientos del escaneo de vulnerabilidades. El objetivo de realizar la auditoría en seguridad, es encontrar las falencias existentes en lo referente a controles de accesos no autorizados a la red.

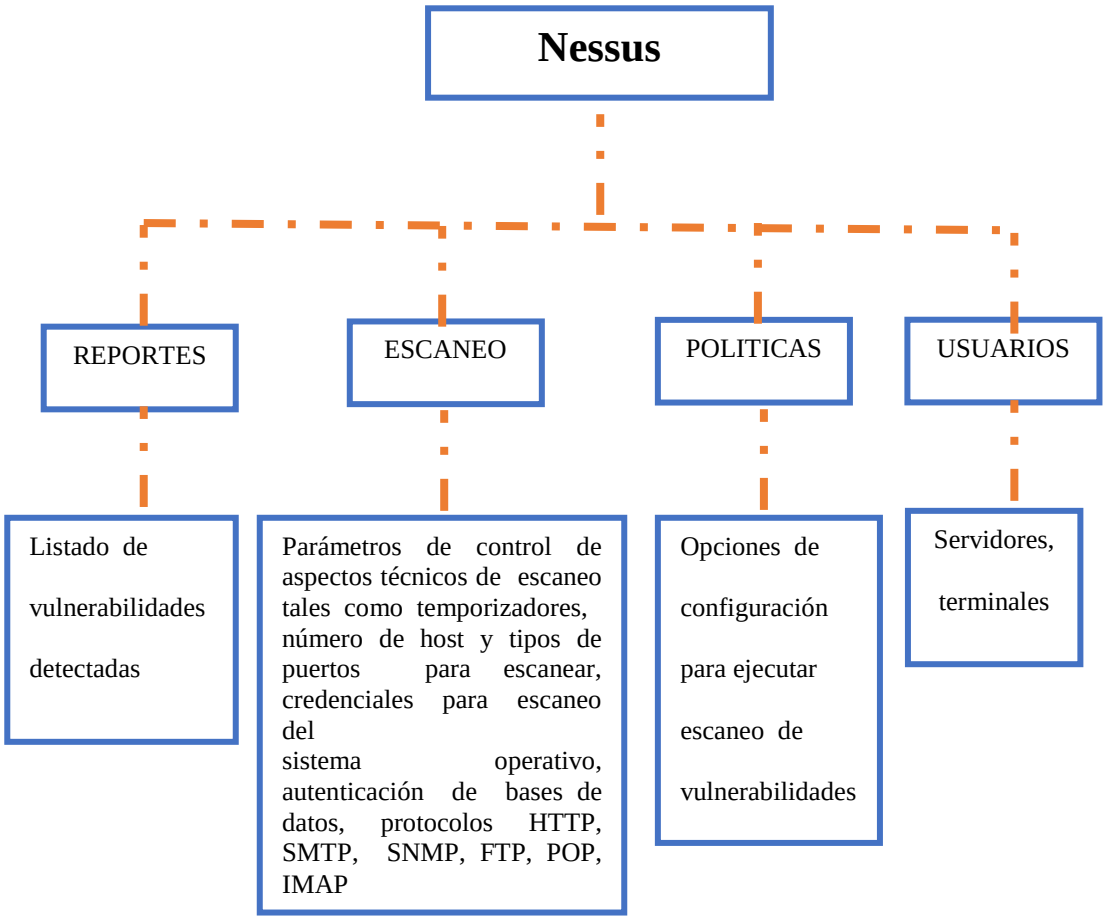


Figura 31: Componentes de la herramienta NESSUS
Fuente: Los Autores

Instalación y configuración:

Descargar la última versión de NESSUS en el sitio oficial (http://www.nessus.org/download/)

Realizar la instalación de la herramienta en base a la guía de instalación.

Una vez realizada la instalación de la herramienta NESSUS, se realiza la configuración.

Para iniciar, parar y configurar el Servidor NESSUS, se usa el NESSUS Server Manager, permitiendo realizar lo siguiente:

- ✓ Registrar el Servidor NESSUS en el sitio para recibir plugins actualizados.
- ✓ Ejecutar un plugin actualizado.
- ✓ Administrar usuarios de NESSUS.
- ✓ Iniciar o parar el Servidor NESSUS.

Para realizar las acciones mencionadas anteriormente ir a Inicio/Todos los programas/Tenable network security/Nessus64/Nessus Server Manager/ y aparecerá la ventana principal. Además se debe obtener el código de activación que será enviado al correo electrónico registrado, luego ingresar el código y hacer clic en Register, para que se active la acción Start Nessus Server.

Se realizará el análisis de vulnerabilidades a los servidores y a los equipos pertenecientes a RECTIGAMOS

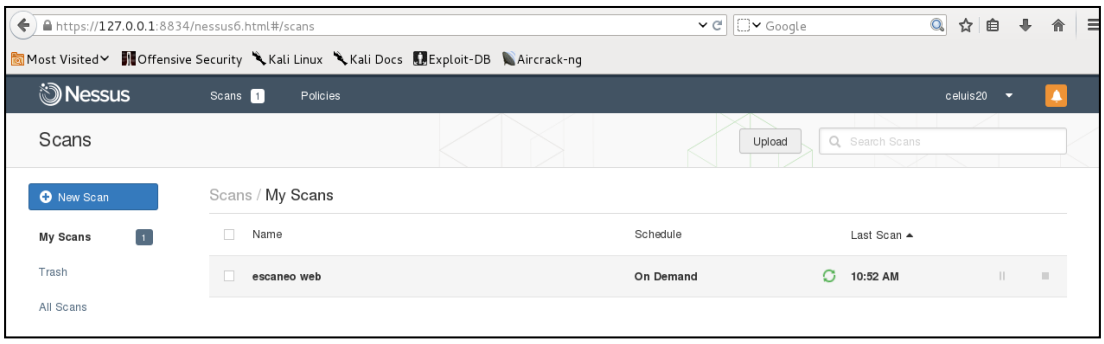


Figura 32: Escaneo web desde Nessus
Fuente: Los Autores

4.3. Evaluación de riesgos con MSAT

Mediante la evaluación con MSAT se puede determinar los riesgos a los que se enfrenta el entorno de TI de RECTIGAMOS S.A., y las medidas que se han implementado para combatirlos. El proceso permite detallar y analizar los resultados con el fin de proporcionar una guía para minimizar los riesgos encontrados.

Para el análisis de riesgos MSAT toma en cuenta las siguientes áreas:

- Infraestructura
- Aplicaciones
- Operaciones
- Personal.

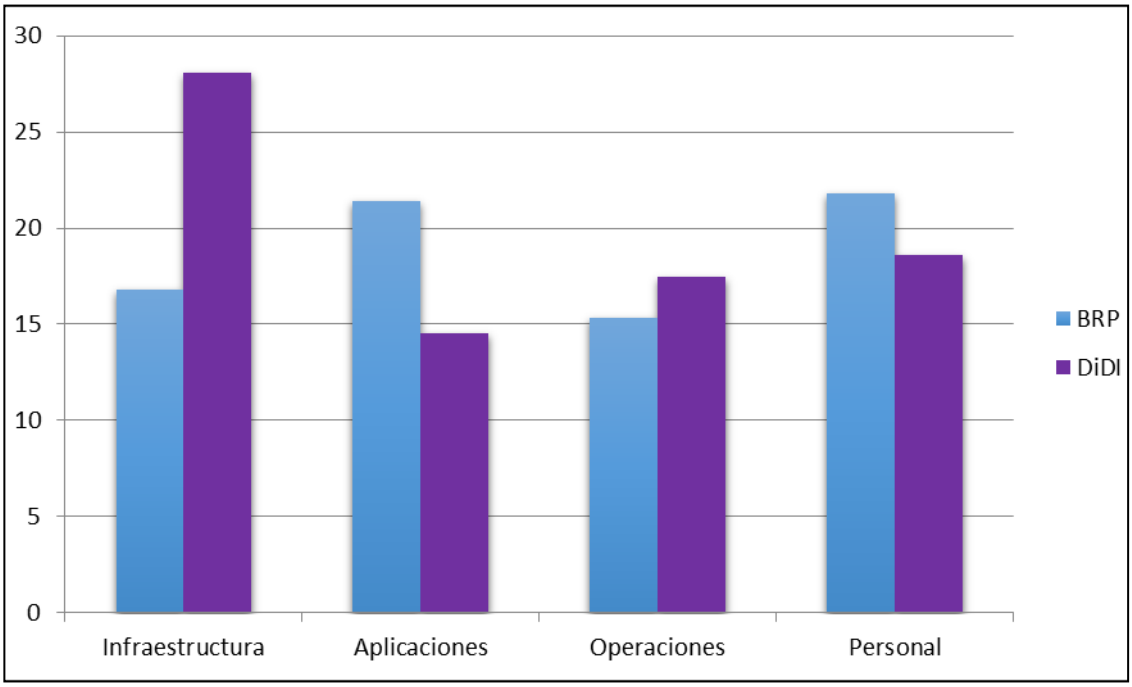


Figura 33: Análisis de riesgos MSAT
Fuente: Los Autores

En la figura 33 dividida en las cuatro áreas de análisis, se muestran las diferencias en el resultado de la defensa en profundidad.

BRP representa la medida del riesgo al que está expuesto la empresa, según el entorno empresarial y el sector en que compite, es importante tener en cuenta que una puntuación de 0 no es posible; dedicarse a una actividad comercial siempre implica un nivel de riesgo.

DiDI es el índice de defensa en la profundidad utilizada en el personal, los procesos y la tecnología para contribuir a reducir los riesgos identificados en la empresa. Según las mejores prácticas se considera adecuado tener un DiDl y un BRP del mismo nivel.

Como se aprecia en el gráfico anterior se puede concluir que RECTIGAMOS S.A. necesita mejorar las medidas de seguridad para proteger su información en relación a los riesgos a los que se encuentra sometida, por lo que se debe considerar destinar más capital, recursos tecnológicos y humanos.

4.3.1. Resultados obtenidos de la evaluación con MSAT

Luego de la evaluación de riesgos se obtiene los siguientes resultados:

Tabla 6: Evaluación de Riesgos MSAT

Áreas de análisis	Distribución de defensa de riesgos	Madurez de la seguridad
Infraestructura		
Aplicaciones		
Operaciones		
Personal		

Elaborado por: Los Autores

4.3.1.1. Infraestructura

La seguridad de la infraestructura se centra en cómo debe funcionar la red, los procesos comerciales (internos o externos) que se deben implantar, cómo se crean y utilizan los hosts, la gestión y el mantenimiento de la red. Puede ayudarle a mejorar significativamente la defensa de la red, las reacciones a incidentes, la disponibilidad de la red y el análisis de fallos. La evaluación permite establecer un diseño de la infraestructura que todos puedan comprender y seguir, podrá identificar las áreas de riesgo y desarrollar métodos para reducir las amenazas.

El área de infraestructura cuenta con las siguientes secciones:

- Defensa del perímetro: cortafuegos, antivirus, acceso remoto, segmentación
- Autentificación: directivas de contraseñas
- Gestión y control: hosts de gestión, archivos de registro
- Estación de trabajo: configuración de creación

Las secciones a su vez tienen sub-secciones, las mismas que son analizadas de acuerdo a los resultados obtenidos.

Defensa del perímetro

La defensa del perímetro trata la seguridad del perímetro de la red, donde la red interna se conecta con el exterior. Este es su primer escudo protector contra los intrusos.

Dentro de esta sección se analizan únicamente las sub-secciones en donde se encontraron riesgos:

Tabla 7: Defensa del perímetro

Infraestructura	
Defensa del perímetro	
Reglas y filtros de cortafuegos	
Antivirus	
Antivirus - Equipos de escritorio	

Antivirus - Servidores	
Acceso remoto	
Segmentación	
Sistema de detección de intrusiones (IDS)	
Inalámbrico	

Elaborado por: Los Autores

Resultados:

Tabla 8: Resultados del Análisis de la defensa del perímetro

Reglas y filtros de cortafuegos	No hay controles de acceso de nivel de red en el perímetro de la misma. Los cortafuegos son la primera línea de defensa, de ahí que resulten imprescindibles para proteger la red de los intrusos. No utiliza software de cortafuegos basados en hosts para proteger los servidores. El cortafuego no se comprueba regularmente para asegurarse de que funciona correctamente.
Acceso Remoto	Existen empleados y/o socios que se conectan remotamente a la red interna, pero no utiliza ninguna tecnología VPN para permitirles un acceso seguro.
Segmentación	La red presenta un sólo segmento.
Sistema de detección de intrusiones (IDS)	No se utiliza ningún hardware ni software de detección de intrusiones.
Inalámbrico	Se ha modificado el SSID

	predeterminado del punto de acceso, se utiliza cifrado WPA en el entorno inalámbrico.

Elaborado por: Los Autores

No hay controles de acceso en el perímetro de la red, no utiliza software de cortafuegos basados en hosts para proteger los servidores.

El cortafuegos no se comprueba regularmente para asegurarse de que funciona correctamente, lo que permite en algunos casos que empleados y/o socios se conecten remotamente a la red interna, sin utilizar tecnología VPN (permite un acceso seguro). Esto pone en riesgo la información a la que se está accediendo, que por un momento está a la vista de todo usuario en internet que sepa cómo acceder a la misma.

La red presenta un sólo segmento, no utilizar segmentos de red en la empresa impide que el tráfico específico se encamine a los servidores de las aplicaciones, y a los puertos para dar servicio a los usuarios. Debido a que RECTIGAMOS S.A no ofrece servicio a los clientes a través de la red y el tráfico de la intranet no es demasiado alto, no sería un requerimiento altamente necesario.

Al revisar las actividades en el computador, la empresa no cuenta con un sistema de detección de intrusos basado en Host que permita detectar anomalías que indiquen un riesgo potencial.

Autenticación

Los procedimientos de autenticación de usuarios, administradores y usuarios remotos ayudan a asegurar que los intrusos no accedan sin autorización a la red mediante ataques locales o remotos, esto ayudará a acceder a los recursos de red en base a una autorización.

En esta sección se analiza únicamente las sub-secciones en donde se encontraron riesgos:

Tabla 9: Riesgos de autenticación

Autenticación	
Usuarios administrativos	
Usuarios internos	
Usuarios de acceso remoto	
Directivas de contraseñas	
Directivas de contraseñas-Cuenta de administrador	
Directivas de contraseñas-Cuenta de usuario	
Directivas de contraseñas-Cuenta de acceso remoto	
Cuentas inactivas	

Elaborado por: Los Autores

Resultados:

Tabla 10: Resultado de los riesgos de autenticación encontrados

Usuarios administrativos	Los usuarios no tienen habilitados accesos administrativos a sus estaciones de trabajo. No se utilizan inicios de sesión distintos para la administración de seguridad de los sistemas ni de los dispositivos del entorno
Usuarios de acceso remoto	Los empleados pueden conectarse a la red de forma remota, no los contratistas, ni terceros usuarios.
Directivas de contraseñas **Cuenta de usuario**	Las cuentas de usuarios no utilizan directivas de contraseñas.
Directivas de contraseñas **Cuenta de acceso remoto**	Las cuentas de acceso remoto no utilizan directivas de contraseñas

Elaborado por: Los Autores

Los usuarios tienen habilitados accesos administrativos a sus estaciones de trabajo. Esto puede provocar que usuarios inexpertos configuren las máquinas de forma errónea, que puedan abrir huecos de seguridad sin saberlo, o que ejecuten servicios que se consideren inseguros tales como FTP o telnet.

Las cuentas de usuarios y de acceso remoto no utilizan directivas de contraseñas.

Los usuarios internos y de acceso remoto crean contraseñas sin utilizar ninguna norma o política de contraseñas seguras. La creación de una política de autenticación multifactor para contraseñas complejas, permitirá incrementar la seguridad sobre los equipos y aplicaciones de la empresa.

Gestión y control

La gestión, supervisión, y el registro adecuado son elementos vitales para mantener y analizar los entornos informáticos. Estas herramientas son aún más importantes después de un ataque, cuando se necesita un análisis del incidente.

Dentro de esta sección se analizaran únicamente las sub-secciones en donde se encontraron riesgos:

Tabla 11: Riesgos de Gestión y control

Gestión y control
Informes sobre incidentes y respuesta
Creación segura
Seguridad física

Elaborado por: Los Autores

Resultados:

Tabla 12: Resultados del análisis de los riesgos de gestión y control

Creación segura	No se ha instalado cortafuegos particulares en todas las estaciones de trabajo del entorno. No hay software de acceso remoto del lado del cliente instalado en las estaciones de trabajo que se conectan remotamente a la red corporativa.
Seguridad física	No están implementadas tarjetas de identificación para empleados y visitantes, acompañantes de visitantes, registros de visitantes, ni controles de entrada. No se han instaurado controles de seguridad física para proteger los activos de la empresa.

Elaborado por: Los Autores

La información de las aplicaciones es almacenada sin ser cifrada en el medio de almacenamiento. Esto exponen los datos de los clientes, y los datos financieros de la empresa a un riesgo alto, ya que las cintas pueden perderse o ser robados y cualquier persona podría acceder a la misma, lo que afectaría las operaciones de la empresa por la pérdida de la información.

No están implementadas tarjetas de identificación para empleados y visitantes, ni controles de entrada. Las tarjetas de identificación garantizan que no acceda personal no autorizado a las instalaciones de la empresa, y los controles de entrada previenen el ingreso de objetos no permitidos como armas. De esta manera se garantiza la seguridad del personal.

Análisis general área infraestructura

Para el área de infraestructura, se analiza las secciones de gestión y control, defensa del perímetro, y autenticación, todas las subsecciones que según MSAT presentan carencias severas de seguridad. En el siguiente apartado se presenta un resumen de los problemas que se consideran más graves dentro de esta área:

Existen empleados y/o socios que se conectan remotamente a la red interna sin utilizar ninguna tecnología VPN que les permita acceso seguro por lo que la información queda expuesta.

Los usuarios tienen habilitados accesos administrativos en sus estaciones de trabajo. Este problema en especial no se lo puede corregir debido a que se ha comprobado que Gestor funciona únicamente si el usuario tiene habilitados los permisos de administrador.

Las contraseñas que se utiliza para acceder a las cuentas de usuarios y para acceso remoto no siguen ninguna política de contraseñas seguras, lo que se debería implementar para aumentar la seguridad.

La información de las aplicaciones es almacenada sin ser cifrada en el medio de almacenamiento. Esto expone a la información que se almacena, ya que cualquier persona que tenga acceso a las cintas puede verla.

Por los motivos expuestos MSAT marca a esta área con un estado de alerta de color amarillo, es decir, que no cumple con las mejores prácticas recomendadas y necesita ser mejorada.

