ESCUELA POLITÉCNICA NACIONAL

FACULTAD DE INGENIERÍA DE SISTEMAS

DIAGNÓSTICO Y DISEÑO DE UN PLAN DE SEGURIDAD DE LA INFORMACIÓN EN LA EMPRESA MANPOWER

PROYECTO PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN SISTEMAS INFORMÁTICOS Y DE COMPUTACIÓN

HENRY GONZALO ACURIO FLORES
henry.acurio@gmail.com

DAVID PATRICIO ESTRELLA MELO
david_patriciom@hotmail.com

DIRECTOR: ENRIQUE MAFLA
mafla@epn.edu.ec

Quito, Junio de 2013

DECLARACIÓN

Nosotros, Henry Gonzalo Acurio Flores y David Patricio Estrella Melo, declaramos bajo juramento que el trabajo aquí descrito es de nuestra autoría; que no ha sido previamente presentada para ningún grado o calificación profesional; y, que hemos consultado las referencias bibliográficas que se incluyen en este documento.

A través de la presente declaración cedemos nuestros derechos de propiedad intelectual correspondientes a este trabajo, a la Escuela Politécnica Nacional, según lo establecido por la Ley de Propiedad Intelectual, por su Reglamento y por la normatividad institucional vigente.

Henry Gonzalo Acurio Flores

David Patricio Estrella Melo

CERTIFICACIÓN

Certifico que el presente trabajo fue desarrollado por Henry Gonzalo Acurio Flores y David Patricio Estrella Melo, bajo mi supervisión.

DR. Enrique Mafla

DIRECTOR DE PROYECTO

CONTENIDO

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

RESUMEN

Ante la necesidad de Manpower de proteger sus sistemas e información sensible, los autores del presente proyecto propusimos llevar a cabo una evaluación de riesgos y desarrollar un plan de mitigación de los mismos. Las metodologías escogidas para el proyecto fueron MSAT y OCTAVE –S, debido a que están basadas en las mejores prácticas de seguridad comúnmente aceptadas, es decir, en estándares como las normas ISO 17799 y NIST-800.x, y son diseñadas especialmente para empresas pequeñas.

El capítulo 1 es una introducción al proyecto. En este, definimos el problema y los objetivos que esperamos alcanzar, caracterizamos la empresa con el fin de conocer claramente los procesos, actividades e información que manejan, y describimos las metodologías escogidas.

El capítulo 2 contiene la evaluación y análisis de riesgos. En la primera parte de este capítulo realizamos la evaluación con MSAT utilizando el cuestionario que propone la herramienta, y analizamos los resultados obtenidos. En la segunda parte desarrollamos la fase 1 y 2 de OCTAVE –S, en donde identificamos la información de la empresa, creamos los perfiles de amenaza y examinamos la infraestructura computacional en relación con los activos críticos. Al final de este capítulo, comparamos los resultados obtenidos con ambas herramientas y sacamos conclusiones.

En el capítulo 3 diseñamos el plan de seguridad. En la primera parte de este capítulo presentamos el plan de seguridad con las recomendaciones que propone MSAT, resumido y adaptado por los autores del presente proyecto. En la segunda parte realizamos la fase 3 de la metodología OCTAVE-S, que corresponde a la identificación de las áreas más críticas y el diseño del plan de seguridad con las actividades de mitigación propuestas por la herramienta. Finalmente diseñamos un plan general con las recomendaciones y actividades de mitigación obtenidas con ambas metodologías, basándonos en la comparación de resultados realizada en el capítulo 2.

1. CAPÍTULO I: INTRODUCCIÓN

En el presente proyecto desarrollamos un plan de seguridad para la empresa Manpower. Un plan de seguridad constituye el documento básico que 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 Manpower, los autores del presente proyecto propusimos 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 17799 y NIST-800.x. Estas metodologías son diseñadas especialmente para instituciones con menos de 1000 empleados y cuya red de datos cuenta con recursos limitados.

En el capítulo 1 realizamos la caracterización de la empresa desde un punto de vista tecnológico, definimos el problema, los objetivos y el alcance de la evaluación, y describimos las metodologías que utilizaremos para realizar el diagnostico de seguridad.

En el capítulo 2 realizamos la evaluación de riesgos tanto con MSAT como con OCTAVE -S. Con la herramienta MSAT evaluamos las áreas de infraestructura, aplicaciones, operaciones y personal, con el fin de conocer los riesgos a los que se encuentra expuesta la empresa a nivel tecnológico.

Con la herramienta OCTAVE -S conformamos el equipo de análisis que consta de 4 personas, los mismos que realizaremos todas las fases, procesos, actividades y pasos que la herramienta propone. Desarrollamos la fase 1 que consta de los procesos S1 y S2. En el proceso S1 identificamos los activos de información y realizamos una evaluación de las prácticas de seguridad implementadas en la empresa. En el proceso S2 seleccionamos de entre los activos de información identificados en el proceso anterior aquellos que sean los más críticos e

identificamos los requerimientos de seguridad y las amenazas a cada uno de los activos críticos. A continuación desarrollamos la fase 2 que consta del proceso S3. En el proceso S3 examinamos la infraestructura computacional en relación con los activos críticos identificados, tomando en cuenta las diferentes rutas o accesos que existen a cada uno de los activos críticos. Analizamos los componentes que están relacionados con los activos críticos y realizamos una estimación del grado en el que la seguridad es considerada en los procesos de configuración y mantenimiento de los componentes de la red. Al final del capítulo realizamos un análisis comparativo de los resultados obtenidos con las herramientas MSAT y OCTAVE –S para verificar la concordancia de los resultados.

En el capítulo 3 diseñamos el plan de seguridad con las recomendaciones que propone MSAT para cada una de las áreas, y desarrollamos la fase 3 de OCTAVE –S que consta de los procesos S4 y S5. En el proceso S4 evaluamos el impacto de las amenazas a los activos críticos y establecemos criterios de evaluación de probabilidad que nos permite conocer la probabilidad de ocurrencia de una amenaza. En el proceso S5 se seleccionan las áreas que presentan mayores problemas y se desarrolla el plan de mitigación de riesgos, que contiene actividades de mitigación propuestas por la herramienta para cada una de las áreas seleccionadas. Al final del capítulo integramos los planes de seguridad de ambas herramientas con el fin de tener un plan de seguridad general.

1.1 CARACTERIZACIÓN DE LA EMPRESA

En este apartado realizamos la caracterización de la empresa y del sistema de información de Manpower. Describimos la topología actual de la red y las aplicaciones utilizadas en la empresa.

1.1.1 CARACTERIZACIÓN DE MANPOWER DESDE UN PUNTO DE VISTA TECNOLÓGICO

Caracterizamos la empresa con el objetivo de conocer los procesos de negocio delicados, y su información sensible. Esta información nos ayudara 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 y Tesorería y caja, y Gerencia Operaciones y Administración con sus sub-áreas: Operaciones, Administración y Sistemas.

Los servicios que ofrece Manpower están destinados a vincular ofertas y demandas de empleo. En este contexto la empresa evalúa a los candidatos y los ubica en un puesto de trabajo (que otras empresas necesitan) de acuerdo a sus conocimientos y habilidades.

Las aplicaciones más importantes que utiliza en sus procesos de negocio son, el sistemas gestor, la intranet, correo electrónico, y la página web. La empresa a través de su página web recoge las hojas de vida de los aspirantes y provee toda la información necesaria para acceder a sus servicios. El servidor de la página web se aloja y mantiene en el exterior, por lo que no será motivo de análisis en el presente proyecto.

Para evaluar las aptitudes de los candidatos, estos deben llenar diferentes tests dependiendo del puesto al que aspiran. Las aplicaciones que se usan para evaluar las aptitudes de los postulantes son DirectQuizz, Career Harmony JPPI (JobPerformancePersonalityInventory), entre otras, y solo se manejan en sucursales de Manpower en el extranjero. Los test se envían a través de la intranet, para que sean procesados, y se devuelvan los resultados. Además la intranet se la usa también para acceder a información y aplicaciones que la empresa almacena en los diferentes servidores alrededor del mundo.

Según los documentos de políticas y procedimientos con los que cuenta la empresa, los activos más importantes que forman parte de la infraestructura de red interna de Manpower son el Sistema Gestor, Servidor de BDD y Servidor de Correo.

El Sistema Gestor es un ERP multiusuario que automatizan los procesos de negocio de Manpower y permite la obtención de información necesaria para la gestión empresarial y la toma de decisiones. La gestión de la base de datos se la realiza a través de Oracle 6i. Para la administración del Servidor de Correo Electrónico se utilizan los programas dovecot, mailscanner y sendmail, y como cliente de correo electrónico se usa Outlook el cual está instalado en todas las estaciones de trabajo de Manpower.

El Servidor de BDD almacena la información que se procesa en el Sistema Gestor, que se considera sensible ya que es información delicada como la contabilidad de la empresa. Además, guarda las fichas de los postulantes que se considera crítica, debido a que Manpower asegura a sus clientes que su información solo puede ser usada para el proceso de selección. 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 MANPOWER

En este apartado presentamos el diagrama y la descripción de la red de la sucursal de Quito que forma parte de una red global de Manpower. Adicionalmente, describimos las herramientas y aplicaciones más importantes que usa la empresa en sus procesos de negocio, para poder brindar los servicios a sus clientes.

1.1.2.1 TOPOLOGÍA DE LA RED

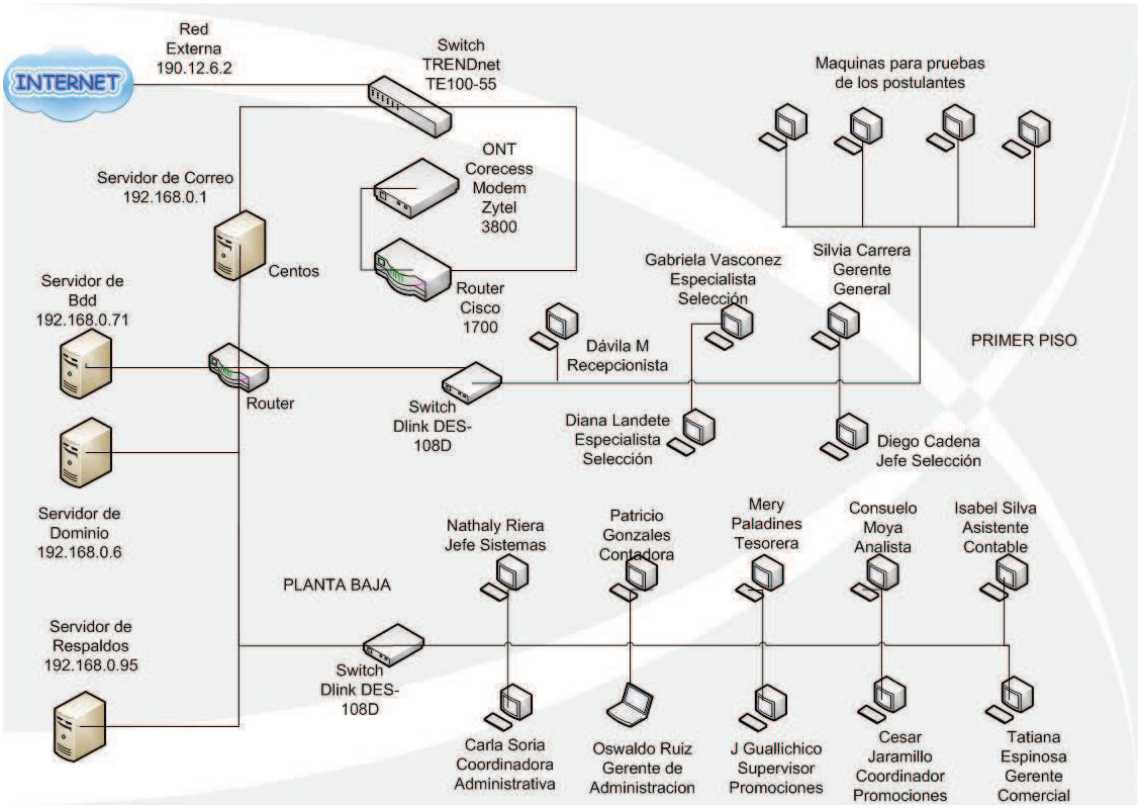

Figura 1.1: Topología actual de la red de información de la empresa Manpower.

La topología actual de red de Manpower es de Tipo Mixta (Estrella y Bus). Como se puede ver en la figura 1.1, 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 ONT Corecess 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 5. En cuanto al software, todas las estaciones de trabajo tienen instalado Windows XP. La información de cada uno de los servidores se encuentra en la tabla 1.1 que se muestra a continuación.

Servidor	Procesador	Velocidad(Ghz)	RAM	SO	Disco
BDD	Intel Xeon	36	4 GB	W Server 2003	500 GB
Correo	Core 2 duo	2,6	4 GB	Centos	500 GB
Respaldo	Pentium III	1,26	1,25 GB	W Server 2003	50 GB
Dominio	Pentium III	1,2	1,25 GB	W Server 2003	40 GB

Tabla 1.1: Datos Servidores de Manpower.

1.1.2.2 HERRAMIENTAS Y APLICACIONES UTILIZADAS EN MANPOWER

En este apartado presentamos una breve descripción de las herramientas y aplicaciones que utiliza Manpower 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 de Manpower.

El Gerente de Operaciones y Administración es el encargado de crear los usuarios y proporcionar los permisos adecuados para cada miembro del personal.

Una de las principales actividades que se realiza en la intranet es la de acceder a los test de evaluación que se les aplica a los postulantes, los mismos que son enviados al exterior donde son procesados, y cuyos resultados son devueltos por el mismo medio.

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 Gestor: El Sistema Gestor es un ERP (Sistema de Gestión Empresarial) multiusuario que consta de 7 módulos, que automatizan los procesos de negocio de Manpower y permite la obtención de información necesaria para la Gestión Empresarial y la toma de decisiones.

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

- Facturación
- Nómina y Personal
- Contabilidad
- Parametrización
- Herramientas
- Proveedores
- Caja Bancos

A continuación se hace una descripción de cada módulo del Sistema Gestor.

Facturación: En este módulo se puede gestionar la información de todos los clientes, por ejemplo ver el estado de cuenta del cliente. Además permite emitir informes de los saldos, cuentas, etc.

Nómina y Personal: En este módulo se registra el ingreso o salida de un miembro del personal, así como las novedades que puedan tener cada uno de ellos. Se mantiene un histórico (entrada, sueldo, salida, anticipos, préstamos, etc) de cada empleado. Adicionalmente en este módulo se generan reportes de sueldos, decimos y aportes al IESS.

Contabilidad: Este módulo reúne la información de todos los módulos, para generar los asientos de todos los movimientos, y a través de estos producir los balances mensuales. Además maneja el centro de costos, que en términos generales ayuda a determinar si un proyecto es o no rentable.

Parametrización: Dentro de este módulo se maneja los permisos de cada usuario que utiliza el sistema. Aquí se determina las formas de pago y cobranzas, la definición de impuestos y retenciones, tipos de identificación, árbol de distribución,

el modelo de los asientos y como van atados los asientos contables del módulo facturación al módulo contabilidad.

Herramientas: Este módulo permite definir las impresoras a utilizarse, la configuración de routers y la definición de formas.

Proveedores: Maneja el estado de la cuenta, el registro de facturas de los proveedores, e información que va al SRI como por ejemplo el RUC.

Caja Bancos: Aquí se gestionan los comprobantes de ingreso, egreso y movimientos a bancos. También se revisa los estados de las cuentas, se realiza la emisión de cheques y la autorización de numeración de emisión de cheques.

El Sistema Gestor no cuenta con un módulo de inventarios ya que la empresa es pequeña y los activos con los que cuenta no son demasiados.

Outlook: Esta aplicación es un cliente de correo electrónico de Microsoft. Se encuentra instalado en todas las computadoras de Manpower porque es un medio importante de comunicación interna y externa.

Herramientas ofimática: En Manpower los miembros de personal utilizan Microsoft Word y Excel 2007 para realizar sus tareas e informes.

1.2 DEFINICIÓN DEL PROBLEMA

Manpower maneja información sensible de los solicitantes, que recibe vía internet a través de una ficha. Esta información es considerada crítica ya que Manpower asegura a sus clientes que sus datos solo pueden ser utilizados para los procesos de selección.

Los datos de los proveedores y clientes, y la información financiera de la empresa también son considerados críticos. Estos se gestionan a través de la aplicación gestor y se almacenan en el servidor de base de datos.

Tomando en cuenta incidentes recientes que ha sufrido la empresa, Manpower considera que los procesos y actividades actuales de seguridad no son suficientes, y tanto la información sensible como las herramientas que las gestionan se encuentran expuestas a posibles ataques tanto internos como externos.

Debido a esto, la empresa Manpower bajo la dirección del Gerente de Operaciones y Administración, considera la necesidad de una revisión global de la seguridad de la información dentro de sus instalaciones.

Frente a estos requerimientos, los autores del presente proyecto de titulación, propusimos aplicar las metodologías MSAT y OCTAVE -S para diagnosticar los riesgos a los que se encuentran expuestos los datos sensibles y diseñar un plan de seguridad de la información adecuado.

1.3 DEFINICIÓN DEL OBJETIVO

1.3.1 OBJETIVO GENERAL

El objetivo del presente proyecto de titulación es diagnosticar y diseñar un plan de seguridad de la información para la empresa Manpower y de esta manera mejorar y desarrollar nuevos procesos de protección de sus activos de información.

1.3.2 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 Manpower.
- 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 Manpower.
- Analizar los resultados obtenidos en las evaluaciones con el fin de encontrar las causas de los problemas y proponer actividades de mitigación.
- Comparar los resultados obtenidos con las herramientas MSAT y OCTAVE –S con el fin de determinar si tienen concordancia las evaluaciones realizadas.

- Elaborar un plan de seguridad para la información de la empresa que es objeto de estudio.

1.4 ALCANCE DE LA EVALUACIÓN

El presente análisis y evaluación de la seguridad de la información se limita a la red interna de Manpower. Las recomendaciones y actividades de mitigación del plan de seguridad serán solo propuestas, queda a consideración de la empresa su implementación en futuros proyectos.

1.5 DESCRIPCIÓN DE LAS METODOLOGÍAS Y HERRAMIENTAS

Se ha escogido MSAT por las siguientes razones que justifican su aplicación en la empresa Manpower

- La Herramienta de Evaluación de Seguridad de Microsoft (MSAT) es una herramienta gratuita diseñada para ayudar a las empresas que tienen menos de 1.000 empleados a evaluar los puntos débiles que tienen en su entorno de seguridad de TI.
- La herramienta está diseñada para ayudar a la organización a identificar y abordar los riesgos de seguridad en su entorno de TI, utiliza un enfoque integral para medir el nivel de seguridad y cubre aspectos tales como usuarios, procesos y tecnología.
- Las preguntas del cuestionario, herramientas, respuestas asociadas y recomendaciones se obtienen a partir de las mejores prácticas de seguridad comúnmente aceptadas, estándares tales como las normas ISO 17799 y NIST-800.x, así como las recomendaciones y orientaciones normativas del Grupo Trustworthy Computing de Microsoft y otras fuentes externas de seguridad.

Se ha escogido OCTAVE -S por las siguientes razones que justifican su aplicación en la empresa Manpower

- OCTAVE -S fue desarrollado para organizaciones pequeñas con alrededor de 100 personas o menos.

- Resume la mayoría de las normas y regulaciones sobre seguridad de información internacionales como la ISO 17799 y NIST.
- Es auto dirigido, ya que recurre al personal de la organización, quienes conocen los problemas que tiene la misma, y pueden enfocar el análisis en los puntos más críticos, con el fin de no desperdiciar recursos ni tiempo en estudios innecesarios y costosos.
- Es una metodología de evaluación integral, que considera el mayor número posible de factores que intervienen en la seguridad.
- OCTAVE -S toma en cuenta los elementos tecnológicos de la seguridad, en relación con la organización, y sus puntos más débiles o vulnerables se los evalúa en relación con los demás factores que afectan la seguridad de la información.

1.5.1 DESCRIPCIÓN DE MSAT (HERRAMIENTA DE EVALUACIÓN DE SEGURIDAD DE MICROSOFT)[1]

La Herramienta de Evaluación de Seguridad de Microsoft (MSAT) es una herramienta gratuita diseñada para ayudar a las empresas que tienen menos de 1.000 empleados a evaluar los puntos débiles que tienen en su entorno de seguridad de TI. Consta de un listado de cuestiones ordenadas por prioridad y orientación específica para minimizar los riesgos.

La herramienta está diseñada para ayudar a la organización a identificar y abordar los riesgos de seguridad en su entorno de TI, utiliza un enfoque integral para medir el nivel de seguridad y cubre aspectos tales como usuarios, procesos y tecnología.

Sus conclusiones incluyen orientaciones y recomendaciones para mitigar los esfuerzos, información de cómo las herramientas y métodos específicos le pueden ayudar a mejorar la situación de seguridad con la que cuenta la empresa, y proporciona enlaces a información adicional sobre cuestiones propias del sector en caso de ser necesario.

[1] http://technet.microsoft.com/es-es/security/cc185712

La evaluación se compone de 200 preguntas distribuidas en cuatro categorías:

- Infraestructura
- Aplicaciones
- Operaciones
- Personal

Infraestructura[2]

La seguridad de la infraestructura se enfoca en cómo debe funcionar la red, cómo se implementan y utilizan las estaciones de trabajo y los hosts de gestión y cómo se administra y mantiene la red. La seguridad de la infraestructura puede ayudar a mejorar significativamente la defensa de la red, las gestiones frente a los incidentes, la disponibilidad de la red y el análisis de fallos. Al establecer un diseño de la infraestructura que todos puedan comprender, se podrá identificar áreas de riesgo y desarrollar métodos para reducir las amenazas. La presente evaluación en esta categoría revisa los procedimientos de alto nivel que la empresa puede seguir para ayudar a mitigar el riesgo para la infraestructura enfocándose en las áreas de seguridad de la infraestructura que se presentan a continuación:

- 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.

Aplicaciones[3]

Para poder empezar a identificar las posibles amenazas es necesaria una comprensión total de la seguridad de las aplicaciones, y un conocimiento profundo de la arquitectura de las aplicaciones subyacentes básicas, así como de un conocimiento sólido de la base de la aplicación del usuario. El objetivo de esta evaluación consiste en revisar las aplicaciones de la empresa y valorarlas desde un punto de vista de la seguridad y disponibilidad. Examina las tecnologías utilizadas en el entorno para contribuir a mejorar la defensa en profundidad. La

[2] Esta información está basada en el informe completo que entrega MSAT, Anexo B.
[3] Esta información está basada en el informe completo que entrega MSAT, Anexo B.

revisión de los procedimientos de alto nivel ayudará a mitigar los riesgos para la infraestructura centrándose en las siguientes áreas de seguridad:

- Utilización y uso — mecanismos para mejorar la disponibilidad.
- Diseño de aplicaciones — autenticación, control de acceso, gestión de actualizaciones, validación de datos de entrada, registros y auditorías.
- Almacenamiento y comunicaciones de datos — cifrado, transferencia de datos, acceso restrictivo.

Operaciones[4]

En esta área de análisis se examina las prácticas, procedimientos y pautas operativas que sigue la empresa para ayudar a mejorar la defensa en profundidad. Esta evaluación analiza directivas y procedimientos que regulan la implementación de sistemas, la documentación de la red y el uso de tecnología en el entorno empresarial. Adicionalmente incluye actividades de apoyo necesarias para gestionar la información y los procedimientos que utilizan los administradores y el equipo de operaciones en el entorno. Para que la empresa tenga la posibilidad de mejorar su defensa en profundidad es necesario establecer prácticas, procedimientos y pautas operativas que se entiendan y que se sigan. La evaluación revisa los procedimientos de alto nivel que la empresa puede seguir para ayudarle a mitigar los riesgos para la infraestructura centrándose en las siguientes áreas de seguridad de las operaciones:

- Entorno — documentación de la red, flujo de datos de aplicación, arquitectura de las aplicaciones
- Directiva de seguridad — protocolos y servicios, uso aceptable, gestión de cuentas de usuarios
- Actualizaciones y gestión de actualizaciones — gestión de actualizaciones, firmas de virus
- Copias de seguridad y recuperación — copias de seguridad, almacenamiento, pruebas.

[4] Esta información está basada en el informe completo que entrega MSAT, Anexo B.

Personal[5]

Los esfuerzos de seguridad en una empresa a menudo pasan por alto los aspectos que son críticos para la ayuda del mantenimiento de la seguridad general en la empresa. Esta sección de la evaluación revisa aquellos procesos de la empresa que regulan las directivas de seguridad corporativa, los procesos de recursos humanos, así como la capacitación y divulgación de materias de seguridad para los empleados. El área de análisis de personal también se centra en la seguridad, ya que relaciona las tareas diarias operativas y las definiciones de los roles. La evaluación revisa los procedimientos de alto nivel que una empresa puede seguir para ayudarle a mitigar los riesgos del personal centrándose en las siguientes áreas de la seguridad del personal:

- Requisitos y evaluaciones—planificación, evaluaciones de terceros
- Directiva y procedimientos—directiva de RR.HH., relaciones con terceros
- Formación y conocimiento—divulgación de las medidas de seguridad

Las preguntas del cuestionario, herramientas, respuestas asociadas y recomendaciones se obtienen a partir de las mejores prácticas de seguridad comúnmente aceptadas, tanto de manera general como específica, estándares tales como las normas ISO 17799 y NIST-800.x, así como las recomendaciones y orientaciones normativas del Grupo Trustworthy Computing de Microsoft y otras fuentes externas de seguridad.

1.5.2 DESCRIPCIÓN DE OCTAVE –S[6]

OCTAVE -S es una variante de OCTAVE y fue desarrollada para responder a las necesidades de pequeñas empresas con menos de 100 personas.

Antes de empezar a utilizar OCTAVE -S es necesario tener en cuenta los siguientes aspectos.

1. OCTAVE -S requiere un equipo de análisis interdisciplinario de 3 a 5 personas quienes deben tener una amplia visión de los procesos de negocio de la organización para poder llevar a cabo todas las actividades de OCTAVE -S.

[5] Esta información está basada en el informe completo que entrega MSAT, Anexo B.
[6] OCTAVE®-S Implementation Guide, Version 1.0, Vol 1, página 3-4.

2. OCTAVE -S incluye una exploración limitada de la infraestructura informática. Generalmente las pequeñas empresas externalizan sus tecnologías de información y no tienen la capacidad de utilizar e interpretar los resultados de las herramientas de evaluación de vulnerabilidades. Sin embargo esta falta de capacidad no impiden a una organización establecer estrategias de protección. Una empresa que realiza una evaluación con OCTAVE -S analiza los procesos utilizados para configurar y mantener la infraestructura informática.

1.5.2.1 El proceso de OCTAVE –S[7]

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.

Como se puede observar en la figura 1.2 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.

[7] OCTAVE®-S Implementation Guide, Version 1.0, Vol 1, página 5.

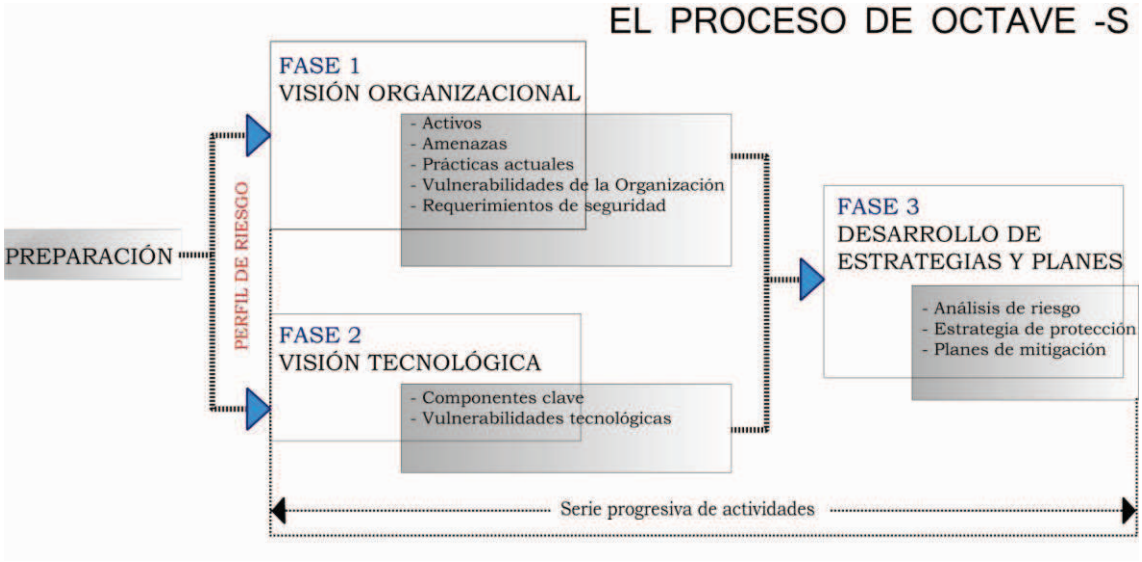

Figura 1.2: El proceso de OCTAVE –S[8].

1.5.2.2 Fases de OCTAVE –S[9]

Como mencionamos 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.

1.5.2.2.1 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.

1.5.2.2.2 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

[8] ALBERTS, Christopher, DOROFEE, Audrey, STEVENS, James, WOODY, Carol, "introducción al enfoque OCTAVE-S", Programa de supervivencia de sistemas en red, Carnegie MellonUniversity, Software EngineeringInstitute, Pittsburgh, PA, Agosto 2003, página 5.
[9] OCTAVE®-S Implementation Guide, Version 1.0, Vol 1, página 5-8.

análisis recolecta toda la información necesaria y completa todas las tareas. Posteriormente se seleccionan de tres a cinco activos de información críticos, basados en la importancia que estos representan para la organización y los cuales se analizarán 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.

La tabla 1.2 muestra con detalle los procesos, actividades y pasos de la fase 1.

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

Tabla 1.2: Procesos, actividades y pasos de la fase 1, Metodología OCTAVE –S.[10]

[10] Fuente: OCTAVE®-S Implementation Guide, Version 1.0, página 6.

1.5.2.2.3 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.

La tabla 1.3 muestra con detalle los procesos, actividades y pasos de la fase 2.

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

Tabla 1.3: Procesos, actividades y pasos de la fase 2, Metodología OCTAVE –S.[11]

1.5.2.2.4 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.

[11] Fuente: OCTAVE®-S Implementation Guide, Version 1.0, página 6.

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.

La tabla 1.4 muestra con detalle los procesos, actividades y pasos de la fase 3.

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

Tabla 1.4: Procesos, actividades y pasos de la fase 3, Metodología OCTAVE –S.[12]

1.5.2.2.5 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.

[12] Fuente: OCTAVE®-S Implementation Guide, Version 1.0, página 7.

- 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, obtendremos como resultado información útil para mejorar la postura de la seguridad de la empresa.

2. CAPÍTULO II: EVALUACIÓN DE RIESGOS

En este capítulo determinamos los potenciales riesgos a los que puede estar expuesta la red de la empresa Manpower, utilizando las herramientas MSAT y OCTAVE -S descritas en el capítulo 1. Con MSAT analizamos los resultados obtenidos en base a las respuestas del cuestionario que propone la herramienta. Con OCTAVE –S desarrollamos las fases 1 y 2 de la metodología, que consta de los pasos 1 al 21. Al final del capítulo realizamos un análisis comparativo de los resultados obtenidos con ambas herramientas.

Para el proceso de evaluación tanto con la herramienta MSAT como con OCTAVE -S, conformamos un equipo de análisis cuyos miembros son: Los desarrolladores del presente proyecto de titulación, el Gerente de Operaciones y Administración y la Administradora de Sistemas. Después de varias reuniones, llenamos el cuestionario que propone MSAT y procesamos los resultados entregados por la herramienta.

Realizamos un análisis del perfil de riesgos de la empresa versus el índice de defensa en profundidad y de cada una de las áreas que considera MSAT (Infraestructura, Aplicaciones, Operaciones y Personal). Todas las áreas están divididas en secciones. Para cada sección presentamos un cuadro de las sub-secciones y el estado del nivel de seguridad de cada una, y otro cuadro con los resultados que entrega MSAT. A continuación realizamos el análisis únicamente de las sub-secciones que según la metodología presentan problemas de seguridad, posteriormente un análisis para cada área y al final un análisis general de la evaluación realizada con MSAT.

En la segunda parte, desarrollamos las 2 primeras fases de OCTAVE -S que abarca los procesos S1, S2 y S3 descritos en la metodología de OCTAVE -S.

Para el proceso S1 identificamos los activos de información que posee la empresa. Realizamos una evaluación de las prácticas de seguridad implementadas en la empresa. En el proceso S2, seleccionamos de entre los activos de información identificados en el proceso anterior aquellos que sean los más críticos para la empresa. Identificamos los requerimientos de seguridad y las amenazas a cada uno de los activos críticos.

En el proceso S3 examinamos la infraestructura computacional en relación con los activos críticos identificados, tomando en cuenta las diferentes rutas o accesos que existen a cada uno de los activos críticos. Analizamos los componentes que están relacionados con los activos críticos, y realizamos una estimación del grado en el que la seguridad es considerada en los procesos de configuración y mantenimiento de los componentes de la red.

Al final realizamos un análisis comparativo de los resultados obtenidos con ambas herramientas, para verificar las concordancias y discrepancias de los resultados, y concluir cuales son los acertados.

Los procesos anteriormente mencionados nos ayudan a conocer las debilidades en la infraestructura de red de la empresa, y todos los posibles escenarios en los que la información de la empresa se pueda ver comprometida, y así se podrán tomar los correctivos necesarios estableciendo las políticas y procedimientos para cerrar dichas brechas de seguridad.

2.1 EVALUACIÓN DE RIESGOS CON MSAT[13]

Mediante la evaluación con MSAT se pueden determinar los riesgos a los que se enfrenta el entorno de TI de Manpower, 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 y Personal.

[13] Esta información está basada en el informe completo que entrega MSAT, Anexo B.

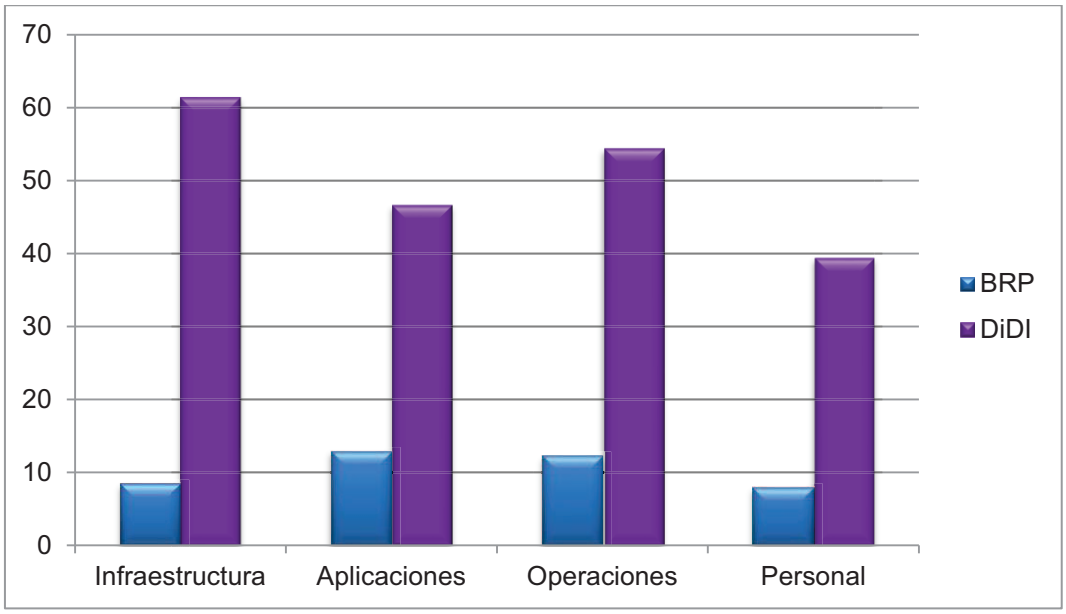

Figura 2.1: Perfil de riesgos para la empresa vs Índice de defensa en profundidad.[14]

En la figura 2.1, dividida en las cuatro áreas de análisis, se muestran las diferencias en el resultado de la defensa en profundidad.

BRP representa el riesgo al que está expuesta la empresa, 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 cuantifica la estrategia global que se utiliza para defender el entorno. Según las mejores prácticas se considera adecuado tener un DiDI y un BRP del mismo nivel.

Como podemos apreciar en la figura, podemos concluir que Manpower adopta medidas de seguridad demasiado altas para proteger su información en relación a los riesgos a la que esta se encuentra sometida, por lo que se están desperdiciando capital, y recursos tecnológicos y humanos que podrían ser destinados a otras tareas.

[14] Figura extraída del informe completo de MSAT, Anexo B, página 3.

2.2 RESULTADOS OBTENIDOS DE LA EVALUACIÓN CON MSAT

Luego de la evaluación se obtuvieron los siguientes resultados:

Leyenda:	● Cumple las mejores prácticas recomendadas	● Necesita mejorar	● Carencias severas

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

Tabla 2.1: Resultados de la evaluación realizada con la herramienta MSAT.[15]

2.2.1 INFRAESTRUCTURA

El área de infraestructura cuenta con las siguientes secciones:

- Defensa del perímetro
- Autenticación
- Gestión y control

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

2.2.1.1 Defensa del perímetro

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

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

INFRAESTRUCTURA	●
Defensa del perímetro	●
Reglas y filtros de cortafuegos	●
Antivirus	●

[15] Tabla extraída del informe completo de MSAT, Anexo B, página 3.

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

Resultados:

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)	Utiliza un sistema de detección de intrusiones basado en red (NIDS) No utiliza ningún sistema de detección de intrusiones basado en host (HIDS)
Inalámbrico	No existe la opción de conexión inalámbrica a su red

Tabla 2.2: Riesgos encontrados en la Defensa del perímetro.[16]

Existen empleados y/o socios que se conectan remotamente a la red interna, pero no utiliza ninguna tecnología VPN para permitirles un acceso seguro. Esto pone en riesgo a 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 trafico especifico se encamine a los servidores de las aplicaciones, y a los puertos para dar servicio a los usuarios. Sin embargo no se ofrece ningún servicio a los clientes a través de la red de Manpower Ecuador, y el tráfico dentro

[16] Tabla extraída del informe completo de MSAT, Anexo B, páginas 8-13.

de la red no es demasiado alto, por lo que no sería un requerimiento altamente necesario.