4.3.1.2. Aplicaciones

El área de aplicaciones cuenta con las siguientes secciones:

- Implementación y uso
- Diseño de aplicaciones

- Almacenamiento y comunicación de datos

Las secciones a su vez tienen sub-secciones, las mismas que serán analizadas de acuerdo a los resultados obtenidos.

Implementación y uso

Al implementar aplicaciones críticas para una empresa, hay que asegurar la seguridad y disponibilidad de esas aplicaciones y de los servidores. El mantenimiento continuo es imprescindible para ayudarle a asegurarse que los errores de seguridad se corrigen, y no se introducen nuevas vulnerabilidades en el entorno.

En esta sección se analiza únicamente las sub-secciones en donde se encontraron riesgos:

Tabla 13: Sub-sección implementación y uso

Aplicaciones	□
Implementación y uso	□
Equilibrio de carga	□
Clústeres	□
Aplicación y recuperación de datos	□
Fabricante de software independiente (ISV)	□
Desarrollado internamente	□
Vulnerabilidades	□

Elaborado por: Los Autores

Resultados:

Tabla 14: Resultados del análisis de implementación y uso de aplicaciones

Equilibrio de carga	No se utilizan equilibradores de carga en el entorno.

Clústeres:	No se utiliza la agrupación en clústeres en el entorno.
Aplicación y recuperación de datos	La empresa no realiza periódicamente pruebas de recuperación de aplicaciones y datos.
Fabricantes de software independientes (ISV)	En la empresa se utilizan aplicaciones que han sido desarrolladas por otros fabricantes. Los fabricantes independientes de software no ofrecen servicios de mantenimiento ni actualizaciones de seguridad.
Desarrollado internamente	Dentro de la empresa no se utiliza macros personalizadas en las aplicaciones ofimáticas.
Vulnerabilidades	No existen procedimientos que aborden los aspectos de las vulnerabilidades de la seguridad conocidos.

Elaborado por: Los Autores

En la empresa no se utiliza equilibradores de carga en el entorno, esto puede afectar la disponibilidad de los servicios especialmente el de correo que es de gran importancia para los procesos de negocio de RECTIGAMOS S.A.

No se utiliza agrupación en clústeres, lo que representa un riesgo al no asegurar una disponibilidad alta sobre todo de la base de datos que es en donde se guardan tanto los datos de clientes y proveedores como los datos de la gestión financiera.

No se realiza pruebas periódicas de recuperación de aplicaciones y datos, esto puede afectar al tiempo de respuesta ante incidentes que necesiten actividades y procedimientos de recuperación.

Se maneja aplicaciones que han sido desarrolladas por terceros, y los mismos no ofrecen un servicio de mantenimiento, ni tampoco de actualizaciones de seguridad, esto representa un riesgo para la información de la empresa ya que si el personal de TI de la organización no conoce las configuraciones necesarias, no garantiza un nivel de seguridad alto.

En la empresa se utiliza macros personalizadas en las aplicaciones ofimáticas y debido a ello las configuraciones de seguridad de office se reclasifican a un nivel inferior, por lo que las aplicaciones ofimáticas quedan expuestas a documentos peligrosos.

Existen vulnerabilidades de seguridad que son conocidas por el personal de TI de RECTIGAMOS S.A., pero no existe un procedimiento formal para hacer frente a dichas vulnerabilidades y esto representa un riesgo potencial.

Diseño de aplicaciones

Un diseño que no aborda adecuadamente los mecanismos de seguridad como la autenticación, autorización, y validación de datos podría permitir que los atacantes aprovechen las vulnerabilidades de seguridad para acceder a información confidencial.

En la presente sección se analiza únicamente las sub-secciones en donde se encontraron riesgos:

Tabla 15: Diseño de aplicaciones

Diseño de aplicaciones	
Autenticación	
Directivas de contraseñas	
Autorización y control de acceso	
Registro	
Validación de datos de entrada	
Metodologías de desarrollo de seguridad de software	

Elaborado por: Los Autores

Resultados:

Tabla 16: Resultado del análisis del diseño de aplicaciones

Validación de datos de entrada	No se utiliza mecanismos para validar los datos de entrada en las aplicaciones del cliente. No se valida los datos de entrada que proceden de un feed de datos.
Metodologías de desarrollo de seguridad de software	La empresa no proporciona formación sobre metodologías de seguridad de software para su personal de desarrollo. La empresa no utiliza herramientas de pruebas de software de seguridad como parte del proceso de desarrollo de seguridad.

Elaborado por: Los Autores

No se realiza una comprobación para verificar que los datos de entrada tengan una sintaxis y semántica correctas, sin embargo esto no representa una vulnerabilidad mayor.

La empresa no se dedica al desarrollo de software por lo tanto se omitirá esta subsección correspondiente a metodologías de desarrollo de seguridad de software.

Almacenamiento y comunicación de datos

Este apartado trata sobre la integridad y confidencialidad de los datos, puesto que la pérdida o el robo de los mismos pueden afectar negativamente a la reputación y economía de la empresa. En este contexto es importante comprender como las aplicaciones controlan y protegen los datos críticos.

A continuación se analiza únicamente las sub-secciones en donde se encontraron riesgos:

Tabla 17: Almacenamiento y comunicación de datos

Almacenamiento y comunicaciones de datos	
Cifrado	
Cifrado - Algoritmo	

Elaborado por: Los Autores

La empresa RECTIGAMOS S.A. a través de sus aplicaciones principales cifra los datos confidenciales cuando están almacenados y antes de ser transmitidos, y para esto utiliza el algoritmo de cifrado DES. El mismo se considera inseguro porque el tamaño de clave de 56 bits es corto, y según resultados analíticos las claves de DES se han roto en menos de 24 horas.

Análisis general del área aplicaciones

Para el Área de Aplicaciones, se analiza las secciones de Implementación y Uso, Diseño de Aplicaciones y Almacenamiento y Comunicación de Datos, todas las subsecciones que según MSAT presentan carencias severas de seguridad. En el siguiente apartado se muestra un resumen de los problemas que se consideran más graves dentro de esta área:

No se asegura una alta disponibilidad de los servicios ofrecidos por RECTIGAMOS S.A. como por ejemplo, el servicio de correo electrónico o el servicio de almacenamiento de datos, ya que no se utiliza ni equilibradores de carga ni agrupación de clústeres.

RECTIGAMOS S.A. utiliza aplicaciones que han sido desarrolladas por otros fabricantes, que no ofrecen servicios de mantenimiento ni actualizaciones de seguridad.

RECTIGAMOS S.A. ha implementado políticas para la gestión y utilización de aplicaciones dentro de la empresa, sin embargo existen muchos problemas que tienen que ver con las vulnerabilidades presentes en sus aplicaciones y con el cifrado de datos, ya que a pesar de que se utiliza un algoritmo para encriptar la información confidencial, el algoritmo de cifrado utilizado es inseguro y lo más recomendable es utilizar un algoritmo que dificulte la intrusión de terceros.

Por los motivos expuestos MSAT marca a esta área con un estado de alerta de color rojo, es decir que presenta carencias severas de seguridad.

4.3.1.3. Operaciones

El área de operaciones cuenta con las siguientes secciones:

- Entorno
- Directiva de seguridad
- Gestión de actualizaciones y revisión
- Copias de seguridad y recuperación.

Las secciones a su vez tienen sub-secciones, las mismas que son analizadas de acuerdo a los resultados obtenidos.

Entorno

La seguridad de RECTIGAMOS S.A. depende de los procedimientos operativos, los procesos y las pautas que se aplican en el entorno. Para aumentar la seguridad es necesaria una documentación clara y exacta del entorno y de las pautas.

En esta sección se analiza únicamente las sub-secciones en donde se detectó riesgos:

Tabla 18: Entorno de Operaciones

Operaciones	
Entorno	
Host de gestión	
Host de gestión-Servidores	
Host de gestión - Dispositivos de red	

Elaborado por: Los Autores

Resultados:

Host de gestión-servidores.

No existe ningún equipo de gestión dedicado a los servidores.

En RECTIGAMOS S.A. no existe ningún equipo de gestión dedicado a los servidores, lo que representa una vulnerabilidad ya que es necesario contar con una estación de gestión de servidores para comprobar que los servicios que ofrecen están disponibles y seguros.

Directiva de seguridad

La política de seguridad corporativa hace referencia a las directivas y a pautas individuales para regular el uso adecuado y seguro de las tecnologías y los procesos de la empresa. Esta área incluye las directivas para todos los aspectos de la seguridad, como los usuarios, los sistemas, y los datos.

Dentro de esta sección se analiza únicamente las sub-secciones en donde se encontró riesgos:

Tabla 19: Directivas de seguridad

Directiva de seguridad	
Clasificación de datos	
Eliminación de datos	
Protocolos y servicios	
Uso aceptable	
Gestión de cuentas de usuarios	
Regulación	
Directiva de seguridad	

Elaborado por: Los Autores

Resultados:

Tabla 20: Resultado del análisis de la directiva de seguridad

Clasificación de datos.	La organización no dispone de un esquema de clasificación de datos o instrucciones de protección de datos basadas en ese esquema.
Eliminación de datos.	Las aplicaciones principales del entorno no cifran los datos confidenciales cuando están almacenados.

Elaborado por: Los Autores

RECTIGAMOS S.A. no dispone de un esquema de clasificación de datos, esta vulnerabilidad puede consentir que personal no autorizado tenga acceso a información confidencial de la empresa y puede suponer la pérdida de la imagen de RECTIGAMOS S.A., debido a la divulgación no autorizada de información sensible para la empresa. Si el personal no sabe qué información de la empresa es confidencial, y cómo se protegen estos datos, existe una alta probabilidad de que esta información quede expuesta a personas no autorizadas.

RECTIGAMOS S.A. no cuenta con procedimientos para la gestión y la eliminación de información en formato impreso y electrónico, debido a esto la confidencialidad de la información se puede ver afectada.

Gestión de actualizaciones y revisiones

RECTIGAMOS S.A. debe gestionar de manera adecuada las actualizaciones y revisiones porque representa un factor importante para la seguridad del entorno informático.

La aplicación oportuna de actualizaciones y revisiones es necesaria para contribuir a la protección del entorno contra las vulnerabilidades conocidas y aquellas que podrían ser un frente de ataque.

En esta sección se analiza únicamente las sub-secciones en donde se encontró riesgos:

Tabla 21: Gestión de actualizaciones y revisiones

Gestión de actualizaciones y revisiones	
Documentación de la red	
Flujo de datos de la aplicación	
Gestión de actualizaciones	
Gestión de cambios y configuración	

Elaborado por: Los Autores

Resultados:

Tabla 22: Resultados del análisis en la gestión de actualizaciones y revisiones

Flujo de datos de la aplicación.	No existen diagramas de la arquitectura ni del flujo de datos de las aplicaciones principales.

Gestión de actualizaciones.	No existen directivas que regulen la gestión de actualizaciones ni revisiones de los sistemas operativos y de las aplicaciones.
Gestión de cambios y configuración.	La empresa no dispone de ningún proceso de gestión de cambios ni configuraciones.

Elaborado por: Los Autores

RECTIGAMOS S.A. no cuenta con diagramas lógicos de red, esto representa una vulnerabilidad ya que sin un diagrama de la red no se podrán realizar actividades de corrección sobre la misma.

No existen directivas que controlen la gestión de actualizaciones ni revisiones de los sistemas operativos, y de las aplicaciones que maneja RECTIGAMOS S.A., lo que representa un riesgo ya que si no se aplican actualizaciones de seguridad y cambios de configuración en intervalos periódicos pueden surgir muchos problemas que afecten a los procesos de negocio de la empresa.

RECTIGAMOS S.A. no cuenta con procesos ni procedimientos formales para la correcta gestión de cambios y configuraciones de hardware y/o software, esto supone una vulnerabilidad ya que por ejemplo, antes de realizar cualquier cambio o configuración debe realizarse pruebas de verificación de compatibilidad antes de ponerlo en producción.

Copias de seguridad y recuperación.

En este apartado se trata sobre la planificación de recuperación ante desastres y reanudación de los procesos de negocio. La aplicación oportuna de procesos de recuperación utilizando copias de seguridad, contribuye a la empresa a continuar con sus actividades y evitar en lo posible las pérdidas económicas y de reputación.

En la presente sección se analiza únicamente las sub-secciones en donde se encontró riesgos:

Tabla 23: Copias de Seguridad y recuperación

Copias de seguridad y recuperación	
Archivos de registro	
Planificación de recuperación ante desastres y reanudación de negocio	
Copias de seguridad	
Dispositivos de copia de seguridad	
Copias de seguridad y restauración	

Elaborado por: Los Autores

Resultados:

Tabla 24: Resultados del análisis en las copias de seguridad y recuperación

Planificación de recuperación ante desastres y reanudación de negocio.	La empresa no tiene procedimientos definidos para la recuperación ante desastres y reanudación de negocio. Los registros del entorno no se repasan periódicamente.

Elaborado por: Los Autores

RECTIGAMOS S.A. no cuenta con políticas para la recuperación ante desastres y reanudación de los procesos de negocio, tampoco se realizan pruebas periódicas para asegurar la recuperación en un periodo de tiempo aceptable ante incidentes graves.

El personal de la empresa no revisa los registros en busca de actividades sospechosas, tampoco cuenta con procedimientos formales para realizar dicha actividad.

Análisis General Área Operaciones

Para el Área de Operaciones, se analiza las secciones de Entorno, Directiva de Seguridad y Gestión de actualizaciones y revisiones, todas las sub-secciones que según MSAT presentan carencias severas de seguridad. En el siguiente apartado se presenta un resumen de los problemas que se consideran graves dentro de esta área: RECTIGAMOS S.A. ha implementado políticas para la gestión y utilización de la tecnología dentro de la empresa, sin embargo existen muchos problemas que tienen que ver con la seguridad de los datos, la gestión de actualizaciones, recuperación ante desastres y con la falta de diagramas en los cuales los miembros de TI puedan basarse para dar solución a muchos incidentes presentes a diario.

Por los motivos expuestos MSAT marca a esta área con un estado de alerta de color amarillo, es decir, que no cumple con las mejores prácticas recomendadas y necesita ser mejorada**.**

4.3.1.4. PERSONAL

El área de personal cuenta con las siguientes secciones:

- Requisitos y evaluaciones
- Directiva y procedimientos
- Formación y conocimiento

Las secciones a su vez tienen sub-secciones, las mismas que son analizadas de acuerdo a los resultados obtenidos.

Requisitos y evaluación

Todos los encargados de la toma de decisiones deben comprender los requisitos de seguridad, para que las decisiones comerciales y técnicas adoptadas aumenten la seguridad, en lugar de contradecirse entre sí.

En esta sección se analiza únicamente las sub-secciones en donde se encontró riesgos:

Tabla 25: Sección de Personal

Personal	
Requisitos y evaluaciones	
Directiva y procedimientos	
Formación y conocimiento	

Elaborado por: Los Autores

Resultados:

Tabla 26: Resultados del análisis en la sección de personal

Evaluaciones de seguridad	Las evaluaciones de la seguridad de su empresa las realiza personal interno.

Elaborado por: Los Autores

Las evaluaciones de seguridad deben ser aplicadas por personal interno y empresas independientes, lo que ayudará a mejorar la seguridad de los recursos de TI y de la información. Las evaluaciones periódicas realizadas por terceros independientes pueden ayudar a la empresa a revisar, evaluar e identificar las posibles mejoras. Estas evaluaciones también podrían resultar beneficiosas para cumplir las estipulaciones normativas, y los requisitos de los clientes, socios y fabricantes.

Directiva y Procedimientos.

Los procedimientos claros y prácticos en la gestión de las relaciones con los fabricantes y socios, pueden ayudarle a minimizar el nivel de riesgos al que se expone la empresa. Los procedimientos para contratar aspirantes y finalizar sus contratos, pueden proteger a la empresa contra empleados sin escrúpulos o descontentos.

Dentro de esta sección se analizaran únicamente las sub-secciones en donde se encontraron riesgos:

Tabla 27: Directivas y procedimientos

Directiva y procedimientos	
Comprobaciones del historial personal	
Directiva de recursos humanos	
Relaciones con terceros	

Elaborado por: Los Autores

Resultados:

Tabla 28: Resultados del análisis de la directiva y procedimientos

Directiva de recursos humanos	Existe una directiva formal para los empleados que dejan la empresa de forma hostil. No existe una directiva para los empleados que dejan la empresa de forma amistosa.

Elaborado por: Los Autores

Existe una directiva formal para los empleados que dejan la empresa de forma hostil. Los procedimientos formales para gestionar el caso de los empleados que dejan la empresa, garantizan que se actúa debidamente cuando se rescinde un contrato de trabajo.

Estos procedimientos deben existir para gestionar la situación de los empleados que dejan la empresa amistosamente, y para los que la dejan de forma hostil.

Formación y Conocimiento.

Este apartado trata sobre la divulgación de las medidas de seguridad con las que cuenta la empresa, así como también se enfoca en la capacitación en seguridad para

los miembros del personal, con el fin de enfrentar muchas vulnerabilidades que se dan a causa de la ignorancia con respecto a este tema.

En esta sección se analiza únicamente las sub-secciones en donde se encontró riesgos:

Tabla 29: Formación y conocimiento

Formación y conocimiento	
Conocimiento de seguridad	
Formación sobre seguridad	

Elaborado por: Los Autores

Resultados:

Tabla 30: Resultados del análisis de la formación y conocimiento

Conocimiento de seguridad	No existe ningún programa de divulgación de las medidas de seguridad en la empresa.
Formación sobre seguridad	La empresa no ofrece actualmente a los empleados formación específica por temas.

Elaborado por: Los Autores

No existe ningún programa de divulgación de las medidas de seguridad en la empresa. La empresa debe seleccionar un medio accesible para todo el personal, para comunicarles las medidas de seguridad que se adoptan en la institución, de tal manera que el personal conozca los riesgos relacionados con los recursos de TI, y cumplan con las medidas dispuestas.

La empresa no ofrece actualmente a los empleados formación sobre seguridad.

Se debe seleccionar personal interno o contratar a una empresa externa para que capacite al personal de la empresa en temas de seguridad de TI. La

capacitación permitirá al personal de TI, mejorar sus conocimientos, habilidades, y estar al día con las nuevas tecnologías, para responder a los incidentes que se presentan de una manera más rápida y eficaz.