La empresa utiliza un sistema de detección de intrusiones basado en red (NIDS). Estos permitirán detectar anomalías que inicien un riesgo potencial tales como ataques de denegación de servicio, escaneadores de puertos, o intentos de entrar en un ordenador, analizando el tráfico en la red en tiempo real. Pero no cuenta con un sistema de detección de intrusos basado en Host, para detectar anomalías que indiquen un riesgo potencial, revisando las actividades en la máquina (host).

2.2.1.2 Autenticación

Los procedimientos estrictos 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.

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

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	🟢

Resultados:

Usuarios administrativos	Los usuarios tienen habilitados accesos administrativos a sus estaciones de trabajo. Sólo se requiere autenticación de contraseñas complejas para el acceso administrativo a dispositivos y hosts.
Usuarios de acceso remoto	Los empleados pueden conectarse a la red de forma remota, no los contratistas, ni terceros usuarios. Se requiere sólo autenticación de contraseñas complejas para el acceso remoto a la red interna y a los hosts.
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

Tabla 2.3: Riesgos encontrados en la Autenticación.[17]

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.

2.2.1.3 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.

[17] Tabla extraída del informe completo de MSAT, Anexo B, páginas 13-21.

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

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

Resultados:

Creación segura	No se han instalado cortafuegos particulares en todas las estaciones de trabajo del entorno. No utiliza ningún software de cifrado de discos en el entorno. No se utilizan módems en el entorno.
Seguridad física	No están implementadas tarjetas de identificación para empleados y visitantes, acompañantes de visitantes, registros de visitantes, ni controles de entrada. Las estaciones de trabajo no están protegidas con cables de seguridad. Los materiales impresos confidenciales no se almacenan en armarios con llave.

Tabla 2.4: Riesgos encontrados en la Gestión y Control.[18]

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.

El mismo problema se tiene por no almacenar la información sensible impresa en armarios con llave, ya que cualquier persona no autorizada puede tener acceso a la misma.

[18] Tabla extraída del informe completo de MSAT, Anexo B, páginas 21-29.

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.

2.2.1.4 Análisis general área infraestructura

Para el área de infraestructura, analizamos de 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 presentamos un resumen de los problemas que consideramos 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.

2.2.2 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.

2.2.2.1 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.

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

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

Resultados:

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 se utiliza macros personalizadas en las aplicaciones ofimáticas.
Vulnerabilidades	No existen procedimientos que aborden los aspectos de las vulnerabilidades de la seguridad conocidos.

Tabla 2.5: Riesgos encontrados en Implementación y uso.[19]

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 Manpower.

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 las fichas de los solicitantes como los datos de la gestión financiera.

No se realizan 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 manejan 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

[19] Tabla extraída del informe completo de MSAT, Anexo B, páginas 30-35.

el personal de TI de la organización no conoce las configuraciones necesarias, no garantiza un nivel de seguridad alto.

En la empresa utilizan 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 Manpower, pero no existe un procedimiento formal para hacer frente a dichas vulnerabilidades y esto representa un riesgo potencial.

2.2.2.2 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.

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

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	🔴

Resultados:

Validación de datos de entrada	No se validan los datos de entrada de las aplicaciones de cliente. No se validan 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.

Tabla 2.6: Riesgos encontrados en Diseño de aplicaciones.[20]

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.

2.2.2.3 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.

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

[20] Tabla extraída del informe completo de MSAT, Anexo B, páginas 35-40.

Almacenamiento y comunicaciones de datos	●
Cifrado	●
Cifrado - Algoritmo	●

Resultados:

Cifrado	Las aplicaciones principales del entorno cifran los datos confidenciales antes de transmitirlos. Las aplicaciones principales del entorno cifran los datos confidenciales cuando están almacenados.
Cifrado - Algoritmo	En la empresa se utiliza cifrado DES.

Tabla 2.7: Riesgos encontrados en Almacenamiento y Comunicación de Datos.[21]

La empresa Manpower 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.

2.2.2.4 Análisis general área aplicaciones

Para el Área de Aplicaciones, analizamos de 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 presentamos un resumen de los problemas que consideramos más graves dentro de esta área:

[21] Tabla extraída del informe completo de MSAT, Anexo B, páginas 40-41.

No se asegura una alta disponibilidad de los servicios ofrecidos por Manpower 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.

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

Manpower 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.

2.2.3 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 serán analizadas de acuerdo a los resultados obtenidos.

2.2.3.1 Entorno

La seguridad de Manpower 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.

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

OPERACIONES	●
Entorno	●
Host de gestión	●
Host de gestión-Servidores	●
Host de gestión - Dispositivos de red	●

Resultados:

Host de gestión-servidores.	No existe ningún equipo de gestión dedicado a los servidores.

Tabla 2.8: Riesgos encontrados en Entorno.[22]

En Manpower 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.

2.2.3.2 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 analizaran únicamente las sub-secciones en donde se encontraron riesgos:

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

[22] Tabla extraída del informe completo de MSAT, Anexo B, páginas 41-42.

Resultados:

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.

Tabla 2.9: Riesgos encontrados en Directivas de Seguridad.[23]

Manpower no dispone de un esquema de clasificación de datos, esta vulnerabilidad puede permitir que personal no autorizado tenga acceso a información confidencial de la empresa y puede suponer la pérdida de la imagen de Manpower, 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.

Manpower 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.

2.2.3.3 Gestión de actualizaciones y revisiones

Manpower 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.

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

[23] Tabla extraída del informe completo de MSAT, Anexo B, páginas 42-46.

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

Resultados:

Documentación de la red.	No existen diagramas lógicos de red en el entorno de la empresa.
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.

Tabla 2.10: Riesgos encontrados en Gestión de Actualizaciones y Revisiones.[24]

Manpower 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 Manpower, 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.

Manpower 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

[24] Tabla extraída del informe completo de MSAT, Anexo B, página 46-48.

configuración deben realizarse pruebas de verificación de compatibilidad antes de ponerlo en producción.

2.2.3.4 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.

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

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	●

Resultados:

Planificación de recuperación ante desastres y reanudación de negocio.	La empresa mantiene procedimientos para la recuperación ante desastres y reanudación de negocio. Los registros se revisan según sea necesario.

Tabla 2.11: Riesgos encontrados en Copias de seguridad y recuperación.[25]

Manpower cuenta con políticas para la recuperación ante desastres y reanudación de los procesos de negocio, sin embargo dichas políticas no han sido revisadas y actualizadas, y tampoco se realizan pruebas periódicas para asegurar la recuperación en un periodo de tiempo aceptable ante incidentes graves.

[25] Tabla extraída del informe completo de MSAT, Anexo B, página 49-52.

La empresa revisa los registros en busca de actividades sospechosas una vez a la semana, sin embargo no cuenta con procedimientos formales para realizar dicha actividad.

2.2.3.5 Análisis General Área Operaciones

Para el Área de Operaciones, analizamos de 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 presentamos un resumen de los problemas que consideramos más graves dentro de esta área:

Manpower 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**.**

2.2.4 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 serán analizadas de acuerdo a los resultados obtenidos.

2.2.4.1 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.

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

PERSONAL	●
Requisitos y evaluaciones	●
Requisitos de seguridad	●
Evaluaciones de seguridad	●

Resultados:

Evaluaciones de seguridad	No se encarga a empresas independientes la evaluación de los medios de seguridad. Las evaluaciones de la seguridad de su empresa no las realiza personal interno.

Tabla 2.12: Riesgos encontrados en Requisitos y evaluación.[26]

Las evaluaciones de seguridad deben ser aplicadas por personal interno y empresas independientes, lo que ayudara 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.

2.2.4.2 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:

[26] Tabla extraída del informe completo de MSAT, Anexo B, páginas 53-54.

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

Resultados:

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

Tabla 2.13: Riesgos encontrados en Directiva y procedimientos.[27]

No existe ninguna 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.

2.2.4.3 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.

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

Formación y conocimiento	●
Conocimiento de seguridad	●
Formación sobre seguridad	●

[27] Tabla extraída del informe completo de MSAT, Anexo B, páginas 54-56.

Resultados:

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.

Tabla 2.14: Riesgos encontrados en Formación y conocimiento.[28]

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.

2.2.4.4 Análisis General Área Personal

Para el área de Personal, se analizaron de 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 presentamos un resumen de los problemas que consideramos 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

[28] Tabla extraída del informe completo de MSAT, Anexo B, páginas 56-59.

evaluaciones, lo que ayuda a la empresa a mejorar la seguridad de los recursos de TI y de la información.

No existe ninguna 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**.**

2.3 ANALISIS 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, las otras áreas cumplen con las mejores prácticas recomendadas.

El área que presenta mayores problemas de seguridad, es el área de aplicaciones que presentan 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.

La tabla 2.15 nos presenta las sub-secciones que presentan mayores problemas, y el nivel de prioridad en el que deberían ser resueltas 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

Tabla 2.15: Sub-secciones con problemas y el nivel de prioridad para ser resueltas[29]

De todas las sub-secciones analizadas, concluimos que acceso remoto no debería tener prioridad alta debido a que actualmente no existe personal de la empresa que se conecte remotamente a la red de la empresa.

2.4 EVALUACIÓN DE RIESGOS CON OCTAVE –S

En este apartado desarrollamos la fase preparatoria, fase 1, y fase 2 de la metodología.

2.4.1 FASE PREPARATORIA: CONFORMACIÓN DEL EQUIPO DE ANÁLISIS

El Gerente de Operaciones y Administración, Ing. Osvaldo Ruiz; ha mostrado mucho interés en el presente proyecto; pues el diseño del plan de seguridad de la información para la empresa Manpower podría constituirse en un valioso aporte y apoyo para el plan informático de la organización.

[29] Tabla extraída del informe completo de MSAT, Anexo B, páginas 5-6.

La participación del Gerente de Operaciones y Administración y la Administradora de Sistemas ha sido de vital importancia para poder poner en marcha la evaluación.

El equipo está conformado por los miembros descritos en la tabla 2.16.

MIEMBROS	FUNCIÓN EN LA EVALUACIÓN
Ing. Osvaldo Ruiz	Gerente de Operaciones y Administración (Supervisa de manera activa la evaluación)
Ing. Náthaly Riera	Administradora de Sistemas
Sr. Henry Acurio Sr. David Estrella	Tesistas de la Facultad de Ingeniería en Sistemas, quienes utilizan los resultados obtenidos de la metodología OCTAVE –S para el desarrollo del presente proyecto.

Tabla 2.16: Miembros del equipo de análisis

2.4.2 FASE 1: CONSTRUIR PERFILES DE AMENAZA BASADOS EN ACTIVOS

En esta fase se desarrollan los procesos S1 y S2 descritos en la tabla 1.2 del capítulo 1, página 25.

2.4.2.1 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 2.2 muestra las actividades y los pasos que se desarrollan en el proceso S1.

Figura 2.2: Actividades y pasos del proceso S1, Metodología OCTAVE –S.

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

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

Paso 1: Definimos los rangos de potencial impacto (alto, medio, bajo) de las amenazas, a los activos de información de la empresa Manpower, 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: Manpower goza de prestigio gracias al abanico de servicios que contempla todo el ciclo laboral y comercial de la empresa. Según Manpower un porcentaje mayor al 20% 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 Manpower.

Financiera: Esta área es de vital importancia para Manpower, ya que es la encargada de gestionar todos los ingresos y egresos de dinero; administrar los pagos de sueldos, decimos, 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 surja en esta área, por más 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 Manpower.

Seguridad de las personas: En realidad en Manpower 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 titulación 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 están cubiertas en su totalidad, y 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 relativamente bajo.

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 realicen con normalidad y sin contratiempos, y no afecten el funcionamiento normal del negocio.

El proceso de mantenimiento de los servidores, la red y los PC's, reinstalación de sistemas operativos, instalación de parches de software o programas antivirus se lo realiza una vez al mes y durante los días sábados con la finalidad de no interrumpir las actividades de los empleados en los días laborables.

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

Sistemas: En esta área se gestiona todo lo que tiene que ver con TI dentro de la empresa. Es la encargada de administrar los servidores, la red, los respaldos de información, y se encarga de brindar soporte técnico a toda la empresa. Una caída en uno de los servidores o en la red representaría un grave problema para el proceso de negocio de la empresa, es por eso que esta área es considerada de potencial alto impacto.

2.4.2.1.2 Actividad S 1.2: Identificar activos de información de la empresa Manpower.

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

Paso 2: Identificamos los activos (sistemas, aplicaciones, información, personas) relacionados con la información de la empresa Manpower. Para identificar dichos activos tomamos como punto de partida la experiencia y los conocimientos que tienen sobre la red tanto el Gerente de Operaciones y Administración como la Administradora de Sistemas, 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 Gestor: Constituye el más importante de los activos de información de Manpower, tanto por la información que maneja como la importancia que el sistema representa para la empresa. Este ERP tiene 7 módulos que automatizan los procesos de negocio de Manpower. Los módulos del sistema son manejados por diferentes áreas de acuerdo a la función que cumpla dentro de la empresa.

Servidor de Correo interno de Manpower: Es un medio importante de comunicación para mantener contacto con clientes, proveedores y usuarios. Además se utilizan los correos como respaldos de confirmaciones y respuestas de diferentes eventos y actividades. Reside en el servidor Linux con S.O. CentOS 5.0, tiene un enlace en la página web http://manpower.ec/webmail/src/login.php la cual utiliza la aplicación webmail "SquirrelMail". Todo el personal de Manpower dispone de una cuenta de correo. El manejo de las contraseñas de correo las gestiona la Administradora de Sistemas.

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 escaneados y almacenados en la computadora de la Gerente General y en un disco duro externo que tiene la Administradora de Sistemas, y los archivos físicos son almacenados por el Gerente de Operaciones y Administración en su oficina.

Servidor de Base de datos: Aquí se guardan los datos que son procesados por el Sistema Gestor, además almacena las fichas de los candidatos. El sistema gestor de base de datos que se utiliza es Oracle en su versión 6.

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 de la sucursal de Ecuador, puede acceder a los servidores que tiene Manpower en el exterior para poder brindar los servicios a sus clientes.

Página web: La página web de la empresa está alojada en un servidor ubicado en una sucursal de Manpower en el exterior y es mantenida y actualizada por personal de dicha sucursal. La página contiene información de cómo acceder a los servicios que presta la empresa, por lo que al inicio le permite escoger el país y el idioma de la persona que ingresa, debido a que los servicios varían de acuerdo al país de residencia.

Además este es el medio por el cual los candidatos pueden enviar sus hojas de vida para postularse a un puesto de trabajo.

2.4.2.1.3 Actividad S 1.3: Evaluar prácticas de seguridad organizacional.

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

Paso 3: El paso 3 se divide en dos sub-pasos, el primero de ellos es el 3a en el cual analizamos hasta qué punto cada práctica de seguridad es utilizada en la empresa Manpower. En el siguiente sub-paso, que es el 3b, registramos 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, asignamos 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 Manpower está llevando a cabo en cada área. Se utilizaron las siguientes definiciones de semáforo como guía.

- Verde → la organización está llevando a cabo las prácticas de seguridad en esta área de una manera correcta, 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 funciones 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 Manpower 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 solo están documentadas las políticas y no 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 la administradora de sistemas de Manpower, la misma que 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 Gerente de Operaciones y Administración no reciben informes por parte de la administradora de sistemas de los problemas, ni de las soluciones que se les dieron a los incidentes de seguridad. También debemos mencionar que no existe un presupuesto real asignado periódicamente para la seguridad de la información de la empresa.

La realización del presente proyecto de titulación puede considerarse como punto positivo dentro de ésta área de práctica de seguridad para Manpower, ya que al efectuar la evaluación con las herramientas MSAT y OCTAVE –S se mejorará la seguridad de la información y su gestión. También debemos recalcar 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 en los miembros de la empresa, esto representa una garantía para la gestión de la seguridad de la información en Manpower.

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 Manpower cuenta con un amplio conjunto de políticas que se encuentran documentadas, sin embargo las mismas no son revisadas ni actualizadas periódicamente, la última revisión que se hiso en este documento fue en el año 2007.

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. El único proveedor con el que cuenta Manpower es el ISP, y los acuerdos a nivel de servicio que se establecen con el mismo están incluidos en los contratos. Se incluyen condiciones específicas de seguridad en los SLAs.

Existen empleados y/o socios que se conectan remotamente a la red interna de Manpower pero no utilizan ninguna tecnología de VPN para permitirles un acceso seguro, y debemos mencionar también que 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

Manpower cuenta con un plan de contingencia el mismo que incluye:

- Seguridad de la instalación.
- Disponibilidad de recursos de hardware y software en la instalación.
- Disponibilidad de recursos de hardware y software en una instalación alterna.
- Políticas y procedimientos de respaldo de información:

- Recuperación de información.
- Procedimientos de simulacros.

Dentro de lo más importante del plan de seguridad de Manpower debemos mencionar que la empresa cuenta con equipos de computación distribuidos en las oficinas descentralizadas de Manpower en Guayaquil, Manta, Cuenca, etc, que soportan el proceso descentralizado de las mismas y de los cuales uno de los equipos instalado en oficinas de Manpower en Guayaquil tiene las capacidades para desempeñarse eventualmente como servidor de Base de Datos Oracle, y asumir las funciones del Servidor de la Instalación Central considerado el más crítico de la Institución. Se mantiene en la oficina de Guayaquil los siguientes recursos de software:

- Copia de los CD's de instalación de Base de Datos Oracle.
- Copia de los CD's de herramientas Developer y Reports de Oracle.
- Copia de CD de aplicativo Gestor.

Existe un procedimiento de simulacros para valorar el impacto real de los escenarios establecidos como posibles, en el cual deben participar los recursos humanos, técnicos y operativos, sin embargo nunca se ha realizado dichos simulacros.

Todo 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, Manpower han instaurado controles de seguridad física para proteger los activos de la empresa y se ha instalado un sistema de alarma para detectar e informar de intrusiones. Los equipos de red se encuentran en una habitación cerrada con acceso restringido, y las estaciones de trabajo y ordenadores portátiles están protegidos con cables de seguridad.

Como puntos negativos dentro de ésta área tenemos que los documentos confidenciales físicos se almacenan en la oficina del Gerente en Operaciones y

Administración 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 amarillo.

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

En Manpower 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 Administrador de Sistemas.

Existe un procedimiento para respaldar y salvaguardar la información. Se ejecutan respaldos diarios (Lunes a Viernes) de toda la base de datos Oracle en producción, del cual se mantienen históricos recientes en el disco del servidor, y se genera 1 DVD semanal que se ubica en casillero bancario. En el casillero se mantiene únicamente los 2 últimos respaldos y se retornan a Centro de cómputo los más antiguos, y 1 DVD quincenal que se envía a la oficina de Guayaquil. Se mantiene únicamente en este lugar los 2 últimos respaldos y se retornan a Centro de cómputo los más antiguos.

Además se mantiene en caja fuerte el software de las aplicaciones necesarias para la producción de la empresa como los CD’s de instalación de Base de Datos

Oracle, las herramientas Developer y Reports de Oracle, una copia del aplicativo Gestor, y los Sistemas operativos Windows 2003 Server y Linux CentOS.

Se tiene una buena política de claves de acceso para ingresar a la intranet o al sistema gestor, las mismas que administra el Gerente de Operaciones y Administración, que 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 Administrador de Sistemas, restringe todos los puertos de internet, para que los usuarios solo puedan acceder a páginas que necesiten para cumplir con sus tareas.