Análisis General Área Personal

Para el área de Personal, se analizó las secciones de Requisitos y Evaluación y Directiva y Procedimientos, todas las sub-secciones que según MSAT presentan carencias severas de seguridad. En el siguiente apartado se presenta un resumen de los problemas que se consideran más urgentes de resolver para esta área:

Nunca se ha realizado anteriormente una evaluación de seguridad dentro de la empresa, ni por personal interno, ni por empresas independientes, por tal motivo se necesita establecer políticas de cómo y con qué frecuencia realizar estas evaluaciones, lo que ayuda a la empresa a mejorar la seguridad de los recursos de TI y de la información. Existe una directiva formal para los empleados que dejan la empresa de forma hostil. Se necesita establecer procedimientos para gestionar la situación de los empleados que dejan la empresa amistosamente, y los que la dejan de forma hostil.

No existe ningún programa de divulgación de las medidas de seguridad en la empresa, y no se ofrece actualmente a los empleados formación relacionada con seguridad de TI.

Por los motivos expuestos MSAT marca a esta área con un estado de alerta de color amarillo, es decir, que no cumple con las mejores prácticas recomendadas y necesita ser mejorada.

4.3.2. Análisis general de la evaluación realizada con MSAT

En principio, una puntuación baja del BRP y alta del DiDI parecería un buen resultado, pero no siempre es así. Una disparidad significativa entre la puntuación del BRP y la del DiDI para un área de análisis específica significa que se recomienda una revisión del área, y en nuestros resultados las 4 áreas presentan un desbalance significativo. Un entorno estable probablemente tendría como resultado puntuaciones iguales en todas las áreas.

Además las 4 áreas presentan disparidades entre las puntuaciones DiDI, lo cual es un indicio de una estrategia general de seguridad concentrada en una sola técnica de mitigación. Si la estrategia de seguridad no abarca el personal, los procesos ni la tecnología, el entorno estará expuesto a un mayor riesgo de ataque.

Las 4 áreas de seguridad que analiza MSAT presentan carencias severas en la distribución de la defensa del riesgo, mientras que en cuanto a la madurez de la seguridad, el área personal necesita mejorar.

El área que presenta mayores problemas de seguridad, es el área de aplicaciones que presenta carencias severas de seguridad, mientras las áreas de Infraestructura, Personal y Operaciones, presentan menos problemas pero de todas maneras no cumplen con las mejores prácticas y se necesita mejorar.

Dentro del área de infraestructura, las 3 sub-secciones tienen que mejorar sus prácticas de seguridad, y las sub-secciones que presentan carencias más severas son las de acceso remoto, inalámbrico, segmentación, directivas de contraseñas y creación segura.

El área de aplicaciones es la que presenta mayores carencias de seguridad principalmente en la sección de implementación y uso. El principal problema dentro de esta área es que la empresa utiliza aplicaciones que han sido desarrolladas por otros fabricantes, que no ofrecen servicios de mantenimiento ni actualizaciones de seguridad, por lo que se encuentra muy expuesta en caso de que dicha aplicación presente problemas.

En el área de operaciones la sección de actualizaciones y revisiones es la que presenta carencias severas de seguridad, principalmente porque no existen diagramas de la arquitectura ni del flujo de datos de las aplicaciones principales, y no existen directivas que regulen la gestión de actualizaciones ni revisiones de los sistemas operativos y de las aplicaciones.

El área de personal presenta carencias severas en las sub-secciones de formación sobre seguridad y evaluaciones de seguridad, ya que en la actualidad no se ofrece a los empleados capacitación en temas relacionados con seguridad de la información, y nunca se ha realizado una evaluación de seguridad dentro de la empresa.

En la tabla 31 se muestran las sub-secciones que presentan mayores problemas, y el nivel de prioridad en el que deben ser resueltas según MSAT.

Tabla 31: Nivel de prioridad para resolución de problemas según MSAT

Prioridad alta	Prioridad intermedia	Prioridad baja
· Creación segura · Planificación de recuperación ante desastres y reanudación de negocio · Acceso remoto · Segmentación · Fabricante de software independiente (ISV)	· Seguridad física · Cifrado · Conocimiento de seguridad · Usuarios administrativos · Validación de datos de entrada	· Host de gestión - Dispositivos de red · Uso aceptable · Copias de seguridad · Antivirus - Equipos de escritorio · Antivirus - Servidores

Elaborado por: Los Autores

4.4. Método OCTAVE-S

Este método surge de acuerdo a la necesidad de empresas más pequeñas alrededor de 100 personas o menos. Se basa en método OCTAVE pero está adaptado a los limitados medios y restricciones únicas de las pequeñas empresas; OCTAVE-S utiliza un proceso simplificado y más hojas de trabajo diferentes, pero produce el mismo tipo de resultados.

Las dos principales diferencias en la versión de OCTAVE-S son:

1. Requiere un pequeño equipo de 3-5 personas que entienden la amplitud y profundidad de la empresa. Esta versión no comienza con el conocimiento formal sino con la obtención de talleres para recopilar información sobre los elementos importantes, los requisitos de seguridad, las amenazas y las prácticas de seguridad.

2. Incluye sólo una exploración limitada de la infraestructura informática. Las pequeñas empresas con frecuencia externalizan sus procesos de TI por completo y no tienen la capacidad de ejecutar o interpretar los resultados de las herramientas de vulnerabilidad.

El principal problema al que se está expuesto al hacer una evaluación de este tipo es que no se identifiquen oportunamente riesgos importantes, a los que eventualmente las organizaciones son vulnerables, por ello metodologías como OCTAVE-S minimizan este problema. Es importante que en el análisis se resalte lo valiosa que es la información, debido a que gran parte de los riesgos provienen de "costumbres" internas de las organizaciones.

Por último, cabe mencionar que una evaluación de riesgos es muy particular para cada organización y que no sería lo más adecuado desarrollar evaluaciones a partir de resultados obtenidos de otras organizaciones.

4.4.1. Proceso de OCTAVE –S

El proceso de OCTAVE -S consta fundamentalmente de dos partes:

1. Identificar el perfil de riesgo, es decir, las amenazas y vulnerabilidades que afectan directamente a los activos críticos, desde el punto de vista organizacional y tecnológico.

2. Análisis del riesgo encontrado como resultado del proceso descrito anteriormente, para desarrollar las estrategias y el plan de mitigación.

El proceso empieza con una fase de preparación para constituir un equipo de análisis y comenzar con las entrevistas iniciales. Una vez establecido el equipo de análisis se llevan a cabo varias actividades para identificar el perfil de riesgos de los activos críticos, desde un punto de vista organizacional (Fase 1) y tecnológico (Fase 2).

Continuando con el proceso de OCTAVE -S el equipo de análisis desarrolla las estrategias y planes de mitigación (Fase 3) basándose en el análisis de riesgo, producto del proceso anterior.

4.4.2. Fases de OCTAVE –S

Como se menciona anteriormente, la metodología OCTAVE -S consta de tres fases, pero previamente cuenta con un fase de preparación. Estas fases se describen con detalle a continuación.

Fase de Preparación

En esta fase de OCTAVE -S se conforma el equipo de análisis, el mismo que está constituido de 3 a 5 personas, este grupo debe tener miembros pertenecientes a la organización que es objeto de evaluación, aunque puede existir colaboración de personal externo. Lo recomendable es que el equipo sea multidisciplinario para que los miembros del equipo enriquezcan su perspectiva.

Fase uno: Construir perfiles de amenaza basados en activos

La fase uno es una evaluación con una visión organizacional. En esta fase, el equipo de análisis determina los criterios de evaluación de impacto que posteriormente serán utilizados para evaluar los riesgos. También se deben

identificar los activos de información de mayor importancia y evaluar las prácticas de control y seguridad que actualmente tiene la organización. El equipo de análisis recolecta toda la información necesaria y completa todas las tareas.

Posteriormente se selecciona de tres a cinco activos de información críticos, basados en la importancia que estos representan para la organización y los cuales serán analizados con una mayor profundidad.

Finalmente, el equipo de análisis define tanto los requerimientos de seguridad como el perfil de amenaza para cada uno de los activos críticos.

Fase 1	Proceso	Actividad	Pasos
Fase 1: Construir perfiles de amenaza basados en activos	Proceso S1: Identificar la información organizacional	S1.1 Establecer los criterios de evaluación de impacto	1
		S1.2 Identificar activos organizacionales	2
		S1.3 Evaluar las prácticas de seguridad organizacionales	3,4
	Proceso S2: Crear perfiles de amenaza	S2.1 Seleccionar activos críticos	5,6,7,8,9
		S2.2 Identificar requerimientos de seguridad para los activos críticos	10,11
		S2.3 Identificar amenazas a los activos críticos	12,13,14,15,16

Figura 34: Procesos, actividades y pasos de la fase 1, Metodología Octave-S
Fuente: Octave- S ® Implementation Guide, Version 1.0, página 6.

Fase dos: Identificar vulnerabilidades de la infraestructura

La fase 2 es una evaluación con una visión tecnológica, en la cual el equipo de análisis conduce una revisión de alto nivel de la infraestructura computacional de la

organización relacionándola con la seguridad considerada por el personal encargado de dicha infraestructura. De esta manera, se evalúa cómo se considera la seguridad de la infraestructura computacional por parte de la organización, es decir, analizar la forma en la que se utiliza la infraestructura, así como conocer quienes acceden a los activos críticos y quiénes son los responsables de configurar y mantener la infraestructura.

El equipo de análisis examina la medida en que cada parte responsable incluye seguridad en sus prácticas y procesos de TI.

Fase	Proceso	Actividad	Pasos
Fase 2: Identificar Vulnerabilidades de la Infraestructura	Proceso S3: Examinar la Infraestructura Computacional en relación con los activos críticos	S3.1 Examinar rutas de acceso	17,18
		S3.2 Analizar procesos relacionados con la tecnología	19,20,21

Figura 35: Procesos, actividades y pasos de la fase 2, Metodología Octave-S
Fuente: Octave- S ® Implementation Guide, Version 1.0, página 6.

Fase tres: Desarrollo de Planes y Estrategias de seguridad

Durante la fase 3, el equipo de análisis identifica los riesgos a los que están expuestos los activos críticos de la organización y decide qué hacer con ellos.

Basado en un análisis de la información recogida, el equipo crea una estrategia de protección para la organización y planes de mitigación para enfrentar los riesgos a los que están expuestos los activos críticos.

Las hojas de trabajo de la metodología OCTAVE -S utilizadas durante esta fase son altamente estructuradas y están enlazadas al catálogo de prácticas de OCTAVE, lo que permite al equipo relacionar sus recomendaciones para el mejoramiento a una referencia aceptada de prácticas de seguridad.

Fase	Proceso	Actividad	Pasos
Fase 3: Desarrollo de estrategias y planes de Seguridad	Proceso S4: Identificar y analizar los riesgos	S4.1 Evaluar el impacto de las amenazas	22
		S4.2 Establecer criterios de evaluación probabilística	23
		S4.3 Evaluar probabilidades de amenazas	24
	Proceso S5: Desarrollar estrategias de protección y planes de mitigación	S5.1 Describir las estrategias de protección actuales	25
		S5.2 Seleccionar aproximaciones de mitigación	26,27
		S5.3 Desarrollar planes de mitigación de riesgos	28
		S5.4 Identificar cambios en las estrategias de protección	29
		S5.5 Identificar los siguientes pasos	30

Figura 36: Procesos, actividades y pasos de la fase 3, Metodología Octave-S
Fuente: Octave- S ® Implementation Guide, Version 1.0, página 6.

4.4.3. Resultados de OCTAVE –S

La gestión de riesgos asociados a las tecnologías de la información requiere de un equilibrio entre las actividades reactivas y proactivas. Durante un proceso de evaluación con OCTAVE–S el equipo de análisis toma en cuenta la seguridad desde diferentes puntos de vista, garantizando que las recomendaciones sean apropiadas, basadas en las necesidades de la empresa.

Cuando se formulan actividades de mitigación para mejorar las prácticas de seguridad de la empresa, el equipo de análisis asume un punto de vista proactivo,

analizando los problemas de una forma global y de una forma específica de cada activo.

El equipo de análisis puede tomar una posición reactiva en cualquier momento durante la evaluación, para identificar elementos de acción destinados a corregir debilidades específicas. Dichos puntos de acción se consideran de carácter reactivo porque llenan un vacío inmediato en lugar de mejorar las prácticas de seguridad de la empresa.

A continuación se listan los principales resultados de la metodología OCTAVE-S.

Una estrategia de protección para toda la organización – La estrategia de protección delinea la dirección de la organización con respecto a sus prácticas de seguridad de la información.

Planes de mitigación de riesgo – Estos planes están pensados para mitigar los riesgos de los activos críticos a través de la mejora de las prácticas de seguridad seleccionadas.

Lista de acción – Estas incluyen elementos de acción de corto plazo necesarios para contrarrestar debilidades específicas.

Otros resultados de OCTAVE –S incluyen:

- Un listado de activos de información importantes que apoyan los objetivos organizacionales y los objetivos de negocio.
- Una perspectiva de los resultados mostrando la capacidad para la cual la organización está siguiendo buenas prácticas de seguridad.
- Un perfil de riesgo para cada activo crítico detallando un rango de riesgos para dicho activo.

Cada fase de la metodología OCTAVE –S produce resultados provechosos, incluso realizando una evaluación parcial, se obtendrá como resultado información útil para mejorar la postura de la seguridad de la empresa.

Conformación del equipo de trabajo

Para conducir correctamente la metodología OCTAVE-S, es necesario definir un equipo de trabajo interdisciplinario, el mismo que será responsable de llevar a cabo varias de las actividades a desarrollarse. Al tener un equipo interdisciplinario permitirá abarcar las principales áreas de la empresa como son el área de los altos directivos, el área operativa y el área de los usuarios finales. Con esto se tendrá una perspectiva más amplia de lo que requiere la empresa a nivel tecnológico y organizacional.

El equipo de análisis facilitará los talleres a desarrollarse dentro de los diferentes procesos de OCTAVE y analizará en cada uno de estos la información obtenida, alcanzando así el objetivo planteado con esta metodología. Las personas que conformen este equipo de análisis tendrán varios roles y responsabilidades, así como también deberán poseer varias habilidades.

Estos detalles se indican a continuación:

Roles y responsabilidades del equipo de análisis:

- Trabajar con los directivos en el alcance de la evaluación, selección de participantes y cuándo se llevarán a cabo cada una de las actividades pertenecientes a cada proceso de la metodología OCTAVE-S.
- Coordinar con los altos directivos, los directivos de áreas operativas y el soporte de TI las respectivas evaluaciones de vulnerabilidades.
- Recopilar, analizar y mantener datos y resultados durante los procesos de OCTAVE-S.
- Proveer de soporte logístico.

Selección de Altos Directivos

Los Altos Directivos que se van a seleccionar para la evaluación, deben tener la capacidad y conocimientos necesarios para identificar correctamente los activos de

información más importantes dentro de la empresa, las distintas amenazas para estos activos, los requerimientos de seguridad de cada activo, las estrategias de protección con las que cuenta la empresa y las vulnerabilidades organizacionales.

Perfil de Altos Directivos

- Estar familiarizado con los tipos de activos de información utilizados en la empresa.
- Ser capaz de destinar el tiempo requerido para las evaluaciones.
- Tener conocimiento de los procesos clave que maneja la empresa para la ejecución normal de sus actividades y tareas.
- Tener autoridad de seleccionar y autorizar el tiempo para los Directivos de áreas operativas.
- Haber estado en su cargo por lo menos dos años.

Selección de los Directivos de Áreas Operativas

Los Directivos de Áreas Operativas deben estar asociados con la operación, mantenimiento y desarrollo de la infraestructura computacional de la organización; son requeridos para identificar los activos de información que posee la empresa, las distintas amenazas para estos activos, los requerimientos de seguridad de cada activo, las estrategias de protección con las que cuenta la empresa y las vulnerabilidades organizacionales.

Perfil de los Directivos de Áreas Operativas

- Amplio conocimiento de los tipos de activos de información que utiliza la empresa.
- Conocer cómo los activos de información son utilizados.
- Conocimiento general de los activos críticos de la organización.
- Conocimiento de estándares de mitigación, medición y controles de riesgo asociados a TI.

- Tener en su cargo por lo menos dos años.

Selección del Personal en General

Se necesita personal que se encargue de identificar los procesos y activos de información que se consideren importantes para la organización, las distintas amenazas para estos activos, requerimientos de seguridad de cada activo, las estrategias de protección con las que cuenta la empresa y las vulnerabilidades organizacionales.

Perfil del Personal en General

- Conocer los tipos de activos de información usados en la organización y cómo son utilizados.
- Conocimiento respecto al tema de riesgo e impacto hacia los activos críticos de las tecnologías de información.
- Tener la autoridad de seleccionar y autorizar el tiempo necesario para el personal en general.
- Haber estado en su cargo por lo menos tres años.

Selección del Equipo de Trabajo para la empresa RECTIGAMOS S.A.

Una vez realizada la selección entre el personal más idóneo para que forme parte del equipo de trabajo que efectuará la evaluación en la organización, se han seleccionado a los siguientes profesionales:

Altos Directivos

Ing. Amada Mosquera - Gerente General

Directivos de Áreas Operativas

Sr. Nelson Luzuriaga – Encargado del Área de Tecnología

Ing. María Fernanda Cevallos - Asistente

Personal en General

Eco. Narcisa Jurado – Administradora Financiera

Beneficios del uso de la metodología para la empresa

- **Ventajas a nivel interno**

Mayor seguridad informática al conocer los controles que se pueden aplicar para los posibles riesgos a la que se encuentra expuesta la información de la empresa.

- **Ventajas a nivel externo**

La imagen positiva que puede ofrecer la empresa a sus clientes habituales o potenciales, de control, eficacia y seguridad de sus datos personales, reforzando el resto de actividades de la empresa frente a la competencia

Identificación de los Activos

Para la identificación de los activos OCTAVE-S proponer dividirlos en dos grupos

1.- Sistemas (Hardware, Software y Datos)
2.- Personas
Los mismos se clasificaron de la siguiente manera:

Sistemas: Bases de datos y archivos de datos, documentación del sistema, manuales de usuario, materiales de entrenamiento, procedimientos operativos de apoyo, planes de continuidad, equipos de comunicación y computación, medios magnéticos, otros equipos técnicos, documentos impresos, contratos, lineamientos,

documentos de la compañía, documentos que contienen resultados importantes del negocio.

Personas: Personal, clientes, otros servicios técnicos.

Tabla 32: Identificación de los Activos

CÓDIGO	ACTIVO	DESCRIPCIÓN	CLASE DE ACTIVO	PROPIETARIO	DEPARTAMENTO
Codificación con que se identificará el activo.	Nombre del activo.	Describir para que esta siendo usado el activo.	La clasificación indicada en la parte superior.	Nombre de la persona responsable del activo.	Nombre del departamento donde está ubicado el activo.

Elaborado por: Los Autores

Evaluación de riesgos con OCTAVE-S

En el siguiente apartado se desarrolla la fase preparatoria, fase 1, y fase 2 de la metodología.

Fase preparatoria: conformación del equipo de análisis

La Gerente General Ing. Amada Mosquera; ha mostrado mucho interés en el presente proyecto; pues el diagnóstico de vulnerabilidades informáticas para proponer un diseño del plan de seguridad de la información para la empresa RECTIGAMOS S.A. podría constituirse en un valioso aporte y apoyo para el plan informático de la organización. La participación del Gerente General, Encargado del área de tecnología y Asistente ha sido de vital importancia para poder poner en marcha la evaluación.

El equipo está conformado por los miembros descritos en la tabla

Tabla 33: Miembros del equipo de Análisis

MIEMBROS	FUNCIÓN EN LA EVALUACIÓN
Ing. Amada Mosquera	Gerente General y Administración

Ing. Francisco Salas	Encargado del área de Tecnología
Ing. María Fernanda Cevallos	Asistente
Srta. Karen Pintado Sr. Cesar Hurtado	Estudiantes de la Facultad de Ingeniería en Sistemas, quienes utilizan los resultados obtenidos de la metodología OCTAVE –S para el desarrollo del presente proyecto.

Elaborada por: Los Autores

Fase 1: Construir perfiles de amenaza basados en activos

En esta fase se desarrollan los procesos S1 y S2

Proceso S1: Identificar la información organizacional.

Este proceso se centra en desarrollar los criterios para evaluar el impacto de los riesgos a la empresa, identificando los activos y evaluando las prácticas de seguridad de la empresa.

La figura 37 muestra las actividades y los pasos que se desarrollan en el proceso S1.

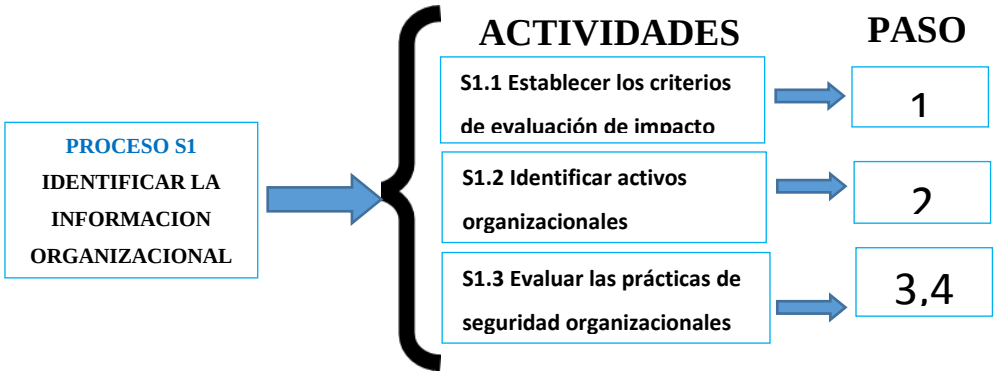


Figura 37: Actividades y pasos del proceso S1, Metodología Octave-S
Fuente: Octave- S ® Implementation Guide, Version 1.0, página 6.

Actividad S1.1: Establecer los criterios de evaluación de impacto.

En esta actividad se desarrolla el paso 1 que se describe a continuación:

Paso 1: Se define los rangos de potencial impacto (alto, medio, bajo) de las amenazas, a los activos de información de la empresa RECTIGAMOS S.A., en

las áreas propuestas por OCTAVE –S, las cuales son:

Confianza de los clientes, financiera, seguridad de las personas, multas o penalizaciones legales, productividad, y sistemas.

Confianza de los clientes: RECTIGAMOS S.A. goza de prestigio gracias al abanico de servicios que contempla todo el ciclo laboral y comercial de la empresa. Según RECTIGAMOS S.A. un porcentaje mayor al 15% de caída de reconocimiento frente a las empresas que utilizan su servicio, significaría un serio problema. Esta área es considerada de potencial medio impacto sobre la empresa RECTIGAMOS S.A.

Financiera: Esta área es de vital importancia para RECTIGAMOS S.A., ya que es la encargada de gestionar todos los ingresos y egresos de dinero; administrar los pagos de salarios, décimos, aportes al IEES, anticipos y préstamos a los empleados de la empresa; revisar las autorizaciones de emisiones de cheques; administrar las conciliaciones bancarias, y realizar los reportes de los estados de las cuentas de los clientes. Cualquier problema que se presente en esta área, por mínimo que sea, representaría un serio problema y se reflejaría en pérdidas económicas para la empresa. Esta área es considerada de potencial alto impacto sobre la empresa

Seguridad de las personas: En realidad en RECTIGAMOS S.A. no se realiza ninguna tarea que pueda poner en riesgo la salud de sus trabajadores o clientes, Por otra parte el ámbito de análisis del presente proyecto de tesis abarca únicamente la seguridad de la información dentro de la empresa, y no cubre directamente la seguridad de las personas. Es por ello que esta área se considera de bajo impacto.

Multas o penalizaciones legales: Las licencias de software no están cubiertas en su totalidad, aunque la empresa nunca ha recibido demandas de ningún tipo por parte de proveedores u otras empresas. Además la empresa cumple con todas las obligaciones que tiene con el estado, por lo tanto el potencial de impacto de esta área es de mediano impacto.

Productividad: El área de TI de la empresa trata de solucionar inmediatamente problemas de virus o fallas en el sistema, para que las actividades se

ejecuten con eficacia sin problemas que afecten el flujo del negocio.

El mantenimiento de los servidores, la red, los PCs, reinstalación de sistemas operativos, instalación y actualización de software o programas se lo realiza el último viernes del mes con el propósito de en lo menos posible obstaculizar las actividades de los empleados en el horario laboral.

Esta área se la considera de mediano impacto debido a que se puede presentar problemas que no se resuelvan inmediatamente y no afectarán las actividades normales del personal de la empresa.

Sistemas: Esta área es la encargada de administrar y gestionar todo lo que tiene que ver con TI (servidores, red, respaldos de información) brindando soporte técnico a toda la empresa. Una caída del servidor o de la red representaría un grave problema para el proceso de negocio, es por eso que esta área es considerada de potencial alto impacto.

Actividad S 1.2: Identificar activos de información de la empresa RECTIGAMOS S.A..

En esta actividad se desarrolla el paso 2 que se describe a continuación:

Paso 2: Se identifican los activos (sistemas, aplicaciones, información, personas) relacionados con la información de la empresa RECTIGAMOS S.A. para identificar dichos activos tomamos como punto de partida la experiencia y los conocimientos que tienen sobre la red tanto el Gerente General como el encargado del área de tecnología, que a su vez también forman parte del equipo de análisis.

A continuación se hace una breve descripción de los activos de información identificados:

Sistema Contable: Constituye el más importante de los activos de información tanto por la información que maneja como la importancia que el sistema representa para la empresa. Este sistema tiene 5 módulos que automatizan los procesos de negocio de RECTIGAMOS S.A., los mismos que son manejados por diferentes áreas

de acuerdo a la función que cumplan.

Servidor de Correo interno de RECTIGAMOS S.A.: Es un medio importante de comunicación para mantener contacto con clientes, proveedores y usuarios. Además se utiliza los correos como respaldos de confirmaciones y respuestas de diferentes eventos y actividades. Reside en el servidor Linux con S.O. CentOS 5.1, tiene un enlace en la página web la cual utiliza la aplicación Webmail o Roundcube Webmail. El personal administrativo de RECTIGAMOS S.A. dispone de una cuenta de correo. El manejo de las contraseñas de correo las gestiona el encargado del área de Tecnología.

Documentos legales: Estos documentos que entre otros son los siguientes: contratos, documentos personales de accionistas, pólizas, poderes de la empresa, tramites de los proveedores, temas legales (juicios), certificados, facturas, RUC, etc., son digitalizados y almacenados en la computadora del Gerente General y en un disco duro externo que tiene su asistente, y los archivos físicos son almacenados por el Administrador Financiero en su oficina.

Servidor de Base de datos: Aquí se guardan los datos que son procesados por el Sistema Contable, además almacena las fichas de los candidatos. El sistema gestor de base de datos que se utiliza es MySQL en su versión 5.3.

Servidor de Respaldo: En este servidor se guarda respaldos del servidor de base de datos. El proceso de respaldo se lo hace una vez cada cuatro meses.

Las computadoras personales, PCs: Funcionan como estaciones de trabajo, y son consideradas un activo importante de la compañía. Las estaciones de trabajo incluyen laptops y PCs, y están todas enlazadas a la red de la empresa. Muchos de estos activos almacenan información sensible para el negocio y significaría una perdida difícil de reponer en caso de que los equipos se dañen.

Intranet: Es el medio por el cual personal autorizado puede acceder a los servidores que tiene RECTIGAMOS S.A. en el exterior para poder brindar los servicios a sus clientes.

Página web: La página web de la empresa está alojada en un servidor externo y

es mantenida y actualizada por personal externo. La página contiene información acerca de los servicios que presta la empresa, y como contactarse con ellos.

Actividad S 1.3: Evaluar prácticas de seguridad organizacional.

En esta actividad se desarrollan los pasos 3 y 4 que se describen a continuación:

Paso 3: El paso 3 se divide en dos, el primero de ellos es el 3a en el cual se analiza hasta qué punto cada práctica de seguridad es utilizada en la empresa RECTIGAMOS S.A.

En el siguiente, que es el 3b, se registra lo que la organización está haciendo bien (prácticas de seguridad), y lo que no está haciendo bien (vulnerabilidades organizacionales) utilizando el estudio del paso 3a.

Las 15 prácticas de seguridad que considera OCTAVE –S, son las siguientes:

- Práctica de Seguridad 1: Concienciación y formación en seguridad.
- Práctica de Seguridad 2: Estrategia de Seguridad
- Práctica de Seguridad 3: Gestión de Seguridad
- Práctica de Seguridad 4: Políticas y Regulaciones de Seguridad
- Práctica de Seguridad 5: Gestión de la Seguridad Colaborativa
- Práctica de Seguridad 6: Planes de Contingencia/Recuperación de Desastres
- Práctica de Seguridad 7: Control de Acceso Físico.
- Práctica de Seguridad 8: Monitoreo y Auditoría de Seguridad Física.
- Práctica de Seguridad 9: Gestión de Sistemas y Redes
- Práctica de Seguridad 10: Monitoreo y Auditoría de Seguridad de TI
- Práctica de Seguridad 11: Autenticación y Autorización
- Práctica de Seguridad 12: Gestión de Vulnerabilidades
- Práctica de Seguridad 13: Encriptación
- Práctica de Seguridad 14: Diseño y Arquitectura de Seguridad
- Práctica de Seguridad 15: Gestión de Incidentes

Paso 4: Después de completar los Pasos 3a y 3b, se asigna un estado de semáforo

(verde, amarillo o rojo) para cada área de práctica de seguridad. El estado de semáforo debe reflejar lo bien que se cree que la empresa RECTIGAMOS S.A. está llevando a cabo en cada área. Se utilizaron las siguientes definiciones de semáforo como guía.

Verde: La empresa está llevando de manera correcta las prácticas de seguridad en esta área, no hay necesidad real de mejora.

Amarillo: La organización está llevando a cabo las prácticas de seguridad hasta cierto punto, hay espacio para la mejora.

Rojo: La organización no está llevando a cabo las prácticas de seguridad en ésta área, existe un amplio margen de mejora.

A continuación se detallan los pasos 3 y 4 de acuerdo con las 15 Áreas de Práctica de Seguridad de OCTAVE –S.

Práctica de Seguridad 1: Concienciación y formación en seguridad.

El personal de la empresa comprende sus roles y responsabilidades ya que a cada uno de ellos se les entregó un documento en donde están detalladas las políticas para el uso de los recursos informáticos, y adicionalmente todos los empleados deben confirmar que han recibido y comprendido las políticas, así como también expresar su acuerdo con el compromiso de cumplir las mismas. Gracias a esto el personal sigue buenas prácticas de seguridad como: No divulgar información sensible a terceros, tener capacidad suficiente para utilizar el hardware y software, y reportar incidentes. Sin embargo, el personal de la empresa no asiste a cursos externos de capacitación en seguridad de la información, y tampoco se brinda una capacitación interna, lo que representa una vulnerabilidad organizacional.

Por los motivos expuestos a esta área de práctica de seguridad se le ha asignado un estado de semáforo amarillo.

Práctica de Seguridad 2: Estrategia de Seguridad

Las estrategias de negocio de RECTIGAMOS S.A. toman en consideración las seguridades respectivas ya que la tecnología de la información es parte fundamental de los procesos de negocio de la empresa. Sin embrago no están documentadas todas las políticas ni las estrategias de negocio como tal, y las documentaciones no son revisadas ni actualizadas cada cierto tiempo.

Por los motivos expuestos a esta área de práctica de seguridad se le ha asignado un estado de semáforo amarillo.

Práctica de Seguridad 3: Gestión de Seguridad

Está área y práctica de seguridad es gestionada por el encargado del área de tecnología de RECTIGAMOS S.A., quien debe dar soluciones a los incidentes de seguridad que se presentan en cada una de las estaciones de trabajo. Sin embargo tanto la Gerente General como el Administrador no reciben informes por parte de sistemas de los problemas, ni de las soluciones que se les dieron a los incidentes de seguridad. También se debe mencionar que no existe un presupuesto real asignado periódicamente para la seguridad de la información de la empresa.

La realización del presente proyecto de tesis puede considerarse como un punto positivo dentro de ésta área de práctica de seguridad para RECTIGAMOS S.A., ya que al efectuar la evaluación con las herramientas MSAT y OCTAVE –S se mejorará la seguridad de la información y su gestión. También se debe acentuar dos puntos importantes, que la organización considera los problemas de seguridad que se pueden presentar en las actividades de contratación y despido del personal, y el segundo punto y no menos importante es que existe ética profesional entre sus miembros, esto representa una garantía para la gestión de la seguridad de la información en RECTIGAMOS S.A..

Por los motivos expuestos a esta área de práctica de seguridad se le ha asignado un estado de semáforo amarillo.

Práctica de Seguridad 4: Políticas y Regulaciones de Seguridad

La empresa RECTIGAMOS S.A. cuenta con un conjunto de políticas que se encuentran documentadas, sin embargo las mismas no son revisadas ni actualizadas periódicamente, la última revisión que se hizo en este documento fue en el año 2011.

No existen procedimientos establecidos para tratar los incidentes de seguridad de la información que se presentan, y tampoco existen procedimientos de documentación para los problemas y soluciones a dichos incidentes.

Por los motivos expuestos a esta área de práctica de seguridad se le ha asignado un estado de semáforo amarillo.

Práctica de Seguridad 5: Gestión de la Seguridad Colaborativa

La empresa cuenta con políticas y procedimientos para proteger la información cuando se trabaja con organizaciones externas, y tiene mecanismos formales para verificar que los terceros cumplan con sus requerimientos y necesidades. Las condiciones específicas de seguridad y los acuerdos a nivel de servicio están incluidos en los contratos.

El acceso remoto está restringido tanto para los contratistas como para terceros usuarios.

Por los motivos expuestos a esta área de práctica de seguridad se le ha asignado un estado de semáforo verde.

Práctica de Seguridad 6: Planes de Contingencia/Recuperación de Desastres

RECTIGAMOS S.A. cuenta con un plan de contingencia el mismo que incluye:

- Seguridad de la instalación.
- Disponibilidad de recursos de hardware y software en la instalación.

Se mantiene en la oficina de Guayaquil los siguientes recursos de software:

- Copia de los CD’s de instalación de Base de Datos
- Copia de CD de aplicativo Gestor.

El personal conoce y entiende el plan de contingencia y es capaz de llevar a cabo sus responsabilidades en caso de un eventual escenario de incidentes.

Por los motivos expuestos a esta área de práctica de seguridad se le ha asignado un estado de semáforo verde.

Práctica de Seguridad 7: Control de Acceso Físico.

Respecto a ésta área de práctica de seguridad, RECTIGAMOS S.A. ha implantado controles de seguridad física para proteger los activos de la empresa y se ha instalado un sistema de circuito cerrado de vigilancia para detectar e informar de intrusiones. Los equipos de red se encuentran en una habitación cerrada sin acceso restringido.

Como puntos negativos dentro de ésta área se tiene que los documentos confidenciales físicos se almacenan en la oficina del Administrador Financiero y no en un armario con llave como es recomendable. Además no existen políticas ni procedimientos implementados para la gestión de visitantes.

Por los motivos expuestos a esta área de práctica de seguridad se le ha asignado un estado de semáforo rojo.

Práctica de Seguridad 8: Monitoreo y Auditoría de Seguridad Física.

En RECTIGAMOS S.A. existe una gestión de inventarios de hardware y software que permite controlar los cambios en los equipos. Pero no cuenta con registros de monitoreo y auditoría de seguridad física.

Por los motivos expuestos a esta área de práctica de seguridad se le ha asignado un estado de semáforo amarillo.

Práctica de Seguridad 9: Gestión de Sistemas y Redes

Existen planes de seguridad documentados, pero no han sido probados, la presente tesis, es el primer intento para realizar una planificación de la seguridad de la información.

La empresa no cuenta con herramientas para gestionar la seguridad de los datos. Todos los equipos tienen antivirus y antispyware, instalado y configurado para que se actualice automáticamente, además los parches y actualizaciones necesarias están programados para que se instalen automáticamente, y en caso de que se necesiten nuevas actualizaciones estas son responsabilidad del departamento de Sistemas.

El Administrador Financiero, es el encargado de eliminar los usuarios que ya no pertenecen a la empresa, y crear nuevos usuarios con los permisos de acuerdo a las funciones que debe cumplir el nuevo empleado dentro de la empresa.

El Encargado del área de Tecnología, restringe todos los puertos de internet, para que los usuarios solo puedan acceder a páginas que necesiten para cumplir con sus tareas.

Por los motivos expuestos a esta área de práctica de seguridad se le ha asignado un estado de semáforo amarillo.

Práctica de Seguridad 10: Monitoreo y Auditoría de Seguridad de TI

En la empresa no se tienen herramientas para llevar a cabo procedimientos de monitoreo y auditorias del sistema o la red. Además no existe una gestión planificada para estos procedimientos. No hay políticas establecidas ni documentadas, de monitoreo y auditoria de la información y nunca se ha realizado una auditoria informática en la red de datos de RECTIGAMOS S.A.

Existen políticas documentadas para la gestión de la seguridad de la información dentro de la empresa, pero no se hace un seguimiento de la aplicación y la validez de las mismas. Por los motivos expuestos a esta área de práctica de seguridad se le ha asignado un estado de semáforo amarillo.