Se utiliza Message WLAVS, que envía mensajes de alerta junto con los correos que se cree pueden tener código malicioso, pero queda a elección del usuario el abrir o no el correo electrónico.

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 Manpower.

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 valides 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 a la intranet o 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 Gerente de Operaciones y Administración es el encargado de eliminar las cuentas del personal que ya no trabaja para la empresa, para evitar que los mismos puedan seguir accediendo con la cuenta que tenían asignada.

Todos los empleados firman un acuerdo, en donde se establece que deben comprometerse a cumplir con las políticas de seguridad de la empresa, de este modo Manpower se asegura que sus empleados no utilicen información sensible de la empresa con ningún otro fin.

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

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.

Los programas antivirus, y los sistemas operativos están programados para actualizarse automáticamente, si se necesita instalar un nuevo parche al sistema este es responsabilidad del administrador de sistemas.

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 Manpower 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 todas las licencias de los equipos de hardware y software que posee la empresa. Existen procedimientos documentados de cómo gestionar los respaldos, y procedimientos de recuperación de datos.

Se mantiene un contrato de seguros con Panamericana del Ecuador S.A. que cubre equipo electrónico por un monto real de costo con una cobertura en caso de incendio, motín, cortocircuitos, robos u otros incidentes.

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

2.4.2.2 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 2.3 muestra las actividades y los pasos que se desarrollan en el proceso S2.

Figura 2.3: Actividades y pasos del proceso S2, Metodología OCTAVE –S.

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

Paso 5: Seleccionamos 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: Identificamos el activo crítico por su nombre.

Paso 7: Especificamos la razón por la cual al activo crítico se le considera como tal.

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

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

A continuación presentamos los resultados de los pasos anteriormente descritos:

Activos Críticos

Sistema Gestor: El Sistema Gestor es un ERP (Sistema de Gestión Empresarial) que permite la funcionalidad y operatividad de las distintas áreas: Contabilidad, Nómina, Caja/Bancos, etc, dentro de Manpower, 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 de recursos humanos.

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 Manpower.

Servidor de Correo interno de Manpower: 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. Todo el personal de Manpower dispone de una cuenta de correo. El manejo de las contraseñas de correo las gestiona la Administradora de Sistemas. Por los motivos expuestos este activo de información es considerado crítico para Manpower.

Servidor de BDD: Este servidor almacena los datos que son procesados por el Sistema Gestor, además de las fichas de los candidatos. Esta información es sensible y debe estar siempre disponible, por lo que la importancia del servidor de BDD para las actividades diarias de la empresa es alta. La administración de este servidor está a cargo de la Administradora de sistemas, y pueden acceder a la base, todos los usuarios que tienen acceso al sistema gestor.

Por los motivos expuestos este activo de información es considerado crítico para Manpower.

Las computadoras personales, PCS: Funcionan como estaciones de trabajo, son la principal herramienta para el desarrollo de las actividades de los empleados de Manpower. Muchos de estos activos almacenan información sensible para el negocio y otros se utilizan para evaluar a los candidatos. 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 Manpower.

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

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

Paso 10: Identificamos los requerimientos de seguridad para cada activo crítico de Manpower.

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: Identificamos los requerimientos más importantes de seguridad para cada activo crítico de Manpower. A continuación presentamos los resultados:

Establecimos que los requerimientos de seguridad más importantes para los activos críticos s*istema gestor* y s*ervidor 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 s*ervidor de correo* es un medio importante

de comunicación y adicionalmente se lo utiliza como respaldos de confirmaciones y respuestas, y el s*istema gestor* es esencial para la gestión empresarial y la toma de decisiones.

Para los activos críticos s*ervidor de BDD* y c*omputadores 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 Manpower, 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.

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

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

Paso 12 [30] **:** Completamos apropiadamente todos los árboles de amenazas, propuestos por OCTAVE-s, para cada activo crítico, tomando en cuenta las siguientes categorías de amenazas[31]:

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

A continuación presentamos los resultados:

1. Activo crítico: Sistema Gestor

1.1 Actores humanos usando acceso a la red.

Determinamos 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 establecimos que pueden existir actores externos a la empresa con acceso a la red que representan una amenaza para este activo crítico y que

[30] Los arboles de amenaza están desarrollados en el anexo C, paginas 2-19
[31] Las categorías que se analizan, son las que propone OCTAVE –S para el paso 12.

actúan deliberadamente. Los mismos pueden causar revelación o modificación de la información procesada por este sistema.

1.2 Actores humanos usando acceso físico.

Determinamos 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, pérdida o interrupción de la información procesada por este sistema.

También establecimos 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.

1.3 Problemas del sistema.

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

1.4 Otros problemas.

Determinamos 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).

2. Activo crítico: Servidor de BDD

2.1 Actores humanos usando acceso a la red.

Determinamos 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.

Descartamos, 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.

2.2 Actores humanos usando acceso físico.

Descartamos 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 jefe de sistemas.

2.3 Problemas del sistema.

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

2.4 Otros problemas.

Determinamos 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.

3. Activo crítico: Servidor de Correo

3.1 Actores humanos usando acceso a la red.

Determinamos 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.

3.2 Actores humanos usando acceso físico.

Descartamos 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 jefe de sistemas.

3.3 Problemas del sistema.

Determinamos 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.

3.4 Otros problemas.

Determinamos 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.

4. Activo crítico: Computadores personales.

4.1 Actores humanos usando acceso a la red.

Determinamos 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 establecimos, 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.

4.2 Actores humanos usando acceso físico.

Determinamos 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 establecimos, 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.

4.3 Problemas del sistema.

Determinamos 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).

4.4 Otros problemas.

Determinamos 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[32]: En este paso determinamos cuales 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.
- Extranjeros actúan por accidente.
- Extranjeros 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 presentamos los resultados:

1. Activo crítico: Sistema Gestor

1.1 Actores humanos usando acceso a la red.

Internos que actúan por accidente: Determinamos 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: Determinamos 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: Determinamos 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.

[32] Las combinaciones de actores y motivos del actor, son las que propone OCTAVE –S para el paso 13.

1.2 Actores humanos usando acceso físico

Internos que actúan por accidente: Determinamos 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: Determinamos 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: Determinamos 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 Manpower, realizar el cobro de algún servicio prestado, o por contactarse con un empleado en específico.

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

2. Activo crítico: Servidor de base de datos

2.1 Actores humanos usando acceso a la red

Internos que actúan por accidente: Determinamos 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 identificamos, personas que de alguna u otra manera les interesa información de la contabilidad de la empresa, o las fichas de los postulantes que buscan acceder al servicio de la empresa.

3. Activo crítico: Servidor de correo

3.1 Actores humanos usando acceso a la red

Internos que actúan por accidente: Determinamos 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 identificamos, personal de la competencia que esté interesado en conocer información de los contratos, o de los proveedores que maneja la empresa.

4. Activo crítico: Computadores personales

4.1 Actores humanos usando acceso a la red.

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

Internos que actúan deliberadamente: Determinamos que la mayor amenaza a éste activo a través de la red, son todos los empleados de Manpower que utilizan las PCs para realizar sus actividades.

Externos que actúan por accidente: Determinamos que la mayor amenaza a éste activo a través de la red, son los usuarios que utilizan los servicios de Manpower, 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: Determinamos que la mayor amenaza a éste activo a través de la red, son los usuarios que utilizan los servicios de Manpower, y que rinden pruebas de aptitud en algunos computadores ubicados en las instalaciones de la empresa, que se utilizan sólo con ese fin.

4.2 Actores humanos usando acceso físico

Internos que actúan por accidente: Determinamos que la mayor amenaza a éste activo por medios físicos, son todos los empleados de Manpower.

Internos que actúan deliberadamente: Determinamos que la mayor amenaza a éste activo por medios físicos, son todos los empleados de Manpower.

Externos que actúan por accidente: Determinamos 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 Manpower, realizar el cobro de algún servicio prestado, o por contactarse con un empleado en específico.

Externos que actúan deliberadamente: Determinamos 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 Manpower, realizar el cobro de algún servicio prestado, o por contactarse con un empleado en específico.

Paso 14[33]: En este paso anotamos 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.
- Extranjeros 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 presentamos los resultados:

1. Activos crítico: Sistema gestor

1.1 Actores humanos usando acceso a la red.

Internos que actúan deliberadamente: Consideramos 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: Consideramos 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.

1.2 Actores humanos usando acceso físico.

Internos que actúan deliberadamente: Consideramos 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

[33] Las combinaciones de actores y motivos del actor, son las que propone OCTAVE –S para el paso 14.

bajas debido a que no se tienen datos objetivos relacionados con dicha estimación.

Externos que actúan deliberadamente: Consideramos 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.

2. Activo crítico: Servidor de base de datos

2.1 Actores humanos usando acceso a la red.

Internos que actúan deliberadamente: Descartamos 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.

3. Activo crítico: Servidor de correo

3.1 Actores humanos usando acceso a la red.

Internos que actúan deliberadamente: Descartamos 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: Identificamos 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.

4. Activo crítico: Computadores personales

4.1 Actores humanos usando acceso a la red.

Internos que actúan deliberadamente: Consideramos 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: Consideramos 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.

4.2 Actores humanos usando acceso físico

Internos que actúan deliberadamente: Consideramos 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: Consideramos 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 debemos 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. Debemos mencionar que el equipo de análisis no cuenta con datos objetivos y se tienen pocos datos subjetivos, motivo por el cual descartamos realizar este paso y nos centramos en llevar a cabo los pasos siguientes.

Paso 16[34]**:** En este paso describimos 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.
- Extranjeros actúan por accidente.
- Extranjeros actúan deliberadamente.

[34] Las combinaciones de actores y motivos del actor, son las que propone OCTAVE –S para el paso 16.

A continuación se describe resultados:

1. **Activo crítico: Sistema gestor**

1.1 Actores humanos usando acceso a la red

Internos que actúan por accidente: Consideramos 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: Consideramos que los usuario 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 Manpower, 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: Consideramos 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.

1.2 Actores humanos usando acceso físico

Internos que actúan por accidente: Consideramos 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: Consideramos 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. Debemos 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: Consideramos 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 Manpower, 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: Consideramos 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 Manpower, 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.

1.3 Problemas del sistema

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

Defectos de Hardware: Consideramos 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 Manpower.

Código Malicioso: Consideramos 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.

1.4 Otros Problemas

Desastres Naturales: Consideramos que no existe una protección adecuada en las instalaciones de Manpower, y en el caso de un evento sísmico en la ciudad de Quito, la empresa no garantizaría la disponibilidad del Sistema Gestor para su utilización.

Problemas de fuente de energía: Consideramos a los problemas de fuente de energía como una amenaza latente, ya que Manpower 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.

2. Activo crítico: Servidor de Base de datos

2.1 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.

2.2 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.

2.3 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 las fichas de nuevos postulantes que intenten ingresar sus datos 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 diarios de la base de datos, el tiempo que tomaría restaurar la base significaría en interrupción de las actividades de la empresa.

3. Activo Crítico: Servidor de Correo

3.1 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.

3.2 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.

3.3 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.

4. Activo Crítico: Computadores Personales

4.1 Actores humanos usando acceso a la red

Internos que actúan por accidente: Consideramos que todo el personal que utilizan 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 Manpower, 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 Manpower.

Internos que actúan deliberadamente: Consideramos 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 Manpower, 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 Manpower.

Externos que actúan por accidente: Consideramos que las personas que utilizan los servicios de Manpower, 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 Manpower, ya que son computadores que se utilizan exclusivamente para rendir las pruebas de aptitud.

Externos que actúan deliberadamente: Consideramos que las personas que utilizan los servicios de Manpower, 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 Manpower, ya que son computadores que se utilizan exclusivamente para rendir las pruebas de aptitud.

4.2 Actores humanos usando acceso físico

Internos que actúan por accidente: Consideramos 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: Consideramos 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.

Externos que actúan por accidente: Consideramos 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 Manpower, realizar el cobro de algún servicio prestado, o por contactarse con un empleado en específico, estos podrían amenazar al activo, ya que muchas de estas personas se dirigen a las diferentes oficinas de la empresa, y las mismas podrían accidentalmente desconectar las PCs o algún componente de este, y causar la caída o el daño del mismo. Además no se podría comprobar quién o quienes causaron los problemas.

Externos que actúan deliberadamente: Consideramos 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 Manpower, realizar el cobro de algún servicio prestado, o por contactarse con un empleado en específico, estos podrían amenazar al activo ya que muchas de estas personas se dirigen a las diferentes oficinas de la empresa, y las mismas podrían deliberadamente desconectar las

PCs o algún componente de este, y causar la caída o el daño del mismo. Además no se podría comprobar quién o quienes causaron los problemas.

4.3 Problemas del sistema

Defectos de software: Consideramos 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: Consideramos 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: Consideramos que cualquiera de las PCs pertenecientes a la empresa, están sujetas a amenazas de este tipo. Si bien todas 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.

4.4 Otros Problemas

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

Problemas de fuente de energía: Consideramos a los problemas de fuente de energía como una amenaza latente, ya que Manpower 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.

4.4.1 FASE 2: IDENTIFICAR VULNERABILIDADES EN LA INFRAESTRUCTURA.

En esta fase desarrollamos el proceso S3 descrito en la tabla 1.3 del capítulo 1, página 26.

4.4.1.1 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 2.4 muestra las actividades, y los pasos que se desarrollan en el proceso S3.

Figura 2.4: Actividades y pasos del proceso S3, Metodología OCTAVE –S.

4.4.1.1.1 Actividad S3.1 Examinar rutas de acceso.

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

Paso 17: En este paso determinamos 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.

En la figura 2.5 podemos ver a todos los usuarios que tienen instalado el sistema en su ordenador, los módulos que tienen habilitados, y la forma en cómo se transmite la información a través de la red de la empresa.

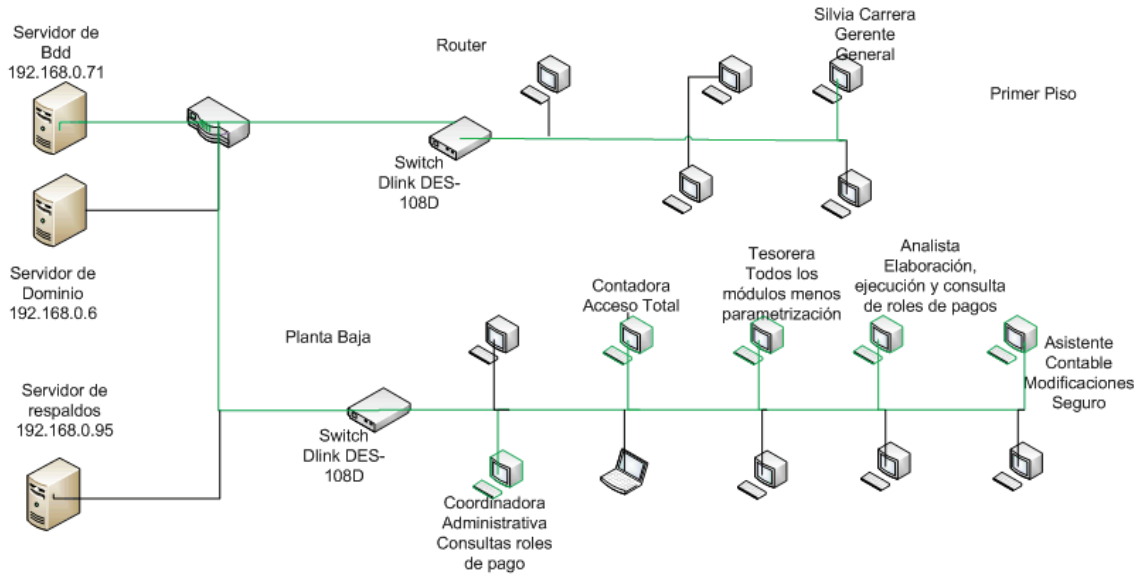

Figura 2.5: Usuarios con acceso al Sistema Gestor.

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

Paso 18a: En este paso examinamos las rutas de acceso e identificamos 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 determinamos 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 determinamos qué clase de componentes pueden utilizar las persona (usuarios, atacantes) para acceder al sistema de interés, y establecimos, que para que una persona pueda acceder al sistema debe tener instalada y configurada la aplicación en su PC, y los únicos usuarios que tienen instalada la aplicación, son los mostrados en la figura 2.5 (pág. 90). 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 determinamos qué clase de componentes se utilizan para realizar respaldos de la información del sistema de interés, y establecimos, que toda la información que procesa el sistema gestor, y se almacena en el servidor de base de datos, es respaldada diariamente en el servidor de respaldo por medio de una tarea programada fuera de los horarios de oficina.

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

4.4.1.1.2 Actividad S3.2 Analizar Procesos Relacionados con la Tecnología.

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

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

Paso 19a: En este paso determinamos 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

establecimos que los componentes relacionados con los activos críticos son los servidores, la red interna, las estaciones de trabajo, y laptops utilizadas dentro de Manpower.

Paso 19b: En este paso relacionamos a los activos críticos con cada clase de componente. Determinamos 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 asignamos la responsabilidad de quien mantiene y se encarga de cada clase de componente en la red. En Manpower estas funciones están únicamente a cargo de la Administradora 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 realizamos 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 realizamos una comparación entre las metodologías utilizadas en el presente proyecto. Primero analizamos las diferencias de realizar la evaluación con MSAT u OCTAVE -S. A continuación comparamos los resultados obtenidos con cada herramienta basándonos en las áreas equivalentes. Las áreas equivalentes se muestran en la tabla 2.17, y 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 determinamos que las áreas de análisis que cubren ambas herramientas, son prácticamente equivalentes salvo pequeñas excepciones que analizaremos 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 basando 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.

A continuación presentamos un análisis comparativo de los resultados obtenidos con ambas metodologías:

Áreas OCTAVE-S	Áreas de MSAT
1. Concienciación y Formación en Seguridad.	Personal **Formación y conocimiento**
2. Estrategia de Seguridad.	
3. Gestión de Seguridad.	**Infraestructura** Gestión y control **Personal** Directiva y procedimientos (menos relaciones con terceros)
4. Políticas y regulaciones de Seguridad.	**Operaciones** Directiva de seguridad
5. Gestión de la Seguridad Colaborativa.	**Personal** Directiva y procedimientos Relaciones con terceros
6. Planes de Contingencia/Recuperación de Desastres.	**Operaciones** Copias de seguridad y recuperación
7. Control de Acceso Físico.	**Infraestructura** Gestión y control Seguridad física
8. Monitoreo y Auditoría de Seguridad Física.	
9. Gestión de Sistemas y Redes.	**Operaciones** Entorno **Infraestructura** Defensa del perímetro
10. Monitoreo y Auditoría de Seguridad de TI.	**Personal** Requisitos y evaluaciones
11. Autenticación y Autorización.	**Infraestructura** Autenticación
12. Gestión de Vulnerabilidades.	**Aplicaciones** Implementación y uso Vulnerabilidades
13. Encriptación.	**Aplicaciones** Almacenamiento y comunicaciones de

	datos
14. Diseño y Arquitectura de Seguridad.	**Operaciones** Gestión de actualizaciones y revisiones Documentación de la red Flujo de datos de la aplicación
15. Gestión de Incidentes.	**Infraestructura** Gestión y control Informes sobre incidentes y respuesta **Aplicaciones** Implementación y uso Diseño de aplicaciones

Tabla 2.17: Áreas equivalentes de ambas metodologías

El área de Concienciación y Formación en Seguridad de OCTAVE -S equivale al área Personal sección Formación y conocimiento de MSAT. A esta área se le ha asignado un estado de semáforo amarillo en OCTAVE –S, y un estado de alerta rojo en MSAT. Ambas herramientas coinciden en que el problema dentro de esta área es que el personal no recibe capacitación ni interna, ni externa sobre seguridad de la información. Además MSAT señala como problema que no existe ningún medio para informar a los usuarios acerca de las políticas de seguridad de la empresa, pero mientras se elaboraban los pasos de OCTAVE -S concluimos que esos datos no son correctos, ya que los usuarios tienen toda esa información disponible en la intranet de la empresa.