Práctica de Seguridad 11: Autenticación y Autorización

Tanto para utilizar una pc como para ingresar al sistema gestor se les asigna un usuario, con privilegios de acuerdo a las funciones del empleado dentro de la empresa, de este modo se asegura que el personal no tenga acceso a información confidencial que no le corresponde.

El área de tecnología es la encargada de eliminar las cuentas del personal que ya no trabaja para la empresa, sin embargo no hay un seguimiento en registros o documentos que demuestren que efectivamente se ha realizado la tarea asignada.

Por los motivos expuestos a esta área de práctica de seguridad se le ha asignado un estado de semáforo amarillo.

Práctica de Seguridad 12: Gestión de Vulnerabilidades

No se manejan herramientas para determinar y eliminar vulnerabilidades en el sistema. No se tienen políticas, ni procedimientos establecidos para hacer un análisis de vulnerabilidades del sistema.

Por los motivos expuestos a esta área de práctica de seguridad se le ha asignado un estado de semáforo rojo.

Práctica de Seguridad 13: Encriptación

La empresa RECTIGAMOS S.A. a través de sus aplicaciones principales cifra los datos confidenciales cuando están almacenados y antes de ser transmitidos, y para ello utiliza el algoritmo de cifrado DES. Este algoritmo se considera inseguro porque el tamaño de clave de 56 bits es corto y según resultados analíticos las claves de DES se han roto en menos de 24 horas.

Por los motivos expuestos a esta área de práctica de seguridad se le ha asignado un estado de semáforo amarillo.

Práctica de Seguridad 14: Diseño y Arquitectura de Seguridad

La empresa no tiene documentados procedimientos formales sobre la arquitectura y diseño especifico de seguridad de la información. Además no se tiene documentado el diseño general de la red, ni el diseño del sistema de seguridad de la información.

Por los motivos expuestos a esta área de práctica de seguridad se le ha asignado un estado de semáforo rojo.

Práctica de Seguridad 15: Gestión de Incidentes

Se tiene un conjunto básico de procedimientos documentados de cómo proceder en caso de Incidentes. Se tienen la mayor parte de licencias de equipos de hardware y software que posee la empresa. Existen instrucciones básicas documentadas de cómo gestionar los respaldos, y recuperación de datos.

Por los motivos expuestos a esta área de práctica de seguridad se le ha asignado un estado de semáforo amarillo.

Proceso S2: Crear perfiles de amenaza.

Este proceso se centra en seleccionar los activos críticos de entre los activos identificados previamente. Posteriormente se identifican los requerimientos de seguridad para esos activos, y se determina las amenazas presentes en contra de ellos.

La figura 38 muestra las actividades y los pasos que se desarrollan en el proceso S2.

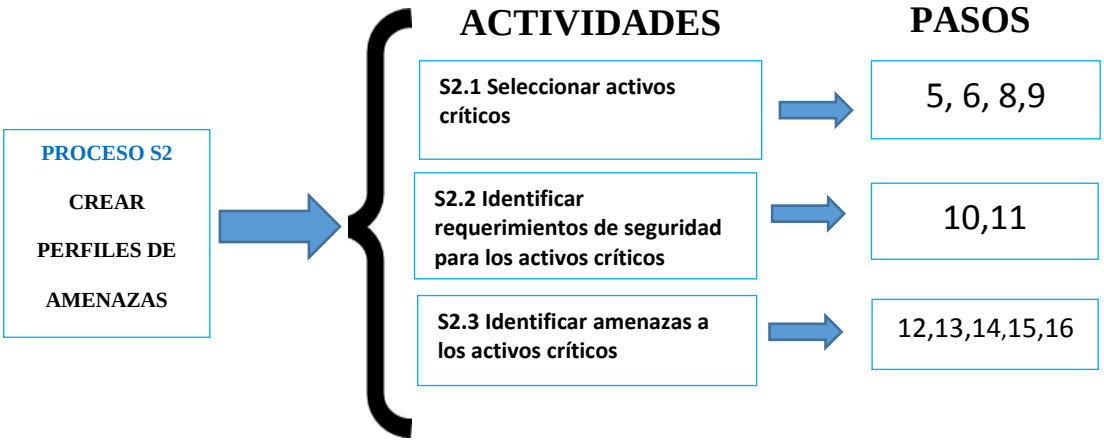


Figura 38: Actividades y pasos del proceso S2, Metodología Octave-S
Fuente: Octave- S ® Implementation Guide, Version 1.0, página 6.

En esta actividad se desarrollan los pasos 5, 6, 7, 8 y 9 que se describen a continuación:

Paso 5: Se selecciona de 3 a 5 activos considerados críticos de entre los activos de información identificados en el paso 2, basados en su importancia para la empresa.

Paso 6: Se identifica el activo crítico por su nombre.

Paso 7: Se especifica la razón por qué el activo crítico se le considera como tal.

Paso 8: Se registra quién usa y quién es responsable del activo crítico.

Paso 9: Se registra cuáles otros activos están relacionados con el activo crítico.

A continuación se muestran los resultados de los pasos anteriormente descritos:

Activos Críticos

Sistema Contable: El Sistema Gestor permite la funcionalidad y operatividad de las distintas áreas: Contabilidad, Facturación, Importaciones, etc., dentro de RECTIGAMOS S.A., y permite la obtención de información necesaria para la Gestión Empresarial y la toma de decisiones. Lo utilizan principalmente los usuarios del área financiera, y ventas.

Tanto por la información que maneja como por la importancia que el

sistema representa para la empresa al Sistema Gestor se lo considera un activo crítico para RECTIGAMOS S.A.

Servidor de Correo interno de RECTIGAMOS S.A.: Es un medio importante de comunicación tanto para mantener contacto con los clientes, proveedores y usuarios, como para utilizarlo como respaldo de confirmaciones y respuestas. El personal administrativo de RECTIGAMOS S.A. dispone de una cuenta de correo. El manejo de las contraseñas de correo las gestiona el área de tecnología. Por los motivos expuestos este activo de información es considerado crítico para RECTIGAMOS S.A.

Las computadoras personales, PCS: Son la principal herramienta para el desarrollo de las actividades de los empleados de RECTIGAMOS S.A., muchos de estos activos almacenan información sensible para el negocio. Las estaciones de trabajo incluyen laptops y PCs, están todas enlazadas a la red de la empresa y significaría una perdida difícil de reponer en caso de que los equipos se dañen o roben. Por los motivos expuestos este activo de información es considerado crítico para RECTIGAMOS S.A.

Actividad S2.2: Identificar los requerimientos de seguridad para los activos críticos.

En esta actividad se desarrolla los pasos 10 y 11 que se describen a continuación:

Paso 10: Se identifican los requerimientos de seguridad para cada activo crítico de RECTIGAMOS S.A.

Los requerimientos de seguridad que propone OCTAVE –S son los siguientes:

- Confidencialidad.- Propiedad de la información, que garantiza que cierta información, está accesible únicamente a personal autorizado.
- Integridad.- Propiedad de la información, que garantiza que cierta información, puede ser modificada, únicamente por personal autorizado.
- Disponibilidad.- El factor de disponibilidad es una medida que indica, cuánto tiempo está en funcionamiento un sistema o equipo, respecto de la duración total que se hubiese deseado que funcionase.

- Otros.

Paso 11: Se identifican los requerimientos más importantes de seguridad para cada activo crítico de RECTIGAMOS S.A.

A continuación se presenta los resultados:

Se estableció que los requerimientos de seguridad más importantes para los activos críticos sistema gestor y servidor de correo son la integridad y la confidencialidad. La información que se maneja en dichos activos son de vital importancia para la empresa ya que el servidor de correo es un medio importante de comunicación y adicionalmente se lo utiliza como respaldos de confirmaciones y respuestas, y el sistema gestor es esencial para la gestión empresarial y la toma de decisiones.

Para los activos críticos servidor de BDD y computadores personales el requerimiento de seguridad más importante es la disponibilidad, debido a que las PCs son la principal herramienta para el desarrollo de las actividades de los empleados de RECTIGAMOS S.A., y que la información que se almacena en el Servidor de BDD es la que se procesa en el sistema gestor, por lo que la misma debe estar disponible cada vez que un usuario autorizado a utilizar el sistema lo requiera.

Actividad S2.3 Identificar las amenazas a los activos críticos.

En esta actividad se desarrolla los pasos 12, 13, 14, 15 y 16 que se describen a continuación:

Paso 12: Se completa apropiadamente todos los árboles de amenazas, propuestos por OCTAVE-S, para cada activo crítico, tomando en cuenta las siguientes categorías de amenazas:

- Actores humanos usando acceso a la red.
- Actores humanos usando acceso físico.
- Problemas del Sistema.
- Otros problemas.

A continuación se presenta los resultados:

Activo crítico: Sistema Gestor

Actores humanos usando acceso físico y acceso a la red.

Se determina que pueden existir actores internos de la empresa con acceso a la red que representan una amenaza para este activo crítico, y que actúan tanto accidental como deliberadamente. Los mismos pueden causar revelación, modificación o interrupción de la información procesada por este sistema.

También se establece que pueden existir actores externos a la empresa con acceso físico que representan una amenaza para este activo crítico y que actúan tanto accidental como deliberadamente. Los mismos pueden causar revelación, pérdida, modificación o interrupción de la información procesada por este sistema.

Problemas del sistema.

Se determina que pueden existir tres actores que representan una amenaza para este activo crítico, los defectos de hardware, los fallos en el sistema y los códigos maliciosos (virus, gusanos, troyanos, backdoors).

Otros problemas.

Se establece que pueden existir dos actores que representan una amenaza para este activo crítico, los problemas de fuente de energía y los desastres naturales (terremotos, inundaciones e incendios).

Activo crítico: Servidor de BDD

Actores humanos usando acceso a la red.

Se determina que pueden existir actores internos de la empresa que accidentalmente pueden revelar, modificar o borrar datos importantes de la base de datos, y también pueden existir actores externos a la empresa que deliberadamente busquen acceder a la información que se almacena en el servidor.

Se descarta, que personal interno busque deliberadamente robar, modificar,

revelar o eliminar información de la base de datos, ya que las motivaciones para un ataque interno son muy bajas.

Actores humanos usando acceso físico.

Se descarta que personal interno o externo a la empresa pueda modificar, borrar o revelar información accidentalmente o deliberadamente, ya que nadie tiene acceso físico al servidor salvo el encargado de sistemas.

Problemas del sistema.

Se determina que la mayor amenaza para el servidor son defectos de hardware, debido a la obsolescencia de los equipos, y código malicioso que pueden provocar interrupción de las actividades normales en la empresa.

Otros problemas.

Se determina que pueden existir dos actores que representan una amenaza para este activo crítico, los problemas de fuente de energía y los desastres naturales (terremotos, incendios), que ocasionarían interrupción del trabajo, y podrían destruir la información.

Activo crítico: Servidor de Correo

Actores humanos usando acceso a la red.

Se determina que pueden existir actores internos de la empresa que accidentalmente pueden borrar correos con información importante para la empresa, y que pueden existir actores externos a la empresa que deliberadamente busquen acceder a la información que se almacena en el servidor.

Actores humanos usando acceso físico.

Se descarta que personal interno o externo a la empresa pueda modificar, borrar o revelar información accidentalmente o deliberadamente, ya que nadie tiene

acceso físico al servidor salvo el encargado de sistemas.

Problemas del sistema.

Se determina que la mayor amenaza para el servidor, es el código malicioso que puede ejecutarse al abrir un correo, lo cual puede dañar la máquina del usuario que lo abre, o alterar el correcto funcionamiento del servidor.

Otros problemas.

Se determina que las amenazas para este activo son, los problemas de fuente de energía y los desastres naturales (terremotos, incendios), que pueden provocar indisponibilidad de la información durante la duración del percance.

Activo crítico: Computadores personales.

Actores humanos usando acceso a la red.

Se determina que pueden existir actores internos de la empresa con acceso a la red que representan una amenaza para este activo crítico y que actúan tanto accidental como deliberadamente. Los mismos pueden causar perdida, modificación o interrupción de la información procesada por este sistema. También se establece, que pueden existir actores externos a la empresa con acceso a la red que representan una amenaza para este activo crítico y actúan tanto accidental como deliberadamente. Los mismos pueden causar revelación, modificación, pérdida o interrupción de la información procesada por este sistema.

Actores humanos usando acceso físico.

Se determina que pueden existir actores internos de la empresa con acceso físico que representan una amenaza para este activo crítico, y que actúan tanto accidental como deliberadamente. Los mismos pueden causar revelación, modificación, pérdida o interrupción de la información procesada por este sistema.

También se establece, que pueden existir actores externos a la empresa con acceso físico que representan una amenaza para este activo crítico y actúan tanto

accidental como deliberadamente. Los mismos pueden causar revelación, modificación, pérdida o interrupción de la información procesada por este sistema.

Problemas del sistema.

Se determina que pueden existir tres actores que representan una amenaza para este activo crítico, los defectos de software, defectos de hardware y los códigos maliciosos (virus, gusanos, troyanos, puertas traseras).

Otros problemas.

Se determina que pueden existir dos actores que representan una amenaza para este activo crítico, los problemas de fuente de energía y los desastres naturales (terremotos, incendios).

Paso 13: En este paso se determina cuáles son los actores que representan la mayor amenaza para cada uno de los activos críticos. Aquí se toma en cuenta las siguientes combinaciones de actores y motivos del actor:

- Internos actúan por accidente.
- Internos actúan deliberadamente.
- Externos actúan por accidente.
- Externos actúan deliberadamente.

Este paso solo se puede completar para las siguientes categorías de amenazas:

- Actores humanos usando acceso a la red.
- Actores humanos usando acceso físico. A continuación se presenta los resultados:

Activo crítico: Sistema Gestor

Actores humanos usando acceso a la red.

Internos que actúan por accidente: Se determina que la mayor amenaza a éste sistema a través de la red, son los usuarios que tienen un permiso y un perfil de usuario para utilizar el sistema.

Internos que actúan deliberadamente: Se determina que la mayor amenaza a éste sistema a través de la red, son todos los usuarios que no tienen permiso para utilizar el sistema.

Externos que actúan deliberadamente: Se determina que la mayor amenaza a éste sistema a través de la red, son actores humanos que quieren obtener información para su beneficio como personal de la competencia que esté interesado en conocer información de los contratos, o los proveedores que maneja la empresa.

Actores humanos usando acceso físico

Internos que actúan por accidente: Se determina que la mayor amenaza a éste sistema por medios físicos, son tanto los usuarios que utilizan el sistema en sus computadores, como los usuarios que no utilizan el sistema

Internos que actúan deliberadamente: Se determina que la mayor amenaza a éste sistema por medios físicos, son tanto los usuarios que utilizan el sistema en sus computadores, como los usuarios que no utilizan el sistema.

Externos que actúan por accidente: Se determina que la mayor amenaza a éste sistema por medios físicos, son los usuarios que ingresan a la empresa ya sea por utilizar los servicios de RECTIGAMOS S.A., realizar el cobro de algún servicio prestado, o por contactarse con un empleado en específico.

Externos que actúan deliberadamente: Se determina que la mayor amenaza a éste sistema por medios físicos, son los usuarios ingresan a la empresa ya sea por utilizar los servicios de RECTIGAMOS S.A., realizar el cobro de algún servicio prestado, o por contactarse con un empleado en específico.

Activo crítico: Servidor de base de datos

Actores humanos usando acceso a la red

Internos que actúan por accidente: Se determina que los empleados que trabajan con algún módulo del sistema gestor, están expuestos a eliminar o modificar accidentalmente algún dato de la base, principalmente por desconocimiento del funcionamiento del sistema.

Externos que actúan deliberadamente: Como actores externos se identifican, personas que de alguna u otra manera les interesa información de la contabilidad de la empresa, o los registros de los clientes y proveedores que buscan acceder al servicio de la empresa.

Activo crítico: Servidor de correo

Actores humanos usando acceso a la red

Internos que actúan por accidente: Se determina que todo el personal de la empresa está expuesto a eliminar accidentalmente un correo electrónico, pero hay que prestar mayor atención a los empleados que reciben en sus correos información sensible.

Además los internos pueden abrir correos que ejecuten código malicioso, que pueden dañar la máquina del usuario o en el peor de los casos el servidor.

Externos que actúan deliberadamente: Como actores externos se identifica, personal de la competencia que esté interesado en conocer información de los contratos, o de los proveedores que maneja la empresa.

Activo crítico: Computadores personales

Actores humanos usando acceso a la red.

Internos que actúan por accidente: Se determina que la mayor amenaza a éste activo a través de la red, son todos los empleados de RECTIGAMOS S.A. que utilizan las PCs para realizar sus actividades.

Internos que actúan deliberadamente: Se determina que la mayor amenaza a éste activo a través de la red, son todos los empleados de RECTIGAMOS S.A. que utilizan las PCs para realizar sus actividades.

Externos que actúan por accidente: Se determina que la mayor amenaza a éste activo a través de la red, son los usuarios que utilizan los servicios de RECTIGAMOS S.A., y que rinden pruebas de aptitud en algunos computadores

ubicados en las instalaciones de la empresa, que se utilizan sólo con ese fin.

Externos que actúan deliberadamente: Se determina que la mayor amenaza a éste activo a través de la red, son los usuarios que utilizan los servicios de RECTIGAMOS S.A., y que rinden pruebas de aptitud en algunos computadores ubicados en las instalaciones de la empresa, que se utilizan sólo con ese fin.

Actores humanos usando acceso físico

Internos que actúan por accidente: Se determina que la mayor amenaza a éste activo por medios físicos, son todos los empleados de RECTIGAMOS S.A.

Internos que actúan deliberadamente: Se determina que la mayor amenaza a éste activo por medios físicos, son todos los empleados de RECTIGAMOS S.A.

Externos que actúan por accidente: Se determina que la mayor amenaza a éste activo por medios físicos, son los usuarios que ingresan a la empresa ya sea por utilizar los servicios de RECTIGAMOS S.A., realizar el cobro de algún servicio prestado, o por contactarse con un empleado en específico.

Externos que actúan deliberadamente: Se determina que la mayor amenaza a éste activo por medios físicos, son los usuarios que ingresan a la empresa ya sea por utilizar los servicios de RECTIGAMOS S.A., realizar el cobro de algún servicio prestado, o por contactarse con un empleado en específico.

Paso 14 En este paso se anota la opinión del equipo de análisis sobre la intensidad de la motivación del actor a realizar un ataque, y el grado de confianza en esa estimación. Aquí se toma en cuenta las siguientes combinaciones de actores y motivos del actor:

- Internos actúan deliberadamente.
- Externos actúan deliberadamente.

Este paso solo se puede completar para las siguientes categorías de amenazas:

- Actores humanos usando acceso a la red.
- Actores humanos usando acceso físico. A continuación se presenta los resultados:

Activos crítico: Sistema gestor

Actores humanos usando acceso a la red.

Internos que actúan deliberadamente: Se considera que la motivación que tienen los actores internos con acceso a la red y que actúan deliberadamente es de puntuación media, pero la estimación que se tienen de estas conclusiones son bajas debido a que no se tienen datos objetivos relacionados con dicha estimación.

Externos que actúan deliberadamente: Se considera que la motivación que tienen los actores externos con acceso a la red que actúan deliberadamente es de puntuación alta, pero la estimación que se tienen de estas conclusiones son bajas debido a que no se tienen datos objetivos relacionados con dicha estimación.

Actores humanos usando acceso físico.

Internos que actúan deliberadamente: Se considera que la motivación que tienen los actores internos con acceso físico que actúan deliberadamente es de puntuación media, pero la estimación que se tienen de estas conclusiones son bajas debido a que no se tienen datos objetivos relacionados con dicha estimación.

Externos que actúan deliberadamente: Se considera que la motivación que tienen los actores externos con acceso físico que actúan deliberadamente es de puntuación alta, pero la estimación que se tienen de estas conclusiones son bajas debido a que no se tienen datos objetivos relacionados con dicha estimación.

Activo crítico: Servidor de base de datos

Actores humanos usando acceso a la red.

Internos que actúan deliberadamente: Se descarta que personal interno busque deliberadamente dañar o robar la información de la base de datos, ya que las motivaciones de los empleados son muy bajas.

Externos que actúan deliberadamente: En cuanto a personal externo las motivaciones de los atacantes se las considera de nivel medio, pero no se tienen datos seguros de esta estimación.

Activo crítico: Servidor de correo

Actores humanos usando acceso a la red.

Internos que actúan deliberadamente: Se descarta que personal interno busque deliberadamente revelar o alterar información sensible de los correos electrónicos, ya que las motivaciones de los empleados son muy bajas.

Externos que actúan deliberadamente: Se identifica que las motivaciones de los atacantes externos son altas, debido a que el jefe de sistemas ha reportado de varios intentos de ataques al servidor que provienen del exterior de la empresa, pero nunca han tenido éxito.

Activo crítico: Computadores personales

Actores humanos usando acceso a la red.

Internos que actúan deliberadamente: Se considera que la motivación que tienen los actores internos con acceso a la red y que actúan deliberadamente es de puntuación media, pero la estimación que se tienen de estas conclusiones son bajas debido a que no se tienen datos objetivos relacionados con dicha estimación.

Externos que actúan deliberadamente: Se considera que la motivación que tienen los actores externos con acceso a la red que actúan deliberadamente es de puntuación alta, pero la estimación que se tienen de estas conclusiones son bajas debido a que no se tienen datos objetivos relacionados con dicha estimación.

Actores humanos usando acceso físico

Internos que actúan deliberadamente: Se considera que la motivación que tienen los actores internos con acceso físico que actúan deliberadamente es de puntuación media, pero la estimación que se tienen de estas conclusiones son bajas debido a que no se tienen datos objetivos relacionados con dicha

estimación.

Externos que actúan deliberadamente: Se considera que la motivación que tienen los actores externos con acceso físico que actúan deliberadamente es de puntuación alta, pero la estimación que se tienen de estas conclusiones son bajas debido a que no se tienen datos objetivos relacionados con dicha estimación.

Paso 15: Para realizar este paso se debe revisar cualquier dato objetivo que pueda tener la empresa (por ejemplo, registros, datos de incidentes, documentación de problemas) así como datos subjetivos (lo que un miembro del personal o del equipo de análisis pueda recordar), tomando en cuenta el grado de confianza en la estimación de los datos obtenidos. Se debe mencionar que el equipo de análisis no cuenta con datos objetivos y se tienen pocos datos subjetivos, motivo por el cual se descarta realizar este paso y se centra en llevar a cabo los pasos siguientes.

Paso 16: En este paso se describen ejemplos o escenarios reales de cómo las amenazas específicas pueden afectar a cada uno de los activos críticos.

Aquí se toma en cuenta las siguientes combinaciones de actores y motivos del actor:

- Internos actúan por accidente.
- Internos actúan deliberadamente.
- Externos actúan por accidente.
- Externos actúan deliberadamente.

A continuación se describe resultados:

Activo crítico: Sistema gestor

Actores humanos usando acceso a la red

Internos que actúan por accidente: Se considera que los usuarios que tienen permiso para utilizar el sistema podrían amenazar el mismo, ya que por falta de conocimiento en la utilización de este activo, la existencia de la amenaza para modificar, perder, o borrar información crítica está presente.

Internos que actúan deliberadamente: Se considera que los usuarios que no tienen permiso para utilizar el sistema podrían amenazarlo, ya que a pesar de que

existen perfiles de usuario para la utilización de este activo, y que todos los empleados de la empresa firman un acuerdo de confidencialidad al momento de formar parte de RECTIGAMOS S.A., dichos usuarios pueden revelar información sensible debido principalmente a que no existe un proceso de control, o auditoría en el manejo de la información que el Sistema Gestor procesa.

Externos que actúan deliberadamente: Se considera que existen actores humanos externos a la empresa que realizan ataques para extraer información, o a su vez modificarla, para obtener algún beneficio, en especial de la sección financiera que es lo más importante de este sistema.

Actores humanos usando acceso físico

Internos que actúan por accidente: Se considera que cualquier usuario perteneciente a la empresa puede amenazar a este activo, ya que no existe un proceso de control de acceso a las oficinas dentro de la empresa, y el sistema al ser utilizado por diferentes personas en diferentes puestos de trabajo, podría causar algunos problemas como desconexión o apagado de las PCs en dónde se encuentra instalado el sistema, y esto produciría la caída del servicio.

Internos que actúan deliberadamente: Se considera que al no existir un proceso de control de acceso a las oficinas, y al no contar con cámaras de seguridad dentro de la empresa, pueden existir usuarios que ingresen a los puestos de trabajo en donde se encuentra instalado el sistema y desconectarlo, o apagarlo con el fin de causar un daño físico. Se debe mencionar que existe la posibilidad de que al ingresar a las oficinas, los usuarios encuentren prendidas las PCs en donde está instalado el sistema y pueden acceder a las mismas para ver o modificar información sensible.

Externos que actúan por accidente: Se considera que al no contar con cámaras de seguridad y al existir muchas personas que ingresan a la empresa ya sea por utilizar los servicios de RECTIGAMOS S.A., realizar el cobro de algún servicio prestado, o por contactarse con un empleado en específico, dichas personas podrían amenazar al activo, ya que las mismas se dirigen a las diferentes oficinas de la empresa, y podrían accidentalmente desconectar las PCs o algún componente

en donde se encuentra instalado el sistema y causar la caída o el daño del mismo. Además no se podría comprobar quién o quienes causaron los problemas.

Externos que actúan deliberadamente: Se considera que al no contar con cámaras de seguridad y al existir muchas personas que ingresan a la empresa ya sea por utilizar los servicios de RECTIGAMOS S.A., realizar el cobro de algún servicio prestado, o por contactarse con un empleado en específico, estas podrían amenazar al activo ya que las mismas se dirigen a las diferentes oficinas de la empresa y podrían deliberadamente desconectar las PCs o algún componente en donde se encuentra instalado el sistema y causar la caída o el daño del mismo. Además no se podría comprobar quién o quienes causaron los problemas.

Problemas del sistema

Fallos del sistema: Se considera que los fallos del sistema son una amenaza que está presente, y que causaría serios problemas a los procesos de negocios de RECTIGAMOS S.A. en caso de producirse alguno, ya que no existe soporte técnico ni manuales para solucionar problemas.

Defectos de Hardware: Se considera que el Sistema Gestor al estar instalado en diferentes computadores, está sujeto a amenazas que le pueden ocurrir a un PC normal, como los defectos de hardware, los mismos que pueden producir interrupción en los procesos de negocio de la empresa y hasta perdida de información crítica. Esto debido a que no existe una política sobre el mantenimiento de la TI de RECTIGAMOS S.A.

Código Malicioso: Se considera que el Sistema Gestor al estar instalado en diferentes computadores, está sujeto a amenazas que le pueden ocurrir a cualquier PC, como los códigos maliciosos. Si bien todas las PCs de la empresa cuentan con un antivirus, siempre existe la posibilidad de que se infecten con este tipo de códigos principalmente por la utilización de las memorias USB, y por la conexión en red con la que cuentan todas las computadoras.

Otros Problemas

Desastres Naturales: Se considera que no existe una protección adecuada en

las instalaciones de RECTIGAMOS S.A., y en el caso de un evento sísmico en la ciudad de Guayaquil, la empresa no garantizaría la disponibilidad del Sistema Gestor para su utilización.

Problemas de fuente de energía: Se considera a los problemas de fuente de energía como una amenaza latente, ya que RECTIGAMOS S.A. no cuenta con una fuente de energía auxiliar, lo que ocasionaría problemas en caso de un eventual corte de energía o problemas similares, y provocaría interrupción en los procesos de negocio de la empresa.

Activo crítico: Servidor de Base de datos

Actores humanos usando acceso a la red

Internos que actúan por accidente: Usuarios internos, que por desconocimiento modifiquen, o expongan a personal no autorizado, información sensible almacenada en la base de datos.

Externos que actúan deliberadamente: Usuarios externos, que les interese la información que se almacena, que ingresen ilícitamente a la red con el fin de obtener los datos que buscan.

Problemas del Sistema

Defectos de Hardware: Podrían presentarse problemas de hardware, debido principalmente a la obsolescencia de los equipos, el servidor de base de datos corre sobre un SO Windows server 2003, ligado a una plataforma de hardware relativamente antigua con una capacidad que podría resultar ineficiente y afectar a la producción de la empresa.

Otros Problemas

Fuente de Energía: La empresa ha adquirido un UPS, pero todavía no lo tienen instalado, por lo que se corre el riesgo de que en caso de un corte de energía se apaguen todos los equipos, se detenga la producción diaria, y se pierdan los datos que no han sido guardados hasta que vuelva la corriente eléctrica. La página web de la empresa seguiría disponible debido a que el servidor se encuentra

en el exterior, pero no se podrá almacenar información que se intente ingresar durante el tiempo de la falta de energía.

Desastres Naturales: La destrucción del servidor por cualquier tipo de desastre natural sería una perdida para la empresa, si bien se guardan respaldos semanales de la base de datos, el tiempo que tomaría restaurar la base significaría en interrupción de las actividades de la empresa.

Activo Crítico: Servidor de Correo

Actores humanos usando acceso a la red

Internos que actúan por accidente: Usuarios internos que por desconocimiento abren correos que contienen código malicioso, el mismo que empieza a enviar spam hacia el servidor, lo que provoca que el servidor empiece a trabajar más de lo normal, se hace más lento el tiempo de respuesta, y en el peor de los casos puede sobrecargar al servidor e interrumpir sus servicios.

Externos que actúan deliberadamente: Se tiene conocimiento que personal externo a la empresa, ha intentado hackear el servidor de correo con el objetivo de conseguir la clave del gerente general, en cuyo caso se procede a cambiar la clave del gerente cada vez que se ha presentado este incidente.

Problemas del Sistema

Código Malicioso: Usuarios que por desconocimiento, abren correos que ejecutan código malicioso. Si bien en la empresa se usa message WLAVS, este únicamente advierte que un mensaje puede ser peligroso, y queda a elección del usuario abrir o no el correo.

Otros problemas

Fuente de Energía: Igual que como ocurre con el servidor de base de datos, el servidor de correo tampoco está conectado a ningún ups, lo que provocaría la pérdida del servicio de correo durante una posible falla de energía, si bien el impacto en el trabajo de los usuarios es mucho menor que cuando falla el servidor de base de datos.

Desastres Naturales: Representaría una gran pérdida para la empresa, si algún desastre natural como incendio, o terremoto destruye el servidor, debido a que no se almacenan respaldos de los correos electrónicos y aquí se almacena información sensible como confirmaciones de contratos, e informaciones de los proveedores.

Activo Crítico: Computadores Personales

Actores humanos usando acceso a la red

Internos que actúan por accidente: Se considera que todo el personal que utiliza las PCs para realizar sus actividades podrían amenazar el mismo, ya que a pesar de que existen perfiles de usuario para la utilización de este activo, y que todos los empleados de la empresa firman un acuerdo de confidencialidad al momento de formar parte de RECTIGAMOS S.A., dichos usuarios accidentalmente pueden revelar, modificar, o perder información sensible que se encuentran en las diferentes PCs de la empresa, debido principalmente a que no existe un proceso de control o auditoría en el manejo de la información que se maneja en cada una de las computadoras de RECTIGAMOS S.A..

Internos que actúan deliberadamente: Se considera que todo el personal que utilizan las PCs para realizar sus actividades podrían amenazar el mismo, ya que a pesar de que existe perfiles de usuario para la utilización de este activo, y que todos los empleados de la empresa firman un acuerdo de confidencialidad al momento de formar parte de RECTIGAMOS S.A., dichos usuarios deliberadamente pueden revelar, modificar, o perder información sensible que se encuentran en las diferentes PCs de la empresa debido principalmente a que no existe un proceso de control o auditoría en el manejo de la información que se maneja en cada una de las computadoras de RECTIGAMOS S.A..

Externos que actúan por accidente: Se considera que las personas que utilizan los servicios de RECTIGAMOS S.A., y que se les brinda un acceso restringido al momento de dar las pruebas de aptitud que la empresa realiza dentro de sus instalaciones, podrían representar una amenaza para este activo, pero dicha amenaza no afectaría a los procesos de negocio de RECTIGAMOS S.A., ya que son computadores que se utilizan exclusivamente para rendir las pruebas de aptitud.

Externos que actúan deliberadamente: Se considera que las personas que utilizan los servicios de RECTIGAMOS S.A., y que se les brinda un acceso restringido al momento de dar las pruebas de aptitud que la empresa realiza dentro de sus instalaciones, podrían representar una amenaza para este activo, pero dicha amenaza no afectaría a los procesos de negocio de RECTIGAMOS S.A., ya que son computadores que se utilizan exclusivamente para rendir las pruebas de aptitud.

Actores humanos usando acceso físico

Internos que actúan por accidente: Se considera que cualquier usuario perteneciente a la empresa puede amenazar a este activo, ya que no existe un proceso de control de acceso a las oficinas dentro de la empresa, y esto podría causar algunos problemas como desconexión o apagado de las PCs.

Internos que actúan deliberadamente: Se considera que cualquier usuario perteneciente a la empresa puede amenazar a este activo, ya que no existe un proceso de control de acceso a las oficinas dentro de la empresa, y esto podría causar algunos problemas como desconexión o apagado de las PCs. Existe además usuarios que no bloquean sus computadores al momento de dejar sus puestos de trabajo, lo que permitiría que otros accedan indebidamente, y modifiquen o borren información sensible.

Problemas del sistema

Defectos de software: Se considera que cualquiera de las PCs pertenecientes a la empresa, están sujetas a amenazas de este tipo, sin embargo se cuenta con personal de Ingeniería en Sistemas que darían una solución oportuna y rápida.

Defectos de Hardware: Se considera que cualquiera de las PCs pertenecientes a la empresa están sujetas a amenazas de este tipo, los mismos que pueden producir interrupción en los procesos de negocio de la empresa y hasta perdida de información crítica, sin embargo se cuenta con personal de Ingeniería en Sistemas que darían una solución oportuna en caso de que una amenaza de este tipo llegara a suceder.

Código Malicioso: Se considera que cualquiera de las PCs pertenecientes a la empresa, están sujetas a amenazas de este tipo. Si bien la mayoría de las PCs de la empresa cuentan con un antivirus, siempre existe la posibilidad de que se infecten con alguno de estos códigos maliciosos principalmente por la utilización de las memorias USB y por la conexión en red con la que cuentan todas las computadoras.

Otros Problemas

Desastres Naturales: Se considera que en el caso de un evento sísmico en la ciudad de Guayaquil, la empresa se vería afectada y no garantizaría la disponibilidad de las PCs para su utilización.

Problemas de fuente de energía: Se considera a los problemas de fuente de energía como una amenaza latente, ya que RECTIGAMOS S.A. no cuenta con una fuente de energía auxiliar, lo que ocasionaría problemas en caso de un eventual corte de energía o problemas similares, y existiría interrupción en los procesos de negocio de la empresa.

FASE 2: Identificar vulnerabilidades en la infraestructura.

En esta fase se desarrolla el proceso S3 descrito anteriormente.

Proceso S3: Examinar la Infraestructura Computacional en relación con los activos críticos.

Este proceso se centra en examinar las vías de acceso a los activos críticos a través de la infraestructura tecnológica, y analizar los procesos relacionados con la tecnología.

La figura 39 muestra las actividades, y los pasos que se desarrollan en el proceso S3.

Figura 39: Actividades y pasos del proceso S3, Metodología Octave-S
Fuente: Octave- S ® Implementation Guide, Version 1.0, página 6.

Actividad S3.1 Examinar rutas de acceso.

En esta actividad se desarrolla los pasos 17 y 18 que se describen a continuación:

Paso 17: En este paso se determina cuál es el sistema que está más estrechamente ligado al activo crítico, para poder identificar el sistema de interés.

El sistema gestor es uno de los activos más importantes de la empresa, debido a que este gestiona todos los procesos de negocio que se realizan en la empresa. Los módulos del sistema son manejados por diferentes usuarios de acuerdo a la función que cada uno tenga en la empresa, y por tal motivo es instalado únicamente en las máquinas de los usuarios que lo utilizan para realizar sus actividades. La información que es procesada por el sistema se transmite al servidor de base de datos a través de los switches para ser almacenada ahí, y de la misma forma es transmitida del servidor de base de datos a las máquinas que tienen instalado el sistema.

Paso 18: El paso 18 se divide en 5 sub pasos y describe cada uno de ellos a continuación:

Paso 18a: En este paso se examina las rutas de acceso y se identifica los componentes claves de red que están relacionados con el sistema gestor. Los computadores personales y laptops son parte importante del sistema, ya que el mismo debe ser instalado directamente en las máquinas. Además el sistema está relacionado con el servidor de base de datos, ya que es aquí en donde se almacenan todos los datos procesados en los diferentes computadores que tienen instalada la aplicación. La información se transmite a los usuarios a través de un switch dependiendo del piso donde esté ubicada la máquina que solicita la misma.

Paso 18b: En este paso se determina qué clase de componentes se utilizan para transmitir información desde el sistema de interés, y se estableció que la información procesada en el sistema gestor no puede ser accedida por usuarios internos desde fuera de la red interna a través de internet, únicamente pueden acceder a través de la red interna, y desde las máquinas que tienen instalado el sistema.