El área Gestión de Seguridad de OCTAVE -S equivale a las áreas Infraestructura sección Gestión y Control, y Personal sección Directiva y procedimientos (menos relaciones con terceros) de MSAT. Esta área para OCTAVE -S tiene asignado un estado de semáforo amarillo, y en MSAT amarillo la sección de Gestión y control y verde la sección de Directiva y procedimientos. Dentro de esta área MSAT considera también la seguridad física, pero OCTAVE -S tiene un área de seguridad propia para este paso por lo que no se considerara en este análisis. Ambas herramientas coinciden que se están llevando bien las actividades para resolver e informar sobre los incidentes que se presentan, y que el problema en esta área, es que se tiene una directiva para los empleados que dejan la empresa

de forma amistosa, pero no para los empleados que dejan la empresa de forma hostil.

El área de Políticas y regulaciones de Seguridad de OCTAVE -S equivale al área Operaciones sección Directiva de seguridad de MSAT. A esta área se le ha asignado un estado de semáforo amarillo en OCTAVE –S, y un estado de alerta verde en MSAT. Con OCTAVE -S determinamos que no existen procedimientos establecidos para tratar los incidentes de seguridad, y con MSAT especificamos las actividades que se están haciendo mal dentro de esta área que son principalmente la clasificación y eliminación de datos.

El área de Gestión de la Seguridad Colaborativa de OCTAVE -S equivale al área Personal sección Directiva y procedimientos sub-sección Relaciones con terceros de MSAT. A esta área se le ha asignado un estado de alerta verde en ambas herramientas. Hay que recordar que el único proveedor del que recibe servicios Manpower es del ISP, y en general se están llevando bien las actividades para gestionar esta área.

El área de Planes de Contingencia/Recuperación de Desastres de OCTAVE -S equivale al área Operaciones sección Copias de seguridad y recuperación de MSAT. A esta área se le ha asignado un estado de alerta verde en ambas herramientas, por lo que podemos concluir que se están manejando bien todas las actividades para esta área.

El área de Control de Acceso Físico de OCTAVE -S equivale al área Infraestructura sección Gestión y control sub-sección Seguridad física de MSAT. A esta área se le ha asignado un estado de alerta amarillo en ambas herramientas. Ambas herramientas coinciden en que se están llevando bien los controles para proteger los activos de la empresa, y que los problemas dentro de esta área son que no existen controles para los visitantes que ingresan a la organización, y que los documentos confidenciales impresos no se almacenan adecuadamente (en un armario con llave).

El área de Gestión de Sistemas y Redes de OCTAVE -S es bastante amplia y se equivale con 2 áreas de MSAT que son Operaciones sección Entorno e Infraestructura sección Defensa del perímetro. Esta área para OCTAVE -S tiene asignado un estado de semáforo amarillo y en MSAT verde la sección de entorno

y amarillo la sección de defensa del perímetro. Ambas coinciden en que se están llevando bien las actividades de gestión de equipos de red y manejo de antivirus. Con MSAT pudimos determinar que las debilidades dentro de esta área son que la red solo posee un segmento de red, y que no se usa una tecnología VPN para permitir el acceso remoto seguro.

El área de Monitoreo y Auditoría de Seguridad de TI de OCTAVE -S equivale al área Personal sección Requisitos y Evaluaciones de MSAT. A esta área se le ha asignado un estado de alerta amarillo en ambas herramientas. Ambas coinciden en que el problema de esta área es que no se realizan evaluaciones de seguridad dentro de la empresa.

El área Autenticación y Autorización de OCTAVE -S equivale al área Infraestructura sección Autenticación de MSAT. A esta área se le ha asignado un estado de semáforo verde en OCTAVE –S, y un estado de alerta amarillo en MSAT. MSAT marca como problema que los usuarios tienen habilitados accesos administrativos a sus estaciones de trabajo. Con OCTAVE -S comprobamos que es cierto, pero es un problema que no se puede solucionar, ya que la aplicación gestor solo funciona correctamente si los usuarios tienen permisos de administrador. Además ambas coinciden en que otro problema es que las cuentas de acceso remoto no utilizan directivas de contraseñas.

El área Gestión de Vulnerabilidades de OCTAVE -S equivale al área Aplicaciones sección Implementación y uso sub-sección Vulnerabilidades de MSAT. A esta área se le ha asignado un estado de alerta rojo en ambas herramientas. Ambas coinciden en que el problema de esta área es que no se manejan herramientas, ni procedimientos, para determinar y eliminar vulnerabilidades en el sistema.

El área Encriptación de OCTAVE -S equivale al área Aplicaciones sección Almacenamiento y comunicaciones de datos de MSAT. A esta área se le ha asignado un estado de alerta amarillo en ambas herramientas. Ambas concluyen que la empresa cifra los datos confidenciales cuando están almacenados y antes de ser transmitidos, pero el problema es que el algoritmo de cifrado (DES), se considera inseguro por el tamaño de su clave.

El área Diseño y Arquitectura de Seguridad de OCTAVE -S equivale al área Operaciones sección Gestión de actualizaciones y revisiones de MSAT. A esta

área se le ha asignado un estado de alerta rojo en ambas herramientas. Ambas concluyen que el problema dentro de esta área es que no existen diagramas de la arquitectura de red, ni del flujo de datos de las aplicaciones principales. Además dentro de esta área MSAT analiza la gestión de actualizaciones, y Gestión de cambios y configuración que no considera OCTAVE -S. Los problemas encontrados dentro de estas secciones son que en la empresa no existen directivas que regulen la gestión de actualizaciones, y que la empresa no dispone de ningún proceso de gestión de cambios y configuraciones.

El área de Gestión de Incidentes de OCTAVE -S equivale al área Infraestructura sección Gestión y control sub-sección Informes sobre incidentes y respuesta de MSAT. A esta área se le ha asignado un estado de alerta verde en ambas herramientas, por lo que podemos concluir que se están manejando bien todas las actividades para esta área.

El área Aplicaciones sección Diseño de aplicaciones de MSAT, no se lo considero dentro del análisis de OCTAVE -S, ya que la empresa no desarrolla aplicaciones de software. Las áreas Estrategia de Seguridad y Monitoreo, y Auditoría de Seguridad Física, no tienen áreas equivalentes en MSAT, por lo que solo consideraremos los resultados obtenidos con OCTAVE -S.

3. CAPITULO III: PLAN DE SEGURIDAD

En este capítulo presentamos el plan de seguridad con las recomendaciones que propone MSAT, desarrollamos la fase tres de la metodología de OCTAVE -S, que constan de los pasos 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 diseñamos 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 analizamos como los riesgos determinados en el capítulo anterior pueden afectar a las diferentes áreas de la empresa (producción, financiera, etc). En la evaluación de probabilidad de las amenazas llegamos 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, identificamos el enfoque actual de la empresa para hacer frente a cada una de las áreas de práctica de seguridad. Para la selección de enfoques de mitigación, seleccionamos las áreas de seguridad, que presentan mayores problemas, que necesitan ser resueltos con más urgencia, que tienen un mayor impacto para la organización y que tienen mayor margen de mejora, y se les seleccionó como áreas de mitigación. En el desarrollo del plan de mitigación desarrollamos los procesos, procedimientos, políticas, roles y responsabilidades para las áreas seleccionadas en el paso anterior. En la Identificación de cambios y pasos siguientes enumeramos 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, nos 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 Manpower con el fin de proteger su información y activos más valiosos.

3.1 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.

3.1.1 ÁREA: INFRAESTRCUTURA

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
		Directivas de contraseñas – cuenta de usuario
		Directivas de contraseñas – cuenta de acceso remoto
	Gestión y control	Creación segura
		Seguridad física

Tabla 3.1: Secciones y sub-secciones del área de infraestructura que presentan problemas.

3.1.1.1 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 Manpower.
- 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 extranets 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 a la administradora de la red que se está produciendo un ataque a fin de que puedan responder inmediatamente.

Inalámbrico

- En la actualidad Manpower 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.

3.1.1.2 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.

3.1.1.3 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.

3.1.2 ÁREA: APLICACIONES

ÁREA	SECCIONES	SUB-SECCIONES
APLICACIONES	Implementación y uso	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

Tabla 3.2: Secciones y sub-secciones del área de aplicaciones que presentan problemas.

3.1.2.1 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.

3.1.2.2 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.

3.1.2.3 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 representan 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 el intrusismo por técnicas de fuerza bruta.

3.1.3 ÁREA: 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

Tabla 3.3: Secciones y sub-secciones del área de operaciones que presentan problemas.

3.1.3.1 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.

3.1.3.2 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 conocerla 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.

3.1.3.3 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.

3.1.3.4 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.

3.1.4 ÁREA: PERSONAL

ÁREA	SECCIONES	SUB-SECCIONES
PERSONAL	Requisitos y evaluación	Evaluación de seguridad
	Directiva y procedimientos	Directiva de recursos humanos
	Formación y conocimiento	Conocimiento de seguridad
		Formación sobre seguridad

Tabla 3.4: Secciones y sub-secciones del área de personal que presentan problemas.

3.1.4.1 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.

3.1.4.2 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.)

3.1.4.3 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.

3.2 PLAN DE SEGURIDAD OCTAVE –S

En este apartado completamos la evaluación de OCTAVE –S desarrollando los procesos y actividades correspondientes a la fase 3 de la metodología.

3.2.1 FASE 3: DESARROLLO DE PLANES Y ESTRATEGIAS DE SEGURIDAD.

En esta fase desarrollamos los procesos S4 y S5 descritos en la tabla 3.1.

3.2.1.1 Proceso S4: Identificación y análisis de riesgos.

Este proceso se centra en evaluar el impacto y la probabilidad de las amenazas a los activos críticos, y establecer criterios de evaluación de probabilidad.

La figura 3.1 muestra las actividades y los pasos que se desarrollan en el proceso S4.

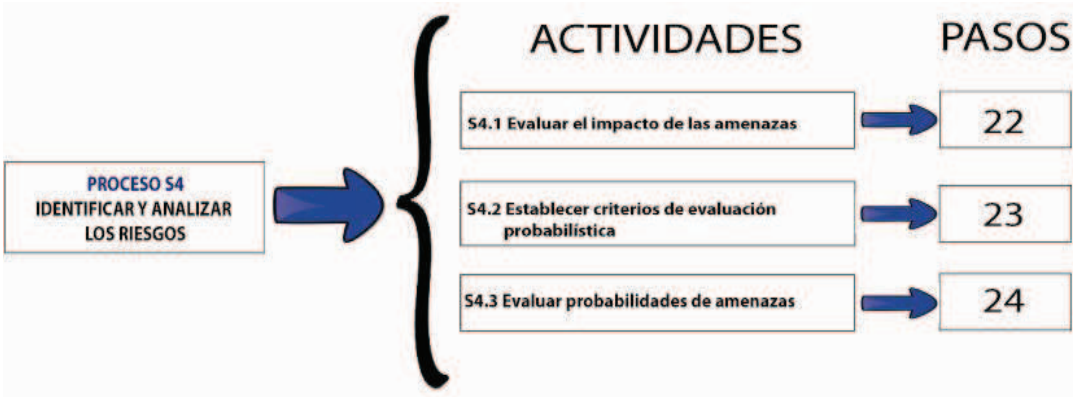

Figura 3.1: Actividades y pasos del proceso S4, Metodología OCTAVE –S.

3.2.1.1.1 Actividad S4.1: Evaluar el impacto de las amenazas.

En esta actividad se desarrolla el paso 22 que se describe a continuación:

Paso 22[35]: En este paso analizamos para cada activo crítico el impacto de las amenazas en las diferentes áreas de la empresa. Las áreas consideradas son las que propone OCTAVE -S en las hojas de trabajo correspondientes a este paso, y son las siguientes:

- Reputación/Confianza del cliente
- Financiera
- Productividad
- Multas
- Seguridad
- Otros

Las amenazas consideradas son las que determinamos en el capítulo anterior (paso 12).

A continuación presentamos los resultados:

1. **Activo crítico: Sistema Gestor**

Determinamos que las amenazas que representan los actores humanos con acceso a la red o con acceso físico, sean internos o externos a la empresa, y que actúan accidentalmente podrían tener un alto impacto en el área financiera y de productividad, ya sea por la modificación, pérdida/destrucción y/o interrupción de la información que el sistema gestor procesa. Adicionalmente establecimos que las amenazas que representan dichos actores, y que actúan deliberadamente podrían tener un alto impacto en el área financiera y de productividad, debido a la revelación, modificación, perdida/destrucción y/o interrupción de la información procesada por el sistema.

Manpower considera que las amenazas que representan los defectos de hardware y los fallos del sistema, pueden tener un alto impacto en el área financiera y de productividad debido a la pérdida/destrucción y/o interrupción de la información que se procesa en el sistema gestor. También establecimos que las amenazas que representan los códigos maliciosos (virus, gusanos, troyanos,

[35] Los resultados de este paso se encuentran en el anexo C.

puertas traseras) podrían tener un alto impacto en el área financiera y de productividad, debido a la modificación y/o interrupción de la información.

Los problemas de fuentes de energía podrían tener un alto impacto en el área financiera y de productividad, debido a la interrupción en los procesos de negocio de la empresa, y en sí de la información que el sistema gestor procesa. Adicionalmente establecimos que las amenazas que representan los desastres naturales (terremotos, incendios) pueden tener un alto impacto en el área financiera y de productividad, debido a la perdida/destrucción y/o interrupción de la información gestionada por el sistema.

2. Activo crítico: Servidor de Base de datos

Para Manpower únicamente se considera de riesgo ataques por personal externo a la empresa, ya que como determinamos en el capítulo 2, en los pasos 12-16, los ataques de personal interno se desestimaron por las bajas motivaciones del personal, y no consideramos factible ataques usando el acceso físico.

Un ataque de una persona al servidor de base de datos, que cause alteración, pérdida, destrucción, o interrupción del flujo de información afecta principalmente en la productividad de la empresa.

Un ataque en el que se robe información del servidor, afectaría a la reputación de la empresa, y traería consigo problemas legales, ya que Manpower garantiza a sus clientes y proveedores la seguridad de su información personal y que la misma solo será usada para prestar adecuadamente los servicios que ofrece la empresa.

Los problemas de fuente de energía y desastres naturales provocarían interrupción de las actividades y pérdida de información, lo cual tendría un impacto en la productividad de la empresa. Además estos problemas dañarían la imagen de Manpower con sus proveedores y clientes, ya que no se podrían prestar los servicios normalmente,

Problemas por fallas del sistema operativo o fallos de hardware por obsolescencia de los equipos provocarían tiempos de respuesta altos o interrupción del servicio lo que afectaría a la producción.

En general para Manpower el impacto que tendría un ataque sobre este servidor se lo considera de nivel alto, ya que este es el activo más importante para la empresa donde se almacena toda la información que procesa el ERP gestor.

3. Activo crítico: Servidor de Correo

Un ataque de una persona al servidor de correo electrónico, que cause alteración perdida, robo o destrucción de los correos afecta principalmente a la reputación de la empresa.

Un ataque que cause interrupción del servicio no trae consigo serios problemas, los usuarios pueden continuar con sus labores normales sin este servicio, por lo que no afectaría a la producción ni a otra área.

Los problemas de fuente de energía y desastres naturales provocarían interrupción de las actividades y pérdida de información, la interrupción del servicio, no representa un problema serio, pero la perdida de información le significaría a la empresa perdida de reputación y problemas legales asociados.

A diferencia de lo que ocurre con el servidor de base de datos un ataque dirigido hacia el servidor de correo que cause la interrupción de los servicios se lo considera de nivel bajo, ya que no afecta en la productividad de la empresa, por otro lado se considera más grave el robo o pérdida de información debido a que la información de los correo se la considera sensible y esto puede traer a la empresa pérdida de reputación y problemas legales.

4. Activo crítico: Computadores personales.

Determinamos que las amenazas que representan los actores humanos con acceso a la red o con acceso físico, sean internos o externos a la empresa, y que actúan accidentalmente podrían tener un alto impacto en el área financiera y de productividad ya sea por la modificación, pérdida/destrucción y/o interrupción de las computadoras y de la información que se maneja en cada una ellas. Adicionalmente establecimos que las amenazas que representan dichos actores y que actúan deliberadamente podrían tener un alto impacto en el área financiera y de productividad debido a la revelación, modificación, pérdida/destrucción y/o

interrupción de los PCs y de la información que se utiliza en los procesos de negocio de la organización.

Manpower considera que las amenazas que representan los defectos de software pueden tener un alto impacto en el área financiera y de productividad ya sea por la modificación, pérdida/destrucción y/o interrupción de la información que se maneja en las PCs y los problemas de defectos de hardware también podrían tener un alto impacto en el área financiera y de productividad debido principalmente a la pérdida/destrucción y/o interrupción de las PCs o de la información que en ellas se gestiona. Adicionalmente el equipo considera que las amenazas que representan los códigos maliciosos (virus, gusanos, troyanos, puertas traseras) tendrían un alto impacto en el área financiera y de productividad por la modificación, perdida/destrucción y/o interrupción de la información que se maneja en cada una de las PCs de Manpower.

Los problemas de fuentes de energía y de desastres naturales (terremotos, incendios) tendrían un alto impacto en el área financiera y de productividad, por la pérdida/destrucción y/o interrupción de las PCs y de la información procesada y almacenada en las mismas.

3.2.1.1.2 Actividad S4.2: Establecer Criterios de Evaluación de la Probabilidad.

En esta actividad desarrollamos el paso 23 que se describe a continuación:

Paso 23: En este paso definimos las medidas para calcular la probabilidad de ocurrencia de una amenaza, basándose en la frecuencia con la que dichos eventos han ocurrido en el pasado. Las probabilidades de amenaza a la seguridad de la información son estimadas utilizando una combinación de datos objetivos y experiencia subjetiva, obtenidos principalmente del personal de TI de la empresa.

Cabe mencionar que este paso es opcional, y decidimos no realizarlo debido a las siguientes razones:

- Es la primera vez que se está utilizando OCTAVE -S en Manpower.
- No se cuenta con datos objetivos ni registros históricos documentados que se relacionen con las amenazas.

- El personal de TI carece de experiencia y conocimientos en seguridad de la información y/o gestión de riesgos.

Por tal motivo el equipo de análisis decidió no calcular la probabilidad de amenazas y por ende continuó con los siguientes pasos a desarrollarse en OCTAVE –S.

3.2.1.1.3 Actividad S4.3: Evaluar Probabilidad de Amenaza.

En esta actividad desarrollamos el paso 24 que se describe a continuación:

Paso 24: Para realizar este paso se utiliza los criterios de evaluación de probabilidad definidos en el paso anterior como una guía para asignar un valor de probabilidad (alta, media o baja) para cada amenaza a cada uno de los activos críticos. Pero, como mencionamos en el paso 23, el equipo de análisis decidió no calcular la probabilidad de amenazas, y por tal motivo este paso también se omite y se continua con los siguientes pasos en el proceso de evaluación con OCTAVE –S.

3.2.1.2 Proceso S5: Desarrollar Estrategias de Protección y Planes de Mitigación.

Este proceso se centra en definir estrategias de protección y planes de mitigación, e incluye actividades para poner en práctica los resultados obtenidos de la evaluación con OCTAVE -S.

La figura 3.2 muestra las actividades y los pasos que se desarrollan en el proceso S5.

Figura 3.2: Actividades y pasos del proceso S5, Metodología OCTAVE –S.

3.2.1.2.1 Actividad S5.1: Describir Estrategias de Protección Actual.

En esta actividad desarrollamos el paso 25 que se describe a continuación:

Paso 25[36]: En este paso transferimos el estado de semáforo (rojo, amarillo o verde) de cada área de práctica de seguridad, definido en el paso 4. Para cada área identificamos el enfoque actual de la empresa para hacer frente a las amenazas.

Las áreas de práctica de seguridad son grupos de prácticas y pueden ser estratégicas u operacionales. Las áreas de prácticas de seguridad estratégicas son generalmente amplias y tienden a afectar a todos los riesgos de todos los activos críticos por igual. Las áreas de prácticas de seguridad operacionales se enfocan en las áreas del día a día y pueden ser dirigidos hacia la mitigación de riesgos específicos de activos específicos. Cabe mencionar que las características de las áreas estratégicas difieren con las características de las áreas operacionales.

Dado que una estrategia de protección proporciona una dirección organizacional con respecto a las actividades de seguridad de la información, esta se estructura de acuerdo a las áreas de práctica de seguridad. A continuación se ilustra en la tabla 3.5 las áreas de práctica de seguridad estratégicas y operacionales.

[36] Fuente: OCTAVE®-S Implementation Guide, Version 1.0

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

Tabla 3.5: Áreas de Práctica de Seguridad Estratégicas y Operacionales[37].

Para el desarrollo de este paso se debe poner atención a la siguiente información para cada área de práctica de seguridad.

- El estado del semáforo.
- El grado en que cada práctica de seguridad para una área se refleja en la empresa.
- Lo que la empresa está haciendo bien actualmente en un área.
- Lo que la empresa no está haciendo bien actualmente en un área.

A continuación se muestran los resultados para cada una de las áreas de práctica de seguridad.

[37] Fuente: OCTAVE®-S Implementation Guide, Version 1.0, página 63.

1. Áreas de Práctica Estratégica[38].

Cada una de estas áreas presentan diferentes características unas con otras.

1.1 Práctica de Seguridad 1: Concienciación y Formación en seguridad.

A esta área de práctica de seguridad se le ha asignado un estado de semáforo amarillo.

En esta área nos enfocamos en sus cinco características:

- Estrategia de capacitación.
- Capacitación en seguridad.
- Capacitación relacionada con seguridad para soporte de tecnología.
- Actualizaciones periódicas de seguridad.
- Verificación de la capacitación.

La empresa Manpower no cuenta con una estrategia de capacitación relacionada con seguridad para el soporte de tecnología que se encuentre documentada.

No existen oportunidades para los miembros del personal de Manpower para que asistan a capacitaciones relacionadas con seguridad para cualquiera de las tecnologías a la que ellos dan soporte. El personal aprende sobre los problemas de seguridad por su propia cuenta.

El personal de la empresa comprende sus funciones 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.

1.2 Práctica de Seguridad 2: Estrategia de Seguridad

A esta área de práctica de seguridad se le ha asignado un estado de semáforo amarillo.

En esta área nos enfocamos en sus tres características:

- Integración de estrategias de seguridad y negocios.
- Estrategias documentadas
- Concienciación al personal

[38] Las características de las áreas de práctica estratégicas son las que propone OCTAVE –S, y difieren para cada área.

Las estrategias de negocio de Manpower toman en consideración seguridades relacionadas con tecnología, ya que ésta es parte fundamental de los procesos de negocio de Manpower. Sin embargo, solo están documentadas las políticas y no las estrategias de seguridad como tal, y dichas documentaciones no son revisadas ni actualizadas periódicamente.

Cabe mencionar que no existe un programa de concienciación y capacitación sobre las estrategias de seguridad de la empresa para el personal.

1.3 Práctica de Seguridad 3: Gestión de Seguridad

A esta área de práctica de seguridad se le ha asignado un estado de semáforo amarillo.

En esta área nos enfocamos en sus seis características:

- Roles y responsabilidades.
- Financiamiento
- Procedimientos de Recursos humanos
- Gestión de riesgos
- Concienciación del personal
- Gestión de la concienciación

La empresa no tiene los roles y responsabilidades de seguridad documentados, sin embargo, la responsabilidad de esta área recae sobre la administradora de sistemas de Manpower.

El presupuesto de la empresa incluye explícitamente las actividades de seguridad de la información en el rubro para TI, y este es determinado mediante procesos informales.

Manpower cuenta con algunos procedimientos en los que incluyen consideraciones de seguridad al momento de contratar un nuevo empleado (por ejemplo, verificando los antecedentes del mismo), y también cuando se da por terminado la relación entre la empresa y un empleado (por ejemplo, eliminando el acceso a la información y a los sistemas).

La empresa no cuenta con procedimientos formales y definidos para evaluar y gestionar los riesgos de seguridad de la información y no existe un programa de

concienciación y capacitación sobre los procesos de gestión de la seguridad de la información.

1.4 Práctica de Seguridad 4: Políticas y Regulaciones de Seguridad

A esta área de práctica de seguridad se le ha asignado un estado de semáforo amarillo.

En esta área nos enfocamos en sus cinco características:

- Políticas Documentadas
- Gestión de políticas
- Cumplimiento de políticas
- Concienciación del Personal
- Cumplimiento de políticas y regulaciones

La empresa Manpower cuenta con un amplio conjunto de políticas documentadas y dentro de las cuales se especifican algunas que están relacionadas con la seguridad de la información, sin embargo las mismas no son revisadas ni actualizadas periódicamente, la última revisión que se hizo en este documento fue en el año 2007.

Manpower cuenta con una evaluación de cumplimiento de las políticas pero no se aplican los procedimientos para realizar dicha evaluación, además a cada empleado se le notifica y entrega las políticas con las que cuenta la empresa pero no se hace un seguimiento para conocer si los empleados leen y aplican las mismas.

No existe un programa de concienciación y capacitación sobre seguridad.

La empresa cuenta con procedimientos no documentados para cumplir con las leyes y reglamentos del Estado Ecuatoriano.

1.5 Práctica de Seguridad 5: Gestión de la Seguridad Colaborativa

A esta área de práctica de seguridad se le ha asignado un estado de semáforo verde.

En esta área nos enfocamos en sus seis características:

- Colaboradores y Socios
- Contratistas y Subcontratistas

- Proveedores de Servicio
- Requerimientos
- Verificación
- Concienciación del personal

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. El único proveedor con el que cuenta Manpower es el ISP y los acuerdos a nivel de servicio que se establecen con el mismo están incluidos en los contratos. Además se incluyen condiciones específicas de seguridad en los SLAs.

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

No existe un programa de concienciación y capacitación sobre seguridad ni sobre las políticas y procedimientos para la gestión de seguridad colaborativa.

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

A esta área de práctica de seguridad se le ha asignado un estado de semáforo verde.

En esta área nos enfocamos en sus cinco características:

- Análisis de operaciones de negocio
- Planes documentados
- Planes probados
- Acceso a la información
- Concienciación del personal

Manpower cuenta con un plan de contingencia el mismo que incluye:

- Seguridad de la instalación.
- Disponibilidad de recursos de hardware y software en la instalación.
- Disponibilidad de recursos de hardware y software en una instalación alterna.
- Políticas y procedimientos de respaldo de información:

- Recuperación de información.
- Procedimientos de simulacros.

Dentro de lo más importante del plan de seguridad de Manpower debemos mencionar que la empresa cuenta con equipos de computación distribuidos en las oficinas descentralizadas de Manpower en Guayaquil, Manta, Cuenca, etc. que soportan el proceso descentralizado de las mismas y de los cuales uno de los equipos instalado en oficinas de Manpower en Guayaquil tiene las capacidades para desempeñarse eventualmente como servidor de Base de Datos y asumir las funciones del Servidor de la Instalación Central considerado uno de los activos críticos de la empresa. Se mantiene en la oficina de Guayaquil los siguientes recursos de software:

- Copia de los CD's de instalación de Base de Datos Oracle.
- Copia de los CD's de herramientas Developer y Reports de Oracle.
- Copia de CD de aplicativo Gestor.

Existe un procedimiento de simulacros para valorar el impacto real de los escenarios establecidos como posibles en el cual deben participar los recursos humanos técnicos y operativos, sin embargo nunca se ha realizado dichos simulacros.

Todo 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. Cabe mencionar que este plan de contingencia no es revisado ni actualizado periódicamente.

2. Áreas de práctica de seguridad operacionales[39]

En estas áreas nos enfocamos en sus cinco características[40]:

- Responsabilidad
- Procedimientos
- Capacitación
- Problemas Colaborativos[41]

[39] Las características de las áreas de práctica operacionales son las que propone OCTAVE –S, y son las mismas para todas las áreas, excepto el área de Encriptación.
[40] Las definiciones de estos conceptos, se encuentran en el Glosario de términos.

- Verificación

Para las siguientes áreas, nos basamos en las actividades que propone OCTAVE -S en sus hojas de trabajo, para determinar las tareas que se realizan dentro de Manpower para mitigar el riesgo dentro cada área.

2.1 Práctica de Seguridad 7: Control de Acceso Físico.

A esta área de práctica de seguridad se le ha asignado un estado de semáforo amarillo.

Las tareas de mitigación para esta área son realizadas completamente por personal interno de la empresa, y son las siguientes:

- Manpower han instaurado controles de seguridad física para proteger los activos de la empresa y se ha instalado un sistema de alarma para detectar e informar de intrusiones.
- Los servidores se encuentran en una habitación cerrada con acceso restringido y las estaciones de trabajo y ordenadores portátiles están protegidos con cables de seguridad.
- Los documentos confidenciales físicos se almacenan en la oficina del Gerente en Operaciones y Administración y no en un armario con llave como es recomendable.

La empresa no tiene políticas ni procedimientos para controlar el acceso de terceros, y no proporciona oportunidades para que el personal designado asista a capacitación para aprender acerca de cómo supervisar el acceso físico.

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

A esta área de práctica de seguridad se le ha asignado un estado de semáforo amarillo.

Las tareas de mitigación para esta área son realizadas completamente por personal interno a la organización, y son las siguientes:

- Mantener registros de reparaciones y modificaciones al hardware.
- Investigar y hacer frente a cualquier actividad inusual que se identifica.

---

[41] Las características de problemas colaborativos y verificación, se las toman en cuenta únicamente cuando personal externo a la empresa está encargado de las tareas del área.

La organización no tiene políticas ni procedimientos para monitorear el acceso físico al edificio, áreas de trabajo, hardware, software ni medios de comunicación, y no proporciona oportunidades para que el personal designado asista a capacitación para aprender acerca de cómo supervisar el acceso físico.

2.3 Práctica de Seguridad 9: Gestión de Sistemas y Redes

A esta área de práctica de seguridad se le ha asignado un estado de semáforo amarillo.

Las tareas que actualmente se realizan para mitigar esta área son completamente responsabilidad del personal interno de la empresa y son las siguientes:

- Configuración de hardware y software
- Almacenar de forma segura la información sensible
- Comprobar la integridad del software instalado
- Mantener los sistemas actualizados y revisar los avisos de seguridad
- Realización y seguimiento de los cambios en el hardware y software
- Gestión de contraseñas,
- Seleccionar el sistema y las herramientas de gestión de red

Manpower tiene documentado formalmente los procedimientos de gestión de sistemas y redes, aunque los mismos en realidad no son llevados a la práctica.

La empresa en general no ofrece oportunidades a los miembros del personal para asistir a capacitación en gestión de redes, y uso de herramientas de gestión de red.

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

A esta área de práctica de seguridad se le ha asignado un estado de semáforo amarillo.

La empresa dispone de procedimientos informales y no documentados para el monitoreo de acceso a los sistemas y a la red. La tarea que se realiza para hacer frente a esta área es resolver cualquier actividad inusual que se identifique y es realizada por personal de la empresa.

Manpower no ofrece oportunidades a los miembros del personal de TI para asistir a capacitación en el uso de herramientas de seguimiento y auditoría, o monitoreo de acceso a la red y a los sistemas.

2.5 Práctica de Seguridad 11: Autenticación y Autorización

A esta área de práctica de seguridad se le ha asignado un estado de semáforo verde.

Las tareas que actualmente se realizan para mitigar esta área son completamente responsabilidad del personal interno de la empresa y consisten en:

- Implementar controles de acceso para restringir el acceso de los usuarios a la intranet, el sistema gestor y los computadores personales.
- Implementar autenticación de usuario por medio de contraseñas para la intranet, el sistema gestor y los computadores personales.
- El establecimiento y la terminación de acceso a los sistemas e información para individuos y grupos.

La empresa ha documentado formalmente los procedimientos de autorización y autenticación para restringir el acceso de los usuarios a la información, los sistemas sensibles, aplicaciones, servicios, y conexiones de red, pero no ofrece oportunidades a los miembros del personal de TI para asistir a capacitación en temas relacionados con el área.

2.6 Práctica de Seguridad 12: Gestión de Vulnerabilidades

A esta área de práctica de seguridad se le ha asignado un estado de semáforo rojo.

Manpower dispone de procedimientos informales e indocumentados para esta área y la tarea que se realiza para hacerle frente es abordar las vulnerabilidades tecnológicas en el momento que son identificadas, la misma que es completamente responsabilidad del personal interno de la organización.

La empresa no ofrece oportunidades a los miembros del personal de TI para asistir a capacitación en gestión de vulnerabilidades tecnológicas y uso de herramientas de evaluación de vulnerabilidades.

2.7 Práctica de Seguridad 13: Encriptación

A esta área de práctica de seguridad se le ha asignado un estado de semáforo amarillo.

La empresa dispone de procedimientos informales e indocumentados para la implementación y uso de tecnologías de cifrado. La tarea de encriptar información confidencial que se almacena o transmite electrónicamente es completa responsabilidad de personal interno de la empresa.

Manpower no ofrece oportunidades a los miembros del personal para asistir a capacitación en manejo de tecnologías de cifrado.

2.8 Práctica de Seguridad 14: Diseño y Arquitectura de Seguridad

A esta área de práctica de seguridad se le ha asignado un estado de semáforo Rojo

La empresa cuenta con una arquitectura de seguridad informal y no documentada, y no se realiza ninguna tarea para hacer frente a esta área. Además no se ofrece oportunidades a los miembros del personal de TI, para asistir a capacitación en diseño de sistemas de seguridad y redes.

2.9 Práctica de Seguridad 15: Gestión de Incidentes

A esta área de práctica de seguridad se le ha asignado un estado de semáforo verde.

Las tareas que actualmente se realizan para mitigar esta área son completamente responsabilidad del personal interno de la empresa y consisten en:

- Identificar, informar y responder a incidentes de seguridad sospechosos y violaciones.
- Actualizar las licencias de los equipos de hardware y software que posee la empresa.
- Gestionar los respaldos, y procedimientos de recuperación de datos.

Manpower no cuenta con políticas ni procedimientos para la gestión de incidentes. Además, no se ofrece oportunidades a los miembros del personal de TI para asistir a capacitación en gestión de incidentes.

3.2.1.2.2 Actividad S5.2: Seleccionar Enfoques de Mitigación.

En esta actividad desarrollamos los pasos 26 y 27 que se describen a continuación:

Paso 26[42]: En este paso transferimos el estado de semáforo para cada área de práctica de seguridad. De esta forma se tiene una visión global de la interacción de los árboles de amenaza con las áreas de práctica de seguridad. Cabe mencionar que algunas de las áreas de práctica de seguridad se encuentran "bloqueadas" dependiendo del perfil de riesgo, debido a que no es factible que una amenaza afecte al área bloqueada. No se registra el estado de semáforo para las áreas bloqueadas.

Paso 27: En este paso seleccionamos las áreas de práctica de seguridad a las que se va a implementar actividades de mitigación. A las áreas seleccionadas se las conoce como áreas de mitigación.

OCTAVE –S recomienda que se escojan 3 áreas con el fin de evitar tener un plan de seguridad extenso, y centrarse en mitigar los riegos más importantes.

No existe un proceso de selección definido que ayude a escoger las áreas de práctica de seguridad como áreas de mitigación. El equipo de análisis debe utilizar su mejor criterio para realizar esta actividad.

Escogimos 5 áreas basándonos en los siguientes factores definidos por el equipo de análisis:

- El valor de impacto de una amenaza (alto).
- Los estados de semáforo (amarillo y rojo).
- Áreas que tengan un mayor margen de mejora.
- Áreas que puedan mitigar muchos riesgos a más de un activo crítico.

Considerando los factores mencionados, se seleccionaron las siguientes áreas de práctica de seguridad como áreas de mitigación.

Área de mitigación 1: Gestión de Seguridad

A ésta área de práctica de seguridad se la ha escogido como área de mitigación debido a las siguientes razones:

[42] Los resultados de este paso, se encuentran en el anexo C, páginas 20-35

El impacto de las amenazas sobre esta área es alto, debido principalmente a que todas las amenazas descritas en el capítulo 2, pasos 12 a 14 afectan a esta área.

A esta área se le ha asignado un estado de semáforo amarillo, esto significa que necesita mejorar. El margen de mejora para esta área es alto, debido a que en la actualidad Manpower no cuenta con procedimientos formales y definidos para evaluar y gestionar los riesgos de seguridad de la información y no existe un programa de concienciación y capacitación sobre los procesos de gestión de la seguridad de la información. Además, no existe un presupuesto real asignado periódicamente para la seguridad de la información.

Al establecer controles para la gestión de la seguridad se protege a todos los activos de la empresa, de las amenazas a las que se encuentran expuestos.

Área de mitigación 2: Control de acceso físico.

A ésta área de práctica de seguridad se la ha escogido como área de mitigación debido a las siguientes razones:

El impacto de las amenazas sobre esta área es alto, debido principalmente a las amenazas asociadas a actores humanos con acceso físico descritas en el capítulo 2, pasos 12 a 14.

A esta área se le ha asignado un estado de semáforo amarillo, esto significa que necesita mejorar. El margen de mejora para esta área es alto, debido a que en la actualidad Manpower no cuenta con políticas ni procedimientos para controlar el acceso físico a las instalaciones de la empresa. Además no existen roles y responsabilidades definidos claramente para el control de acceso físico.

Al establecer controles para el acceso físico se protege a todos los activos de la empresa, de las amenazas relacionadas con acceso físico.

Área de mitigación 3: Monitoreo y Auditoría de Seguridad Física.

A ésta área de práctica de seguridad se la ha escogido como área de mitigación debido a las siguientes razones:

El impacto de las amenazas sobre esta área es alto, debido principalmente a las amenazas asociadas a actores humanos con acceso físico descritas en el capítulo 2, pasos 12 a 14.

A esta área se le ha asignado un estado de semáforo amarillo, esto significa que necesita mejorar. El margen de mejora para esta área es alto, debido a que en la actualidad Manpower no cuenta con políticas ni procedimientos para monitorear el acceso físico al edificio y áreas de trabajo de la empresa. Además no existen roles y responsabilidades definidos claramente para la gestión de la seguridad física, y la empresa no proporciona al personal capacitaciones periódicas para que tengan un mayor conocimiento de la gestión de la seguridad física.