Paso 18c: En este paso se determina qué clase de componentes pueden utilizar la

persona (usuarios, atacantes) para acceder al sistema de interés, y se establece, que para que una persona pueda acceder al sistema debe tener instalada y configurada la aplicación en su PC. Para que un atacante externo pueda acceder a los registros que almacena el sistema gestor, debería físicamente acceder a la computadora de uno de los trabajadores mencionados.

Paso 18d: En este paso se determina qué clase de componentes se utilizan para realizar respaldos de la información del sistema de interés, y se establece, que toda la información que procesa el sistema gestor, se almacena en el servidor de base de datos, y es respaldada semanalmente en el servidor de respaldo por medio de una tarea programada fuera de los horarios de oficina.

Paso 18e: En este paso se determina si existen otros sistemas o componentes que acceden a la información, servicios, o aplicaciones del sistema de interés, y se establece que no existe ningún otro sistema o componente que se utilice para acceder a la información crítica del sistema gestor.

Actividad S3.2 Analizar Procesos Relacionados con la Tecnología.

En esta actividad se desarrolla los pasos 19, 20 y 21 que se describen a continuación:

Paso 19: El paso 19 se divide en 2 sub pasos y se describen cada uno de ellos a continuación:

Paso 19a: En este paso se determina qué clase de componentes están relacionados con uno o más activos críticos. Se marca la ruta en las ramas del sistema de interés para cada clase seleccionada en los pasos 18a – 18e. Aquí se establece que los componentes relacionados con los activos críticos son los servidores, la red interna, las estaciones de trabajo, y laptops utilizadas dentro de RECTIGAMOS S.A.

Paso 19b: En este paso se relaciona a los activos críticos con cada clase de componente. Se determina que el sistema gestor está estrechamente relacionado con el servidor de base de datos y con las estaciones de trabajo en donde se encuentra instalado. Además, el servidor de base de datos está relacionado con el servidor de correo, servidor de respaldo y con todas las estaciones de trabajo de la

empresa. El servidor de correo está relacionado con todas las estaciones de trabajo.

Paso 20: En este paso se asigna la responsabilidad de quien mantiene y se encarga de cada clase de componente en la red. En RECTIGAMOS S.A. estas funciones están únicamente a cargo del Encargado de Sistemas. La seguridad de las portátiles y los computadores, son responsabilidad del usuario al cual se le ha asignado.

Paso 21: En este paso se realiza una estimación del grado en el que la seguridad es considerada en los procesos de configuración y mantenimiento de los componentes de la red, y se llegó a la conclusión de que la empresa realiza las configuraciones, enfocándose principalmente en la producción, y se deja de un lado muchos aspectos de seguridad.

No se identificaron otros Ítems de Acción, Notas o Recomendaciones para el Proceso S3.

4.5. Análisis comparativo de los resultados obtenidos

En este apartado se realiza una comparación entre las metodologías utilizadas en el presente proyecto. Primero se analiza las diferencias de realizar la evaluación con MSAT y OCTAVE -S. A continuación se compara los resultados obtenidos con cada herramienta basada en las áreas equivalentes. Las áreas equivalentes se obtuvieron de ligar las áreas de práctica de seguridad de OCTAVE –S que cubren ámbitos similares a las secciones de cada una de las áreas de MSAT.

Como conclusión se determina que las áreas de análisis que cubren ambas herramientas, son prácticamente equivalentes salvo pequeñas excepciones que se analizarán más adelante.

La principal diferencia para decantarse a realizar un análisis con una u otra herramienta, es la experiencia y conocimiento que tenga sobre la empresa el equipo de análisis. Para escoger MSAT, se necesita que el equipo tenga un amplio conocimiento sobre cómo se gestionan las diferentes áreas de la empresa, de esta manera se puede responder adecuadamente el cuestionario y hacer el análisis

respectivo de los resultados. Se inclina por OCTAVE -S, si el equipo no tiene conocimiento de cómo funcionan los procesos dentro de la empresa. El equipo basado en las hojas de trabajo que ofrece la herramienta, debe irse informando conforme avanza el proyecto, para desarrollar cada una de las actividades que propone OCTAVE –S.

Otra diferencia entre las metodologías es el tiempo de duración de las evaluaciones para llegar a obtener los resultados con cada una de ellas. Con MSAT si el equipo conoce los procesos de la empresa, puede llenar el cuestionario, analizar los resultados y escoger las recomendaciones adecuadas para la empresa, en un periodo de tiempo relativamente corto. Por otro lado en OCTAVE -S, incluso si el equipo tiene conocimiento de las actividades de la empresa, se deben elaborar los 30 pasos que propone la metodología para poder obtener los resultados de la evaluación, lo cual toma un tiempo más significativo respecto a la evaluación con MSAT.

Además MSAT analiza los riesgos y entrega recomendaciones para todas las áreas de estudio que propone la herramienta. En cambio OCTAVE -S hace un análisis de las áreas que presentan mayores problemas, y que necesitan resolverse con mayor urgencia, y se elaboran las recomendaciones y procedimientos únicamente para estas áreas.

CAPITULO V

CONCLUSIONES Y RECOMENDACIONES

En este capítulo se presentan las conclusiones y recomendaciones a las que se ha llegado una vez concluido el proceso de evaluación y análisis de riesgos.

5.1. Conclusiones

a) Se cumple con el principal objetivo del proyecto que era realizar un diagnóstico de vulnerabilidades mediante el análisis de riesgos, y desarrollar un plan de seguridad para la información de la empresa RECTIGAMOS S.A.

b) Se realiza la evaluación utilizando las herramientas OCTAVE –S y MSAT y a partir de los resultados obtenidos se diseña el plan de seguridad para RECTIGAMOS S.A.

c) Se confirma que los activos críticos más importantes para los procesos de negocio de la empresa son el sistema contable y de exportaciones y el servidor de base de datos y correo electrónico.

d) Se determina que la información sensible que maneja la empresa, son los datos que se procesa en el sistema contable, correos electrónicos y la información de clientes y proveedores.

e). Para utilizar OCTAVE -S, el equipo basándose en las hojas de trabajo que ofrece la herramienta, puede irse informando conforme avanza el proyecto, para desarrollar cada una de las actividades que propone OCTAVE –S.

f) OCTAVE -S utiliza estados de alerta para determinar el nivel de criticidad de un área en particular, se analiza las actividades que se llevan a cabo correctamente, y las que faltan o no se hacen apropiadamente dentro de cada área de seguridad, lo cual sirve para asignar un estado de semáforo.

g) Se obtuvo un listado de los activos importantes de RECTIGAMOS S.A. una perspectiva del enfoque actual de la empresa para hacer frente a cada una de las áreas de práctica de seguridad y un perfil de riesgo para cada activo crítico.

h) La creación de perfiles de amenaza permite tener una idea clara de posibles situaciones dentro de los cuales los activos críticos podrían verse comprometidos, fundamentando este análisis sobre las 4 categorías de amenaza: actores humanos utilizando acceso a la red, actores humanos utilizando acceso físico, problemas de sistemas y otros problemas.

i) Se determina que las áreas más críticas, y que necesitan un plan de seguridad con más urgencia son las áreas de Gerencia, Contabilidad y Taller.

j) El plan de seguridad sirve para crear una base para prevenir posibles riesgos a futuro. La herramienta utiliza la experiencia del equipo de análisis, y los registros históricos de ataques en el pasado, para determinar la probabilidad de que una amenaza pueda sucederse e implementar los correctivos necesarios.

k) Con OCTAVE –S, incluso realizando una evaluación parcial, se obtiene información útil para mejorar la postura de la seguridad de la empresa.

l) El apoyo financiero es necesario para posibilitar la implementación del plan de seguridad y garantizar la continua gestión sobre el cumplimiento de los planes establecidos y la actualización constante sobre los mismos.

m) El entendimiento y comunicación entre los miembros del equipo de análisis es de vital importancia para llevar a cabo la evaluación de una manera correcta y ordenada.

5.2. Recomendaciones

a) Implementar, controlar y monitorear las actividades sugeridas en la propuesta del plan de seguridad del presente proyecto, con el fin de eliminar vulnerabilidades encontradas y disminuir la probabilidad de ocurrencia de los riesgos a futuro.

b) Es necesario que RECTIGAMOS S.A. cuente con una fuente alternativa de energía para evitar en lo posible que los procesos de negocio de la empresa se vean afectados a falta de energía eléctrica.

c) Crear programas de capacitación técnicos para el personal de TI, e informativos para el resto del personal, en temas relacionados con seguridad de la información. Esto ayuda al personal de TI a estar al día con las nuevas tecnologías y sus amenazas para hacerles frente, y al resto del personal a concientizar sobre la importancia de dar un buen uso a los recursos informáticos por la importancia que estos representan para la empresa.

d) Realizar evaluaciones periódicas de seguridad a la empresa ya sea por personal interno o externo. Estas evaluaciones periódicas ayudarán a mejorar la seguridad de los recursos de TI y de la información. Además podrían resultar beneficiosas para cumplir las estipulaciones, normativas y requisitos de clientes, socios y fabricantes.

e) Revisar periódicamente las políticas y procedimientos, debido a que la tecnología tiene avances constantemente y por ende aparecen riesgos que deben ser mitigados para evitar problemas futuros.

f) Actualizar los equipos de hardware sobre todo de los servidores ya que estos están obsoletos y pueden causar problemas a las actividades normales de la empresa.

h) Implementar procedimientos (simulacros), para que el personal de la empresa conozca a detalle las actividades que le corresponden a cada uno en caso de una emergencia

g) Aumentar el personal del área de TI, ya que el personal actual se considera insuficiente para llevar a cabo todas las actividades propuestas. O contratar empresas especializadas que se encarguen de llevar estas actividades.

CAPITULO VI

PROPUESTA

6.1. Datos informativos

- **Titulo**

"Diagnóstico de las vulnerabilidades informáticas en los Sistemas de Información para proponer soluciones de Seguridad a la empresa RECTIGAMOS S.A".

- **Institución ejecutora**

RECTIGAMOS S.A

- **Director de tesis**

Msig. Nelson Mora.

- **Beneficiario**

Rectificadora Gabriel Mosquera.

- **Ubicación**

Av. Cosme Renella y Av. de las Américas

- **Tiempo estimado para la ejecución**

Fecha de inicio: Octubre del 2014

Fecha de Finalización: Marzo del 2015

- **Equipo técnico responsable**

Investigadores: Karen Pintado y Cesar Hurtado

6.2. Antecedentes de la propuesta

En la actualidad gran parte de las empresas, instituciones públicas privadas y gubernamentales han sufrido un sin número de ataques informáticos especialmente en lo que respecta al robo, alteración y modificación de la información, por tal motivo surge la necesidad de tomar medidas de seguridad para salvaguardar confidencialmente su información.

Luego de haber aplicado una entrevista al personal encargado del departamento de sistemas se ha podido averiguar lo siguiente que RECTIGAMOS S.A no cuenta con ningún software informático para la detección de vulnerabilidades en los sistemas informáticos que posee la institución por lo que se está poniendo en riesgo la seguridad de la información. Además el portal web de la institución fue comprometido en algún momento por lo que se puso en riesgo el buen nombre de la organización.

Es por esto que la empresa debe contar con software informático para detectar vulnerabilidades en los servidores y servicios que posee la empresa, así como también se debe aumentar la seguridad en los sistemas informáticos estableciendo algunas políticas de seguridad dentro de la institución, Para conseguir mejorar la confidencialidad al momento del envió de archivos es conveniente usar el metodologías para detectar vulnerabilidades en los servicios que corren en la intranet de la empresa.

6.3. Justificación de la propuesta

Es primordial que el presente trabajo investigativo se lo realice ya que la detección de vulnerabilidades dentro de los sistemas de información de RECTIGAMOS S.A ayudará a evaluar, y determinar el grado de incidencia de las mismas en cuanto a la seguridad de la información se refiere.

Proteger la información

Con la aplicación de la metodología Octave-S y la herramienta MSAT se podrá detectar a tiempo las vulnerabilidades informáticas en la empresa, ayudando a alertar al administrador antes de un ataque a los servidores por ser estos vulnerables.

Estabilidad en los servicios

Es importante que los servidores que son los que contiene la información más crítica sean seguros de esta manera los servicios que estos prestan serán seguros y así la transmisión de la información se realizará en forma segura.

Es por esto que los servidores con sus respectivos servicios tienen que estar bien configurados con todas las medidas de seguridad, para cuando se necesite cualquier información esta sea transparente.

6.4. Objetivos de la propuesta

6.4.1. Objetivo General

El objetivo de la presente propuesta es diagnosticar y diseñar un plan de seguridad de la información para la empresa RECTIGAMOS S.A. logrando mejorar y desarrollar nuevos procesos de protección de sus activos de información.

6.4.2. Objetivos Específicos

- Caracterizar la empresa desde un punto de vista tecnológico.
- Revisar los activos importantes de la empresa y valorarlas desde el punto de vista de la seguridad y disponibilidad.
- Evaluar los riesgos a los cuales se encuentra expuesta la información de RECTIGAMOS S.A.

- Realizar un diagnóstico de la seguridad de la información que abarcará las áreas de seguridad en la infraestructura, aplicaciones, operaciones y del personal.
- Utilizar las herramientas propuestas para efectuar la evaluación de riesgos de la información en la empresa RECTIGAMOS S.A.
- Analizar los resultados obtenidos en las evaluaciones con el fin de encontrar las causas de los problemas y proponer actividades de mitigación.

6.5. Análisis de Factibilidad

Según el tipo de propuesta se debe tener en cuenta ciertos aspectos de viabilidad:

Política: La empresa RECTIGAMOS.SA tiene como política asegurar la información por lo cual es viable realizar el estudio.

Tecnológica: El uso de metodologías como OCTAVE-S para detectar riesgos en los sistemas de información mejorará las condiciones de seguridad en los servicios de RECTIGAMOS.SA.

Ambiental: En la realización del presente proyecto no se afectará al medio ambiente.

Económico-financiera: El proyecto en el ámbito económico es factible de realizarlo ya que todas las herramientas de software que se utilizarán son libres por lo cual no se pagarán los costos de licencia.

Legal: El proyecto de investigación es viable porque está cumpliendo todas las leyes, normas y metodologías.

6.6. Plan de seguridad

En este capítulo se presenta el plan de seguridad con las recomendaciones que propone MSAT, se desarrolla en la fase tres de la metodología de OCTAVE -S, que consta de los pasos del 22 al 30 y contienen las siguientes actividades:

Evaluación del impacto de las amenazas, evaluación de probabilidad de las amenazas, descripción de estrategias de protección actual, selección de enfoques de mitigación, desarrollo de planes de mitigación, e identificación de cambios y pasos siguientes, y finalmente se diseña un plan de seguridad general.

El plan de seguridad de MSAT contiene las recomendaciones y buenas prácticas que entrega la herramienta en su informe completo, resumidas y adaptadas por los autores del presente proyecto.

En relación con las actividades que corresponden a OCTAVE-S, para la evaluación del impacto de las amenazas se analiza como los riesgos determinados en el capítulo anterior pueden afectar a las diferentes áreas de la empresa. En la evaluación de probabilidad de las amenazas se llega a la conclusión de no desarrollar estas actividades, debido a que no se tienen registros históricos documentados que se relacionen con las amenazas, y el personal de TI carece de experiencia y conocimientos en seguridad de la información y/o gestión de riesgos. En la descripción de estrategias de protección actual, se identifica el enfoque actual de la empresa para hacer frente a cada una de las áreas. Para la selección de enfoques de mitigación, se seleccionan las áreas de seguridad, que presentan mayores problemas, que necesitan ser resueltos con más urgencia, teniendo un mayor impacto para la organización y mayor margen de mejora, seleccionándose como áreas de mitigación. En el desarrollo del plan de mitigación se desarrolla los procesos, procedimientos, políticas, roles y responsabilidades para las áreas seleccionadas en el paso anterior. En la Identificación de cambios y pasos siguientes se enumeran un conjunto de actividades para dar apoyo a la implementación del Plan de Seguridad.

El plan general recopila las recomendaciones y actividades de mitigación de ambos planes de seguridad, revisados y adaptados de acuerdo a los resultados

obtenidos en la comparación de las herramientas. El diseño del plan incluye únicamente las áreas que OCTAVE -S considera de mayor riesgo para la empresa, y sus equivalentes de MSAT.

El desarrollo de todas las actividades anteriormente mencionadas, permitió detectar las áreas más vulnerables, y que representan un impacto más grave para la empresa, y desarrollar un conjunto de actividades y procedimientos para cada una de las áreas seleccionadas, que se recomienda implementar en RECTIGAMOS S.A. con el fin de proteger su información y activos más valiosos.

6.7. Plan de seguridad de MSAT

El plan de seguridad de MSAT contiene las recomendaciones propuestas por la herramienta para las secciones y sub-secciones de cada área que presentan problemas y/o necesitan mejoras.

6.7.1. ÁREA: INFRAESTRUCTURA

Tabla 34: Área de Infraestructura

ÁREA	SECCIONES	SUB-SECCIONES
INFRAESTRUCTURA	Defensa del perímetro	Acceso remoto
		Segmentación
		Sistema de detección de intrusiones (IDS)
		Inalámbrico
	Autenticación	Usuarios administrativos
		Usuarios de acceso remoto
		Directivas de contraseñas
		Cuentas de usuario

		Directivas de contraseñas Cuentas de acceso remoto
	Gestión y Control	Creación segura
		Seguridad física

Elaborado por: Los autores

6.7.1.1 Defensa del Perímetro

Acceso remoto

Revisar con regularidad la lista de acceso de los usuarios que tienen permiso para acceder remotamente a la red de RECTIGAMOS S.A..

Utilizar VPN para la conectividad de acceso de usuario remoto basada en las tecnologías IPSec, SSL, y SSH.

Segmentación

Asegurar que los cortafuegos, la segmentación y los sistemas de detección de intrusiones permiten proteger la infraestructura de la empresa de los ataques desde Internet.

Utilizar segmentos para separar extranet específicas y el acceso de fabricantes, socios o clientes.

Gestionar los controles de red para permitir sólo el acceso necesario para cada conexión de terceros.

Sistema de detección de intrusiones (IDS)

Continuar con la práctica de utilización de sistemas de detección de intrusiones basados en red para detectar anomalías que inicien un riesgo potencial e investigar la tecnología de prevención de intrusiones a medida que esté disponible.

En lo posible implementar un sistema de detección de intrusiones basado en host con el fin de notificar al encargado de la red que se está produciendo un ataque a fin de que puedan responder inmediatamente.