Al establecer procedimientos para el monitoreo y auditoría de la seguridad física, se identifican las debilidades de seguridad en la infraestructura física, y se implementan controles para proteger a todos los activos de la empresa.

Área de mitigación 4: Gestión de Vulnerabilidades.

A ésta área de práctica de seguridad se la ha escogido como área de mitigación debido a las siguientes razones:

El impacto de las amenazas sobre esta área es alto, debido principalmente a las amenazas asociadas a actores humanos con acceso a la red y problemas del sistema, descritas en el capítulo 2, pasos 12 a 14.

A esta área, se le ha asignado un estado de semáforo rojo, es decir, que presenta carencias severas de seguridad. Esta área tiene un amplio margen de mejora, debido a que en la actualidad, Manpower no cuenta con herramientas ni procedimientos para detectar y eliminar vulnerabilidades.

Establecerse controles ayudaría a detectar y corregir defectos de diseño, implementación o de gestión. Además, corregir las vulnerabilidades de la red de datos de la empresa, protegería a todos los elementos de la red, de los posibles riesgos a los que puedan estar expuestos.

Una de las políticas de Manpower, garantiza a sus clientes que la información proporcionada solo puede ser usada con fines de selección. Corregir las vulnerabilidades encontradas en la red, disminuiría la probabilidad que atacantes externos puedan ingresar ilícitamente a la red y extraer dicha información.

Área de mitigación 5: Diseño y Arquitectura de Seguridad

A ésta área de práctica de seguridad se la ha escogido como área de mitigación debido a las siguientes razones:

A esta área, se le ha asignado un estado de semáforo rojo, es decir, que presenta carencias severas de seguridad. El margen de mejora para esta área es alto, debido a que en la actualidad, Manpower no tiene documentado ni el diagrama de topología de red, mucho menos un diagrama de seguridad.

El diseño de un diagrama de Arquitectura de Seguridad de Información, ligado a un conjunto de mejores prácticas dirigidas a la adaptabilidad de la seguridad, escalabilidad, manejabilidad etc, protege a todos los activos de la empresa, de las amenazas a las que se encuentran expuestos. Además, asegura que la estrategia de negocio y la seguridad de las tecnologías de la información están alineadas, y apoyan la toma de decisiones.

3.2.1.2.3 Actividad S5.3: Desarrollar Planes de Mitigación de Riesgos.

En esta actividad desarrolla el paso 28 que se describe a continuación:

Paso 28: En este paso desarrollamos los planes de mitigación de riesgos para las áreas seleccionadas en el paso 27.

Un plan de mitigación de riesgos tiene como objetivo reducir los riesgos a un activo crítico y generalmente incorporan actividades o medidas para contrarrestar las amenazas a los activos.

OCTAVE –S proporciona una guía con actividades de mitigación para cada una de las áreas de práctica de seguridad. Consideramos las actividades de mitigación que proporciona la herramienta y las adaptamos para desarrollar el plan de seguridad.

A continuación se muestran los resultados para cada una de las áreas de práctica de seguridad seleccionadas.

1. **Área de Mitigación: Gestión de la Seguridad**[43]

Roles y Responsabilidades.

La empresa debe documentar los roles y responsabilidades de seguridad, esta actividad debe ser llevada a cabo por el Gerente de Operaciones y Administración y la Administradora de Sistemas y deben proporcionar dicha documentación a todo el personal de la empresa. Actualmente la única encargada de la seguridad

[43] Los ítems considerados para esta área son los que propone OCTAVE –S.

de la información es la Administradora de Sistema, la cual no emite informes de los problemas y soluciones que se les brindaron a los incidentes de seguridad cuando estos se presentan en las estaciones de trabajo de la empresa.

Al documentar los roles y responsabilidades de seguridad existirá un mejor manejo de los incidentes de seguridad y una supervisión constante por parte del Gerente de Operaciones y Administración sobre la Administradora de Sistemas.

Manpower cuenta con políticas y procedimientos para la utilización de los recursos informáticos dentro de la empresa, los mismos que deben ser recibidos, leídos, firmados y aceptados por todos los empleados. Sin embargo, dichas políticas y procedimientos no han sido actualizados desde el 2007.

El equipo de análisis definió que las actividades de revisión y actualización de las políticas y procedimientos para la utilización de los recursos informáticos deben realizarse periódicamente dos veces por año para brindar mayor seguridad a los recursos de tecnología de la información. Las actividades de actualización y mejora en las políticas y procedimientos mencionados deben estar a cargo del Gerente de Operaciones y Administración conjuntamente con la Administradora de Sistemas.

Financiamiento

Manpower debe incluir un presupuesto anual para las diferentes actividades de seguridad de la información. La determinación de dichos fondos se realizará utilizando procesos formales de evaluación de riesgos. La información que se maneja sobre todo en el Sistema Gestor y en el Servidor de BDD es muy sensible para la empresa, es por esto que incluir un presupuesto para la seguridad de la información es de vital importancia. La gestión de los fondos destinados a la seguridad de la información estará a cargo de la Administradora de Sistemas.

Procedimientos de Recursos Humanos

Manpower cuenta con políticas y procedimientos en los que incluyen consideraciones de seguridad al momento de contratar un nuevo empleado y también cuando se da por terminado la relación entre la empresa y un miembro del personal. Sin embargo, dichas políticas y procedimientos no han sido actualizados desde el 2007. El equipo de análisis definió que las actividades de revisión y actualización de estas políticas y procedimientos deben realizarse una

vez por año para contar con una cantidad mayor de factores a considerar en estos tipos de procesos con los empleados y postulantes a formar parte de la empresa. Los responsables de realizar estas actividades son el Gerente de Operaciones y Administración conjuntamente con la Coordinadora Administrativa.

Gestión de Riesgos

La empresa debe crear y documentar políticas y procedimientos formales para evaluar y gestionar los riesgos de seguridad de la información. Contar con políticas y procedimientos para la gestión de riesgos es de vital importancia para la empresa sobre todo si se toma en cuenta que se mejorará las estrategias del Área de Tecnología de la Información. El proceso de documentación de la Gestión de riesgos también ayudará como documento de apoyo para la gestión de presupuesto. Los responsables de realizar estas actividades son el Gerente de Operaciones y Administración conjuntamente con la Administradora de Sistemas.

Gestión de Almacenamiento y Comunicación de Datos

Manpower debe crear y documentar políticas y procedimientos formales para el almacenamiento y la comunicación de datos utilizando un algoritmo de cifrado que maneje claves de 128 bits como AES o 3DES. Este tipo de algoritmos permitirá dificultar la intrusión por ataques de fuerza bruta y brindar mayor seguridad a la información crítica de la empresa.

Esta actividad de creación y documentación de las políticas y procedimientos para el almacenamiento y la comunicación de datos debe ser realizada por la Administración de Sistemas bajo la supervisión del Gerente de Operaciones y Administración y deben ser entregados a los miembros del personal para que todos las conozcan y las apliquen de una manera adecuada.

Clasificación de datos.

Manpower debe crear y documentar políticas y procedimientos formales para la clasificación de datos para impedir que personal no autorizado tenga acceso a la información confidencial de la empresa. Si el personal no sabe qué datos de la empresa son confidenciales, existe una alta probabilidad de que esta información quede expuesta a personas no autorizadas.

Esta actividad de creación y documentación de las políticas y procedimientos para la clasificación de datos debe ser realizada por la Administración de Sistemas bajo la supervisión del Gerente de Operaciones y Administración y deben ser entregados a los miembros del personal para que todos los conozcan y las apliquen de una manera adecuada.

Alertas al Personal

La empresa debe proporcionar a todos los miembros del personal capacitación relacionada con seguridad de la información periódicamente 2 veces por año. Adicionalmente el personal de TI debe recibir capacitaciones relacionadas con la gestión de la seguridad 3 veces por año.

Dentro de las políticas y procedimientos para la utilización de los recursos informáticos, los mismos que deben ser recibidos, leídos y aceptados por todos los empleados de Manpower, constan de actividades relacionadas con seguridad pero el equipo de análisis definió que se debe incluir una política y procedimiento para reportar los incidentes de seguridad al área de tecnología de la información.

Las actividades de capacitación deben ser coordinadas por el Gerente de Operaciones y Administración conjuntamente con la Administradora de Sistemas. La actividad de creación de la política y procedimiento para reportar los incidentes de seguridad al área de tecnología de la información debe ser realizada por la Administradora de Sistemas y supervisada por el Gerente de Operaciones y Administración.

Alertas para la gestión

Manpower debe crear una política y procedimiento formal para proporcionar a los altos funcionarios de la empresa con reportes y resúmenes periódicos trimestrales de información importante relacionada con seguridad. La Administradora de Sistemas elaborará una planilla de resumen ejecutivo y lo distribuirá por medio impreso o digital a los respectivos Gerentes de la empresa. La actividad de creación y aplicación de la política y procedimiento para proporcionar a los altos funcionarios de la empresa con reportes y resúmenes relacionados con seguridad debe ser realizada por la Administradora de Sistemas y supervisada por el Gerente de Operaciones y Administración.

Verificación

La empresa a través de la Administradora de Sistemas debe verificar que:

El personal conoce, acepta y firma las medidas de seguridad establecidas, los acuerdos de confidencialidad y sus responsabilidades relacionadas con seguridad.

2. Área de Mitigación: Control de Acceso Físico[44]

Responsabilidad

Manpower debe designar roles y responsabilidades para controlar el acceso físico al edificio, áreas de trabajo, hardware de TI y software. Actualmente la empresa controla el acceso a personal de la empresa de una manera informal y sin llevar registros escritos. Además, la empresa no tiene un responsable de registrar el ingreso a las instalaciones de los visitantes. Designar roles y responsabilidades para controlar el acceso físico a las instalaciones, permitirá proteger a todos los activos de la empresa, de las amenazas relacionadas con acceso físico.

La actividad de designar roles y responsabilidades para controlar el acceso físico debe ser realizada por el Gerente de Operaciones y Administración y supervisada por la Gerente General.

Procedimientos

La empresa debe crear y documentar políticas y procedimientos formales para controlar el acceso físico al edificio, áreas de trabajo, hardware de TI y software. Las actividades que proponemos a continuación deben formar parte de las políticas y procedimientos para el control de acceso físico.

- Implementar hojas de registro para que sean llenadas con los datos de las personas que ingresan a las instalaciones (visitantes). Los datos deben incluir: nombres, número de cédula, motivo, hora de ingreso y hora de salida.
- Implementar tarjetas de acceso para que sean entregadas a las personas que se dirigen a las diferentes oficinas de la empresa (visitantes).
- Implementar un mecanismo formal (hojas de registro o timbres) para controlar la hora de ingreso y de salida de los miembros del personal.

[44] Los ítems considerados para esta área son los que propone OCTAVE –S.

- Contratar los servicios de guardias de seguridad para proteger las instalaciones.
- En lo posible, reorganizar la disposición física de los equipos informáticos en áreas específicas para contrarrestar las amenazas relacionadas con desastres naturales.

Es muy importante que la empresa cuente con procedimientos formales para que terceros accedan a las instalaciones y áreas de trabajo para evitar en lo posible daños y/o perdidas de los activos. Además, es importante controlar que los miembros del personal cumplen con su horario de trabajo.

Las actividades de mitigación mencionadas deben ser creadas y documentadas por el Gerente de Operaciones y Administración y supervisada por la Gerente General.

Capacitación

Manpower debe proporcionar a determinados miembros del personal capacitaciones relacionadas con el control de acceso físico a las instalaciones de una empresa. Es muy importante que Manpower proporcione dichas capacitaciones con el fin de contar con personal apto para realizar las actividades de control de acceso físico.

Las actividades de capacitación al personal de la empresa deben ser gestionadas por el Gerente de Operaciones y Administración.

Verificación

La empresa debe implementar mecanismos formales para verificar que las actividades de mitigación para esta área se cumplen, y documentar todos los procesos de verificación, esto con el fin de gestionar de una manera correcta el control de acceso físico. Esta actividad deberá realizarse trimestralmente y el responsable de esta actividad es el Gerente de Operaciones y Administración.

3. Área de Mitigación: Monitoreo y Auditoría de Seguridad Física[45]

Responsabilidad

Manpower debe crear y documentar políticas y procedimientos formales para implementar monitoreos y auditorías de la seguridad física de la empresa, ya que

[45] Los ítems considerados para esta área son los que propone OCTAVE –S.

esta actividad no es realiza por ningún miembro del personal en la actualidad. En dichas políticas y procedimientos se debe tomar en cuenta el control sobre las áreas de trabajo, el hardware y software de TI y se deben definir roles y responsabilidades tanto para controlar como para hacer frente a posibles eventualidades inusuales que se identifiquen. La actividad de creación de las políticas y procedimientos para implementar monitoreos y auditorías de la seguridad física debe ser realizada por la Administradora de Sistemas y supervisada por el Gerente de Operaciones y Administración.

Procedimientos

Manpower debe crear y documentar políticas y procedimientos formales para monitorear el acceso físico a las instalaciones de la empresa ya que a pesar de que se hayan instaurado controles de seguridad física para proteger los activos de la empresa y se ha instalado un sistema de alarma para detectar e informar de intrusiones, estos no son suficientes para garantizar la seguridad de los activos y evitar pérdidas de equipos de TI o de información crítica.

Las actividades que proponemos a continuación deben formar parte de las políticas y procedimientos para el monitoreo y auditoria de las seguridad física.

- La Administradora de Sistemas supervisada por el Gerente de Operaciones y Administración debe realizar un monitoreo trimestral y llevar registro del inventario de hardware y software de la empresa.
- En lo posible, instalar cámaras de seguridad en la entrada al edificio, en los pasillos y en cada una de las oficinas con las que cuenta la empresa.
- Ampliar los requerimientos a nivel de control de acceso físico, impidiendo el acceso a personas en estado etílico. Esta actividad le corresponde a los guardias de seguridad los mismos que deben recibir capacitaciones periódicas relacionadas con la seguridad física.

Es muy importante que la empresa cuente con procedimientos formales para que terceros accedan a las instalaciones y áreas de trabajo para evitar en lo posible daños y/o perdidas de los activos.

Las actividades de mitigación mencionadas deben ser documentadas por la Administradora de Sistemas y supervisada por el Gerente de Operaciones y Administración.

Capacitaciones

Manpower debe proporcionar a determinados miembros del personal capacitaciones relacionadas con el monitoreo de acceso físico a las instalaciones de una empresa. Es muy importante que Manpower proporcione dichas capacitaciones con el fin de contar con personal apto para realizar los monitoreos y auditorías de seguridad física.

Las actividades de capacitación al personal de la empresa deben ser gestionadas por el Gerente de Operaciones y Administración.

Verificación

La empresa debe implementar mecanismos formales para verificar que las actividades de mitigación para esta área se cumplen, y documentar todos los procesos de verificación, esto con el fin de gestionar de una manera correcta el monitoreo y auditoría de la seguridad física. Esta actividad deberá realizarse trimestralmente y el responsable de esta actividad es el Gerente de Operaciones y Administración.

4. Área de Mitigación 12: Gestión de Vulnerabilidades[46].

Responsabilidad

Manpower debe crear y documentar políticas y procedimientos formales para la gestión de vulnerabilidades de la red de información, y definir los roles y responsabilidades de todo el personal involucrado, ya que en la actualidad todas las tareas de seguridad de la información están a cargo de la Administradora de Sistemas, y no se tiene herramientas, ni tareas asignadas para detectar vulnerabilidades en la red de la empresa. El equipo de análisis determino que el personal de Ti que actualmente tiene la empresa es insuficiente, por lo que se recomienda que para no sobrecargar de trabajo a la Administradora de sistemas, se contrate nuevo personal en el área de Ti, o a una empresa externa especializada que se dedique exclusivamente a monitorear e informar de las vulnerabilidades detectadas en la red de datos de Manpower.

[46] Los ítems considerados para esta área son los que propone OCTAVE –S.

La actividad de creación de las políticas y procedimientos para la Gestión de vulnerabilidades será responsabilidad de la Administradora de sistemas en colaboración con el gerente de operaciones y administración.

Procedimientos

Manpower debe crear políticas y procedimientos para la gestión de vulnerabilidades ya que solo se detecta una vulnerabilidad en el momento que se produce un incidente.

El proceso de gestión de vulnerabilidades incluye el descubrimiento de vulnerabilidad, análisis de riesgos, medidas de mitigación, y una infraestructura que permita un adecuado y continuo monitoreo, seguimiento y mejora.

A continuación el equipo de análisis propone los pasos y actividades a seguir para determinar las vulnerabilidades dentro de la red de la empresa:

Preparación inicial:

- Establecer las políticas y procedimientos de seguridad
- Establecer los roles y responsabilidades del personal involucrado en el proceso
- Establecer un inventario de activos de TI.
- Establecer los roles de los activos del inventario.
- Desarrollar métricas de seguridad de la información.
- Establecer la línea base donde se comienza y el gap donde se desea llegar.

Pasos:

- Identificación
    - Crear el inventario y categorizar los activos
    - Identificar en el inventario el rol, criticidad de negocio, unidad de negocio, agrupación geográfica o lógica.
    - Priorización por impacto al negocio
- Evaluación.- La detección de vulnerabilidades
- Verificación de la vulnerabilidad contra el inventario: Revisar y verificar la existencia de una vulnerabilidad contra la base de datos del inventario, lo

que permite reducir el esfuerzo que se dedica a controlar una vulnerabilidad que no aplica a la configuración de la red

- Clasificación y valoración del riesgo: Las vulnerabilidades deben se categorizadas, segmentadas y priorizadas en base a la criticidad del activo para el negocio
- Remediación: Es el proceso de control de la vulnerabilidad que puede ser directa o indirecta.

Verificación

El presente documento puede servir de ayuda a la empresa para la elaboración de estas tareas, ya que en el mismo se han identificado los activos que posee la empresa, los activos críticos, y los posibles riesgos a los que estos pueden estar sometidos.

A continuación el equipo de análisis propone un conjunto de actividades que se recomienda formen parte de las políticas y procedimientos para gestión de vulnerabilidades:

- Actividades iniciales.
    - Remover servicios, funciones, usuarios no requeridos
    - Mantener solo una función por servidor
    - Cambiar las configuraciones de fábrica en Sistemas Operativos y Aplicaciones.
    - Instalar parches al Sistema operativo
    - Instalar aplicaciones adicionales (solo requeridas)
    - Instalar parches de aplicaciones adicionales
    - Instalar y mantener un antivirus
    - Documentar estándar de configuración
    - Implementar respaldos y bitácoras
    - Generar lista de revisión
- Seleccionar las herramientas de evaluación de vulnerabilidades, listas de control y secuencias de comandos, tomando en cuenta que las mismas posean las siguientes características:
    - Sistema de tickets y workflow
    - Sistema de reportes en el tiempo

    - Permita la clasificación y el inventario de activos
    - Permita la clasificación correcta y valoración del riesgo de activos
    - Permita el establecimiento de pruebas por cronograma
    - Permita establecer los roles de los activos
    - La creación de los roles de personal involucrado en el proceso
- Programar y realizar evaluaciones de vulnerabilidad de tecnología en forma periódica.
- Mantenerse al día con los tipos de vulnerabilidades conocidas y métodos de ataque.
- Revisar las fuentes de información sobre anuncios de vulnerabilidad, alertas de seguridad y comunicaciones.
- Interpretar los resultados de las evaluaciones de vulnerabilidades tecnológicas realizadas.
- Mantener un almacenamiento seguro y disponible de los datos de vulnerabilidades tecnológicas
- Realizar una auditoría de las tecnologías de información para identificar las debilidades de seguridad en la infraestructura informática.
- Contratar a una organización externa para atacar los sistemas de la organización y a la red a través de Internet (es decir, pruebas de penetración).
- En caso de contratar a una empresa externa para que se encargue de esta área. Organizar una reunión con todos los contratistas correspondientes, proveedores de servicios y terceros, para comunicar los requisitos, y comprobar que dichos requisitos se han cumplido.