Inalámbrico

En la actualidad RECTIGAMOS S.A. no cuenta con la opción de conexión inalámbrica a la red con lo que se minimizan los riesgos. Sin embargo, si la empresa a futuro se planea o pone en práctica el acceso inalámbrico, no debería incluir la difusión del SSID, pero sí el cifrado WPA, además de tratar la red como una de no confianza.

6.7.1.2. Autenticación

Usuarios administrativos

· Eliminar los accesos administrativos a las estaciones de trabajo para los usuarios que no cuenten con los permisos respectivos.

· Implantar otro mecanismo de autenticación para disminuir el riesgo de accesos no autorizados es otro factor que debe ser tomado en cuenta por los miembros del personal de TI.

· Poner en práctica una directiva de contraseñas complejas para las cuentas administrativas, las contraseñas deben cumplir las siguientes condiciones:

- Alfanumérico
- Mayúsculas y minúsculas
- Contiene al menos un carácter especial
- Contiene como mínimo 14 caracteres

- Para limitar más los riesgos de ataques a las contraseñas, se debe poner en práctica los siguientes controles.
- Caducidad de contraseñas
- Bloqueo de la cuenta después de entre 7 y 10 intentos de registro fallidos
- Registro del sistema

Usuarios de acceso remoto

· Limitar el acceso únicamente a aquellos empleados que tengan una necesidad empresarial de conectividad remota.

· Implementar controles de contraseña complejos para los usuarios de acceso remoto, si se ha concedido este acceso mediante el uso de tecnologías de acceso telefónico o VPN. Utilizar una contraseña compleja que cumpla con los siguientes criterios:

- Caracteres alfanuméricos
- Uso de mayúsculas y minúsculas
- Al menos un carácter especial
- Longitud mínima de 8 caracteres

· Considerar la posibilidad de implementar controles avanzados para la gestión de cuentas y para el registro de acceso a cuentas.

· Al no permitir el acceso remoto ni a contratistas ni a terceros usuarios, se reduce los riesgos globales para la empresa. Sin embargo, si el acceso remoto se utiliza en el futuro, se debe asegurar que se lo hace conforme a la mejor práctica recomendada para minimizar así el riesgo asociado con esta forma de acceso.

Directivas de contraseñas

· Utilizar contraseñas complejas es un elemento fundamental del índice de defensa en profundidad. Las contraseñas complejas deben tener de 8 a 14 caracteres e incluir caracteres alfanuméricos y especiales. Establecer una longitud mínima, un historial, un límite a la duración y una caducidad para reforzar la defensa, debe ser

un factor a tomar en cuenta. Generalmente la caducidad de las contraseñas debe configurarse de la siguiente forma:

- Duración máxima de 90 días
- Las cuentas nuevas deben cambiar la contraseña al inicio de la sesión
- Un historial de 8 contraseñas (mínimo de 8 días)
- Activar un proceso de bloqueo de cuenta tras 10 intentos de registro fallidos en todas las cuentas de usuario.
- Utilizar el mecanismo de autenticación multifactor, especialmente para las cuentas administrativas y de usuarios remotos.
- Activar el bloqueo en las cuentas administrativas, para evitar que la cuenta se pueda bloquear desde fuera de la consola y que solamente lo haga desde la red. Cuando se ponga en práctica controles de bloqueo de cuenta, se deben seguir las siguientes normas.
- Bloqueo después de entre 7 y 10 intentos de registro fallidos para las cuentas administrativas y de acceso remoto.
- Bloqueo después de 10 intentos de registro fallidos para las cuentas de usuario estándar.
- Requerir la intervención de un administrador para desbloquear las cuentas de acceso remoto y de administrador, y para reactivar automáticamente las cuentas de usuarios estándar al cabo de 5 minutos.
- Las limitaciones para crear cuentas de administrador deben ser más estrictas que las que se aplican a las cuentas de usuarios normales.
- Establecer contraseñas de 14 caracteres alfanuméricos y especiales para las cuentas de administrador.

Directivas de contraseñas - Cuenta de usuario

· Poner en práctica las recomendaciones realizadas en la sub-categoría anterior, en donde se dan las pautas necesarias para el manejo de las contraseñas de las cuentas de usuario.

Directivas de contraseñas - Cuenta de acceso remoto

· Poner en práctica las recomendaciones realizadas en la sub-categoría: directivas de contraseñas, en donde se dan las pautas necesarias para el manejo de las contraseñas de las cuentas de acceso remoto.

6.7.1.3. Gestión y control

Creación segura

· Aplicar una directiva que solicite una revisión periódica de las configuraciones predeterminadas de los cortafuegos para tener en cuenta los cambios en las aplicaciones o los servicios utilizados.

· Implementar un proceso de creación documentado para los dispositivos de la infraestructura de red y asegurar que se mantiene la creación actualizada a medida que se publican nuevas actualizaciones.

· Utilizar software de cifrado de discos con el fin de no poner en peligro la confidencialidad de los datos en caso de robo del equipo.

· Continuar con la práctica de exigir a todos los usuarios que tengan un protector de pantalla protegido por contraseña con un tiempo de espera corto.

Seguridad física

· Continuar con los controles físicos y considerar la implementación de los controles a los equipos informáticos que aún no se hayan tomado en cuenta.

· Continuar con la utilización del sistema de alarma y comprobar periódicamente su funcionamiento para garantizar la protección de las instalaciones.

· Establecer controles de acceso físico como protección contra personas no autorizadas que acceden al edificio y a información confidencial.

· Considerar la posibilidad de volver a evaluar todos los controles de acceso físico para garantizar que son adecuados y que se cumplen.

· Continuar con la práctica de proteger los servidores en una habitación cerrada y asegúrese de que únicamente acceden las personas que cuentan con los respectivos permisos.

· El acceso físico se debe controlar estrictamente, evitando que las personas no autorizadas accedan a las instalaciones de la empresa, datos confidenciales y sistemas.

· Asegurar las estaciones de trabajo con cables de seguridad, para evitar posibles robos.

· Continuar con la práctica de asegurar los equipos portátiles mediante cables de seguridad.

· Guardar en armarios cerrados los documentos confidenciales, para que no resulten robados ni se revele información confidencial.

6.7.2. ÁREA: APLICACIONES

Tabla 35: Área de Aplicaciones

ÁREA	SECCIONES	SUB-SECCIONES
APLICACIONES	Implementación y uso de datos	Equilibrio de carga
		Clústeres
		Aplicación y recuperación de datos
		Fabricante de software Independiente
		Desarrollado internamente
		Vulnerabilidades
	Diseño de aplicaciones	Validación de datos de entrada
		Metodologías de

		desarrollo de seguridad de software
	Almacenamiento y comunicación de datos	Cifrado
		Cifrado - Algoritmo

Elaborado por: Los autores

6.7.2.1 Implementación y uso

Equilibrio de carga

· Utilizar equilibradores de carga en el entorno para asegurar una mayor disponibilidad de los servicios.

Clústeres

· Utilizar mecanismos de clúster para asegurar una disponibilidad alta de la bases de datos.

Aplicación y recuperación de datos

· Realizar pruebas periódicas de recuperación de aplicaciones y datos, para mejorar los tiempos de respuesta ante incidentes que necesiten actividades y procedimientos de recuperación.

· Al no tener ninguna aplicación de línea comercial de propósito crítico, la empresa se evita el riesgo de que tales sistemas fallen. Sin embargo, si se llega a utilizar alguna en el futuro, estas aplicaciones deberán evaluarse periódicamente para su seguridad, someterse a procesos regulares de copias de seguridad, documentarse a fondo y contar con planes de contingencia en caso de que se produzcan fallos.

· Realizar copias de seguridad regularmente. Probar cada cierto periodo de tiempo el mecanismo de copias de seguridad y recuperación que restaura la aplicación a un estado normal de operación.

Fabricante de software independiente

· Asegurarse de seguir disponiendo de servicio técnico y actualizaciones periódicas para el software clave de su empresa.

· Colaborar con el fabricante de aplicaciones para recibir actualizaciones y revisiones lo más frecuentemente posible. Probar completamente las actualizaciones que aparezcan en el entorno de laboratorio antes de utilizarla.

· La empresa debe conocer las configuraciones necesarias de las aplicaciones desarrolladas por terceros para garantizar un nivel de seguridad más alto.

Desarrollado internamente

· Dar permisos para desarrollar y ejecutar macros personalizadas sólo a quienes lo necesitan por alguna actividad relacionada con la empresa.

Vulnerabilidades

· Identificar y corregir todas las vulnerabilidades de seguridad conocidas.

· Visitar los sitios de los fabricantes y otros proveedores de soluciones de seguridad para buscar información sobre nuevas vulnerabilidades, así como las soluciones disponibles.

6.7.2.2. Diseño de aplicaciones

Validación de datos de entrada

· Utilizar mecanismos para las restricciones de validación de datos de entrada que permitan datos con sintaxis y semántica correctas y no sólo que efectúen únicamente el análisis para la detección de caracteres no válidos.

6.7.2.3. Almacenamiento y comunicación de datos

Cifrado

· Cifrar los datos confidenciales antes de transmitirlos a otros componentes de la red. Verificar que los componentes intermedios que controlan los datos en un formato de texto sin formato antes o después de la transmisión no representa una amenaza.

· Utilizar claves de 128 bits como mínimo para cifrar los datos. Algunos de los algoritmos de cifrado más fiables son: 3DES, AES, RSA, RC4 y Blowfish.

Cifrado - Algoritmo

· Actualizar el cifrado a 3DES o AES con el fin de dificultar en gran medida la intrusión por técnicas de fuerza bruta.

6.7.3 ÁREA: OPERACIONES

Tabla 36: Área de Operaciones

ÁREA	SECCIONES	SUB-SECCIONES
OPERACIONES	Entorno	Host de gestión de servidores
	Directiva de seguridad	Clasificación de datos
		Eliminación de datos
	Gestión de actualizaciones y revisión	Documentación de la red
		Flujo de datos de la aplicación
		Gestión de

		actualizaciones
		Gestión de cambios y configuración
	Copias de seguridad y recuperación	Planificación de recuperación ante desastres y reanudación del negocio

Elaborado por: Los Autores

6.7.3.1. Entorno

Host de gestión de servidores

· Utilizar un equipo de gestión dedicado a los servidores para comprobar que los servicios que ofrecen están disponibles y seguros.

6.7.3.2 Directiva de seguridad

Clasificación de datos

· Utilizar IPSec y SSL para todos los canales de comunicación de la empresa.

· Definir un esquema de clasificación de datos corporativos y proporcionar a todo el personal una guía y un proceso de capacitación adecuados acerca de la clasificación de datos. Es importante tener un esquema de clasificación de datos con las directrices de protección de datos correspondientes. Es posible que los recursos utilizados para asegurar la información también se asignen erróneamente sin la clasificación adecuada de la información. El personal debe conocer la información de la empresa que es confidencial y cómo se protegen estos datos, existe una alta probabilidad de que esta información quede expuesta a personas no autorizadas.

Eliminación de datos

· Definir e implementar procedimientos para la gestión y la eliminación de información en formato impreso y electrónico. Proporcionar a todos los usuarios dichos procedimientos para que los lean y los apliquen. La confidencialidad de la información se puede ver en peligro si no se proporcionan instrucciones y procesos para destruir la información de forma segura.

6.7.3.3 Gestiones de actualizaciones y revisión

Documentación de la red.

· Actualizar el diagrama de red de la empresa conforme se produzcan cambios en el mismo.

· Limitar el acceso al diagrama de red solo al personal de TI.

Flujo de datos de la aplicación

· Diseñar los diagramas de la arquitectura de las aplicaciones de tal manera que se muestren los principales componentes y los flujos de datos fundamentales del entorno, además de los sistemas por los que pasa el tráfico de información y cómo se gestionan estos datos.

· Crear una directiva para actualizar estos diagramas cuando el entorno se cambie.

Gestión de actualizaciones

· Desarrollar una directiva para actualizar periódicamente los sistemas operativos y todas las aplicaciones utilizando procesos adecuados.

· Aplicar actualizaciones de seguridad y cambios de configuración en intervalos periódicos indicados por las directivas de seguridad. Estas actualizaciones y revisiones se comprobarán exhaustivamente en un entorno de laboratorio antes de su instalación definitiva. Por otra parte, una vez instaladas, se

probarán cada uno de los sistemas para detectar conflictos exclusivos que podrían demandar desinstalar la actualización.

Gestión de cambios y configuración

· Poner en práctica un proceso formal de gestión para las configuraciones y los cambios para verificar y documentar todas las actualizaciones antes de su puesta en práctica. Guardar una documentación completa acerca de la configuración de todos los sistemas de producción.

6.7.3.4. Copias de seguridad y revisión

Planificación de recuperación ante desastres y reanudación de negocio

· Desarrollar, documentar, implementar y someter los planes de recuperación ante desastres a revisiones, pruebas y actualizaciones periódicas. Desarrollar planes de continuidad de negocio que incluyan personal, ubicaciones, así como sistemas y otras cuestiones de tecnología.

· Los planes de recuperación ante desastres y de reanudación de negocio deben estar bien documentados y actualizados para asegurar la recuperación en un período de tiempo aceptable.

· Los planes de continuidad de negocio se deben centrar en todo el entorno: físico, tecnológico y personal.

6.7.4. ÁREA: PERSONAL

Tabla 37: Área de Personal

ÁREA	SECCIONES	SUB-SECCIONES
	Requisitos y evaluación	Evaluación de seguridad

PERSONAL	Directiva y procedimiento	Directiva de recursos humanos
	Formación y conocimiento	Conocimiento de seguridad
		Formación sobre seguridad

Elaborado por: Los Autores

6.7.4.1. Requisitos y evaluaciones

Evaluaciones de seguridad

· Desarrollar un plan que solicite evaluaciones regulares realizadas por terceros para la infraestructura crítica de red y de las aplicaciones.

· Incluir los resultados de la presente evaluación en los proyectos de mejora.

· Realizar evaluaciones de seguridad frecuentes con el personal interno de TI de la empresa. Estas evaluaciones no deben centrarse exclusivamente en la identificación de vulnerabilidades, sino también en señalar configuraciones que no sean seguras o privilegios de acceso innecesarios.

6.7.4.2. Directiva y procedimientos

Directiva de recursos humanos

· Colaborar con el departamento de recursos humanos para desarrollar un procedimiento para los empleados que dejan la empresa de forma hostil.

· Revisar periódicamente el procedimiento para empleados que dejan la empresa amistosamente y analizar las lagunas que podrían existir.

· Los procedimientos para gestionar la situación de los empleados que dejan la empresa amistosamente y los que la dejan de forma hostil deben incluir:

· Notificación a todos los departamentos (Recursos humanos, TI, Seguridad física, Servicio de atención al cliente, Finanzas, etc.)

· Acompañamiento del empleado al abandonar las instalaciones.

· Cancelación de todas las cuentas del usuario y de su acceso a la red.

· Recuperación de todos los bienes de la empresa (portátiles, PDA, dispositivos electrónicos, documentos confidenciales, etc.)

6.7.4.3 Formación y conocimiento

Conocimiento de seguridad

· Poner en práctica un programa formal de divulgación de seguridad para que los empleados conozcan los riesgos relacionados con los recursos de TI. Un programa formal de divulgación de las medidas de seguridad ayuda a los empleados a contribuir a la seguridad global de la empresa, puesto que se los mantiene informados acerca de los riesgos existentes. La mejor garantía de alerta ante problemas potenciales es formar debidamente al personal en materia de seguridad. Un programa de divulgación efectivo debe tener en cuenta todos los aspectos de la seguridad (aplicaciones, redes y soportes físicos) y ofrecer también pautas claras a los empleados en caso de que detecten un riesgo para la seguridad de cualquiera de estos elementos.

· Desarrollar directivas que regulen la utilización de los recursos y las tecnologías corporativas por parte de los empleados e incluya un programa de divulgación de seguridad en el curso de orientación para nuevos empleados.

· Asegurar que la empresa cuenta con personal responsable de la seguridad y que antes de realizar cambios en el entorno informático se consulte primero con el dicho personal.

· Realizar comprobaciones periódicas para asegurarse de que los empleados han asimilado la información.

Formación sobre seguridad

· Desarrollar un plan para que el equipo de TI tenga una capacitación apropiada en seguridad. El plan debe incluir la asistencia de este personal a sesiones de formación como seminarios y foros específicos. Redactar el plan para que incluya cualquier tipo de curso básico para todos los empleados en el futuro.

BIBLIOGRAFÍA

Referencias

Alegsa, L. (n.d.). alegsa. Retrieved from http://www.alegsa.com.ar/Dic/sistema%20informatico.php

CATOIRA, F. (n.d.). welivesecurity. Retrieved from welivesecurity: http://www.welivesecurity.com/la-es/2012/07/24/penetration-test-en-que-consiste/

Jeimy J. Cano, P. C. (s.f.). Seguridad para todos. (L. Emergentes, Editor) Obtenido de http://www.seguridadparatodos.es/2011/10/seguridad-informatica-o-seguridad-de-la.html

Luis Gomez Fernandez, A. A. (n.d.). Guía de aplicación de la Norma UNE-ISO/IEC 27001 sobre seguridad en sistemas de información para pymes. In A. A. Luis Gomez Fernandez, Guía de aplicación de la Norma UNE-ISO/IEC 27001 sobre seguridad en sistemas de información para pymes.

Mifsud, E. (s.f.). recursostic. Obtenido de http://recursostic.educacion.es/observatorio/web/es/component/content/article/1040-introduccion-a-la-seguridad-informatica?start=1

Mifsud, E. (n.d.). recursostic. Retrieved from http://recursostic.educacion.es/observatorio/web/es/component/content/article/1040-introduccion-a-la-seguridad-informatica?start=3

Namakforoosh, M. N. (2005). Metodología de la investigación . Mexico: Limusa.

Roldan, C. S. (s.f.). codejobs. Obtenido de http://www.codejobs.biz/

Samuel. (n.d.). laseguridadinformatica. Retrieved from laseguridadinformatica: http://laseguridadinformatica.blogspot.com/2007/07/caractersticas-de-un-sistema-seguro.html

seguridadinformatica. (n.d.). seguridadinformatica. Retrieved from seguridadinformatica: http://www.seguridadinformatica.unlu.edu.ar/?q=node/12

seguridadpc. (n.d.). seguridadpc. Retrieved from seguridadpc: http://www.seguridadpc.net/conceptos.html

Tori, C. (s.f.). Hacking Etico. En C. Tori, Hacking Etico (págs. 12,41).

Wiley. (2012). Fundamentos de Seguridad. In Wiley, Fundamentos de Seguridad (p. 1).