Capacitaciones

Manpower debe proporcionar al personal involucrado en esta tarea capacitaciones relacionadas con Gestión de vulnerabilidades, y uso de herramientas de evaluación de vulnerabilidades.

Las actividades de capacitación al personal de la empresa deben ser gestionadas por el Gerente de Operaciones y Administración.

En el caso de que Manpower decida contratar una empresa externa para que se encargue de las actividades de esta área, la tarea de selección será responsabilidad del Gerente de Operaciones y Administración.

Verificación

La empresa debe implementar mecanismos formales para verificar que las actividades de mitigación para esta área se cumplen, y documentar todos los procesos de verificación.

Esta actividad deberá realizarse trimestralmente y el responsable de esta actividad es el Gerente de Operaciones y Administración.

En el caso de que esta tarea la realice una empresa externa, se debe Implementar un mecanismo formal (por ejemplo, a través de un contrato) para verificar que los requisitos de la organización para la gestión de vulnerabilidades tecnológicas se han cumplido por todos los contratistas, proveedores de servicios y terceros correspondientes.

5. Área de Mitigación 14: Arquitectura y Diseño de la Seguridad[47].

Roles y Responsabilidades.

La empresa debe documentar formalmente la arquitectura de seguridad, las prácticas de diseño, y definir los roles y responsabilidades del personal involucrado en esta tarea. Estas actividades otorgaran mayores responsabilidades al Jefe de sistemas y a todo el personal de TI, en especial a la Administradora de Sistemas ya que es quien actualmente es responsable de Administrar la red, y de la Arquitectura y el diseño de seguridad de la información. Estas actividades se hallan bajo supervisión del Gerente de Operaciones y Administración. Todo cambio en la arquitectura debe ser aprobado por el comité técnico.

Procedimientos

Hasta antes del presente proyecto la empresa no contaba con el diagrama de topología de la red, y nunca se ha hecho de manera organizada e integral el diseño y arquitectura de seguridad en la red de información. Es por ello que no hay diagramas que muestren la arquitectura de la seguridad de la red en la topología actual. El documentar formalmente las prácticas y procedimientos de

[47] Los ítems considerados para esta área son los que propone OCTAVE –S.

Arquitectura y Diseño de Seguridad de la información, facilita la presentación de propuestas ante las autoridades y agilitan su gestión.

Entrenamiento

En el actual equipo de Ti con que cuenta la empresa, no se tienen miembros que tengan experiencia en el diseño y arquitectura de redes seguras. Por ello se recomienda que los miembros de ti delegados en esta área deban asistir a cursos de entrenamiento en el diseño de sistemas y redes seguras.

Asuntos colaborativos

Como no se tiene personal suficiente ni capacitado adecuadamente para gestionar esta área, se recomienda que se contrate una empresa especializada que se encargue del diseño de la arquitectura de seguridad.

El equipo de análisis según los resultados obtenidos en la presente evaluación, determino que las principales necesidades de la red de la empresa son las siguientes:

- Implementar un firewall que soporte VPN para que los usuarios puedan realizar acceso remoto a través del internet
- Instalar un servidor proxy para proteger las direcciones IP de la red de datos.
- Implementar un sistema inspector de contenido web, para optimizar el uso del ancho de banda de internet
- Implementar un sistema de detección de intrusos basado en Host, para detectar anomalías que indiquen un riesgo potencial, revisando las actividades en la máquina (host).
- Implementar el servicio NAT, Network Address Translation o traducción de direcciones de red en el mismo firewall.

Con el diseño propuesto, contactar con otras empresas o la misma que vendan equipos que cumplan con los requisitos anteriormente expuestos.

Requerimientos y verificación

El diseño de la red segura, deberá ser revisado y aprobado por el comité de la empresa. Una vez aprobado el Gerente de Operaciones y Administración, gestionara el financiamiento de todos los nuevos equipos que sean necesarios, y

se establecerán procedimientos para verificar que la nueva arquitectura cumpla con los objetivos propuestos.

En caso de que se contrate una empresa externa para la realización de esta tarea, se debe Implementar un mecanismo formal de control, por medio de un contrato para verificar que se cumpla con los requisitos de la organización

Actividades de mitigación

- Documentar los diagramas que muestran la arquitectura de seguridad en toda la empresa, y la topología de la red.
- Diseñar controles de seguridad en sistemas y redes, nuevos y revisados.
- Actualizar el diseño de los sistemas utilizados, para incluir controles de seguridad apropiados.
- Investigar los incidentes periódicos en los sistemas utilizados, y corregir los problemas de diseño que provocan estos incidentes.
- En el caso de que esta tarea la realice una empresa externa. Organizar una reunión con todos los contratistas correspondientes, proveedores de servicios y terceros para comunicar los requisitos, y comprobar que dichos requisitos se han cumplido.

3.2.1.2.4 Actividad S5.4: Identificar Cambios en la Estrategia de Protección.

En esta actividad desarrollamos el paso 29 que se describe a continuación:

Paso 29: En este paso revisamos cada una de las áreas seleccionadas y verificamos si existe un cambio que se presente en la estrategia de protección para la respectiva área de práctica de seguridad. Dichos cambios generalmente tienen que ver con los roles y responsabilidades en cada una de las áreas.

El equipo de análisis debe transcribir las sugerencias de cambio a las actividades de mitigación.

Cabe recalcar que todas estas características ya fueron tomadas en cuenta en el paso 28 en donde se desarrolla el plan de mitigación, y dentro del cual se definen las responsabilidades para cada una de las actividades de mitigación.

3.2.1.2.5 Actividad S5.5: Identificar los Pasos Siguientes.

En esta actividad se desarrolla el paso 30 que se describe a continuación:

Paso 30[48]: En este paso determinamos un conjunto de actividades para facilitar la implementación de los resultados obtenidos durante el proceso de evaluación. Con este paso se marca el final de la evaluación de riesgos de la información.

Dentro de este conjunto de actividades se debe tomar en cuenta los siguientes puntos propuestos por OCTAVE -S:

- El apoyo por parte de los altos funcionarios.
- Aplicación de las actividades de mitigación.
- Monitoreo de la implementación del plan.
- Realización de evaluaciones posteriores.

A continuación se muestra el conjunto de actividades que el equipo de análisis definió para dar apoyo a la implementación de los resultados obtenidos durante la evaluación.

- Los altos funcionarios de Manpower deben proporcionar un presupuesto para implementar el plan de seguridad.
- Manpower debe considerar a la seguridad de la información como una prioridad dentro de sus procesos de negocio.
- Los responsables de crear y desarrollar las diferentes políticas y procedimientos propuestos por el equipo de análisis deberán proporcionar una documentación detallada de los mismos a todos los miembros del personal para que sean revisados.
- La Administradora de Sistemas deberá emitir informes sobre el grado de implementación y cumplimiento del plan de seguridad.
- El Gerente de Operaciones y Administración deberá monitorear constantemente la implementación y cumplimiento del plan de seguridad.
- Manpower debe asegurar que los miembros del personal tengan el tiempo suficiente para participar en todas las actividades relacionadas con seguridad.

[48] El conjunto de actividades descritas en este paso son las que propone OCTAVE –S, adaptas al proyecto.

- Es importante que el personal de TI este al día en lo que respecta a nuevas amenazas frente a virus, ataques de denegación de servicio, etcétera y que adopte las medidas necesarias de actualización de hardware y software.
- Se recomienda realizar otra evaluación de riesgos a la información de 18 a 24 meses a partir de la implementación del plan de seguridad propuesto.

3.3 PLAN GENERAL 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.

3.3.1 Área: Gestión de la Seguridad

Actividades de Mitigación

- Documentar los roles y responsabilidades de seguridad y proporcionar dicha documentación a todo el personal de la empresa.
- Desarrollar y documentar políticas y procedimientos para la utilización de los recursos informáticos de la empresa.
- Incluir un presupuesto anual para las diferentes actividades de seguridad de la información. La determinación de dichos fondos se realizará utilizando procesos formales de evaluación de riesgos.
- Actualizar las políticas y procedimientos de la empresa en los que incluyen consideraciones de seguridad al momento de contratar un nuevo empleado o al dar por terminado la relación entre la empresa y un miembro del personal. Los procedimientos que se deben incluir son:
- Notificación a todos los departamentos (Recursos humanos, TI, Seguridad física, Servicio de atención al cliente, Finanzas, etc.)
- 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.)

- Crear y documentar políticas y procedimientos formales para evaluar y gestionar los riesgos de seguridad de la información.
- Desarrollar y documentar políticas y procedimientos formales para el almacenamiento y la comunicación de datos utilizando un algoritmo de cifrado que maneje claves de 128 bits como AES o 3DES.
- Crear y documentar políticas y procedimientos formales para clasificar la información e impedir que personal no autorizado tenga acceso a datos confidenciales de la empresa.
- Desarrollar y documentar una política y procedimiento para reportar los incidentes de seguridad al área de tecnología de la información.
- Proporcionar a todos los miembros del personal capacitación relacionada con seguridad de la información periódicamente 2 veces por año.
- Proporcionar al personal de TI debe recibir capacitaciones relacionadas con la gestión de la seguridad 3 veces por año.
- Desarrollar una política y procedimiento formal para proporcionar a los altos funcionarios de la empresa con reportes y resúmenes periódicos trimestrales de información importante relacionada con seguridad.
- Verificar que el personal conoce, acepta y firma las medidas de seguridad establecidas, los acuerdos de confidencialidad y sus responsabilidades relacionadas con seguridad.
- Revisar y actualizar las políticas y procedimientos para el área de gestión de seguridad dos veces por año.

Roles y Responsabilidades

- Las actividades de desarrollo y actualización de las políticas y procedimientos deben estar a cargo del Gerente de Operaciones y Administración conjuntamente con la Administradora de Sistemas.
- La gestión de los fondos destinados a la seguridad de la información estará a cargo de la Administradora de Sistemas.
- Las actividades de actualización de políticas y procedimientos en los que incluyen consideraciones de seguridad al momento de iniciar o terminar la relación con un empleado deben ser realizadas por el Gerente de

Operaciones y Administración conjuntamente con la Coordinadora Administrativa.

- Los responsables de realizar la actividad de creación y documentación de las políticas y procedimientos para evaluar y gestionar los riesgos de seguridad de la información son el Gerente de Operaciones y Administración conjuntamente con la Administradora de Sistemas.
- La actividad de creación y documentación de las políticas y procedimientos para el almacenamiento, comunicación y clasificación de datos está a cargo de la Administración de Sistemas bajo la supervisión del Gerente de Operaciones y Administración y deben ser entregados a los miembros del personal para que todos las conozcan y las apliquen de una manera adecuada.
- Las actividades de capacitación deben ser coordinadas por el Gerente de Operaciones y Administración conjuntamente con la Administradora de Sistemas.
- La actividad de creación de la política y procedimiento para reportar los incidentes de seguridad al área de tecnología de la información debe ser realizada por la Administradora de Sistemas y supervisada por el Gerente de Operaciones y Administración.
- La actividad de creación y aplicación de la política y procedimiento para proporcionar a los altos funcionarios de la empresa con reportes y resúmenes relacionados con seguridad debe ser realizada por la Administradora de Sistemas y supervisada por el Gerente de Operaciones y Administración.
- La Administradora de Sistemas bajo la supervisión del Gerente de Operaciones y Administración debe verificar que los empleados lean, firmen y apliquen las medidas de seguridad establecidas.

3.3.2 Área: Control de Acceso Físico

Actividades de Mitigación

- Designar roles y responsabilidades para controlar el acceso físico al edificio, áreas de trabajo, hardware de TI y software.

- Crear y documentar políticas y procedimientos formales para controlar el acceso físico al edificio, áreas de trabajo, hardware de TI y software.
- Implementar hojas de registro para que sean llenadas con los datos de las personas que ingresan a las instalaciones (visitantes). Los datos deben incluir: nombres, número de cédula, motivo, hora de ingreso y hora de salida.
- Implementar tarjetas de acceso para que sean entregadas a las personas que se dirigen a las diferentes oficinas de la empresa (visitantes).
- Implementar un mecanismo formal (hojas de registro o timbres) para controlar la hora de ingreso y de salida de los miembros del personal.
- Contratar los servicios de guardias de seguridad para proteger las instalaciones.
- En lo posible, reorganizar la disposición física de los equipos informáticos en áreas específicas para contrarrestar las amenazas relacionadas con desastres naturales.
- Proporcionar a determinados miembros del personal capacitaciones relacionadas con el control de acceso físico al edificio, instalaciones y áreas de trabajo. Implementar mecanismos formales para verificar que las actividades de mitigación para esta área se cumplen, y documentar todos los procesos de verificación.
- 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.
- 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.
- 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.

Roles y Responsabilidades

- La actividad de creación de las políticas y procedimientos para implementar controles de acceso físico debe ser realizada por el Gerente de Operaciones y Administración y supervisada por la Gerente General.
- Las actividades de mitigación para el control de acceso físico deben ser documentadas por el Gerente de Operaciones y Administración y supervisada por la Gerente General.
- Las actividades de capacitación al personal de la empresa deben ser gestionadas por el Gerente de Operaciones y Administración.
- El responsable de la actividad de verificación es el Gerente de Operaciones y Administración.

3.3.3 Área: Monitoreo y Auditoría de Seguridad Física

Actividades de mitigación:

- Crear y documentar políticas y procedimientos formales para implementar monitoreos y auditorías de la seguridad física de la empresa tomando en cuenta el control sobre las áreas de trabajo, el hardware y software de TI.
- Desarrollar y documentar políticas y procedimientos formales para monitorear el acceso físico a las instalaciones de la empresa. Las actividades que el equipo de análisis recomienda a continuación deben formar parte de las políticas y procedimientos para el monitoreo y auditoría de las seguridad física.
- Realizar un monitoreo trimestral y llevar registro del inventario de hardware y software de la empresa.
- En lo posible, instalar cámaras de seguridad en la entrada al edificio, en los pasillos y en cada una de las oficinas con las que cuenta la empresa.
- Ampliar los requerimientos a nivel de control de acceso físico, impidiendo el acceso a personas en estado etílico. Esta actividad le corresponde a los guardias de seguridad los mismos que deben recibir capacitaciones periódicas relacionadas con la seguridad física.

- Proporcionar a determinados miembros del personal capacitaciones relacionadas con monitoreo de acceso físico a las instalaciones y áreas de trabajo.
- Implementar y documentar mecanismos formales para verificar que las actividades de mitigación recomendadas al área de seguridad física se cumplen. Esta actividad de verificación deberá realizarse trimestralmente.

Roles y Responsabilidades

- La actividad de creación de las políticas y procedimientos para implementar monitoreos y auditorías de la seguridad física debe ser realizada por la Administradora de Sistemas y supervisada por el Gerente de Operaciones y Administración.
- Las actividades de mitigación para monitorear el acceso físico a las instalaciones de la empresa deben ser documentadas por la Administradora de Sistemas y supervisada por el Gerente de Operaciones y Administración.
- Las actividades de capacitación al personal de la empresa deben ser gestionadas por el Gerente de Operaciones y Administración.
- El responsable de la actividad de verificación es el Gerente de Operaciones y Administración.

3.3.4 Área: Gestión de Vulnerabilidades

Actividades de mitigación:

El proceso de gestión de vulnerabilidades incluye el descubrimiento de vulnerabilidad, análisis de riesgos, medidas de mitigación, y una infraestructura que permita un adecuado y continuo monitoreo, seguimiento y mejora.

A continuación el equipo de análisis propone los pasos y actividades a seguir para determinar las vulnerabilidades dentro de la red de la empresa:

Preparación inicial:

- Establecer las políticas y procedimientos de seguridad
- Establecer los roles y responsabilidades del personal involucrado en el proceso

- Establecer un inventario de activos de la plataforma tecnológica
- Establecer los roles de los activos del inventario
- Desarrollar métricas de seguridad de la información
- Establecer la línea base donde se comienza y el gap donde se desea llegar

Pasos:

- Identificación
    - Crear el inventario y categorizar los activos
    - Identificar en el inventario el rol, criticidad de negocio, unidad de negocio, agrupación geográfica o lógica.
    - Priorización por impacto al negocio
- Evaluación.- La detección de vulnerabilidades
- Verificación de la vulnerabilidad contra el inventario: Revisar y verificar la existencia de una vulnerabilidad contra la base de datos del inventario, lo que permite reducir el esfuerzo que se dedica a controlar una vulnerabilidad que no aplica a la configuración de la red
- Clasificación y valoración del riesgo: Las vulnerabilidades deben se categorizadas, segmentadas y priorizadas en base a la criticidad del activo para el negocio
- Remediación: Es el proceso de control de la vulnerabilidad que puede ser directa o indirecta.
- Verificación

El presente documento puede servir de ayuda a la empresa para la elaboración de estas tareas, ya que en el mismo se han identificado los activos que posee la empresa, los activos críticos, y los posibles riesgos a los que estos pueden estar sometidos.

A continuación el equipo de análisis propone un conjunto de actividades que se recomienda formen parte de las políticas y procedimientos para gestión de vulnerabilidades:

- Definir los roles y responsabilidades de todo el personal involucrado.
- Actividades iniciales:
    - Remover servicios, funciones, usuarios no requeridos

  - Mantener solo una función por servidor
  - Cambiar las configuraciones de fábrica en Sistemas Operativos y Aplicaciones.
  - Instalar parches al Sistema operativo
  - Instalar aplicaciones adicionales (solo requeridas)
  - Instalar parches de aplicaciones adicionales
  - Instalar y mantener un antivirus
  - Documentar estándar de configuración
  - Implementar respaldos y bitácoras
- Generar lista de revisión
- 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
- Seleccionar las herramientas de evaluación de vulnerabilidades, listas de control y secuencias de comandos, tomando en cuenta que las mismas posean las siguientes características:
  - Sistema de tickets y workflow
  - Sistema de reportes en el tiempo
  - Permita la clasificación y el inventario de activos
  - Permita la clasificación correcta y valoración del riesgo de activos
  - Permita el establecimiento de pruebas por cronograma
  - Permita establecer los roles de los activos
  - La creación de los roles de personal involucrado en el proceso
- Programar y realizar evaluaciones de vulnerabilidad de tecnología en forma periódica.
- Mantenerse al día con los tipos de vulnerabilidades conocidas y métodos de ataque.
- Revisar las fuentes de información sobre anuncios de vulnerabilidad, alertas de seguridad y comunicaciones.
- Si no existen actualizaciones disponibles para vulnerabilidades de seguridad conocidas, intente averiguar cuándo podrá disponer de una y desarrolle un plan de seguridad provisional.

- Interpretar los resultados de las evaluaciones de vulnerabilidades tecnológicas realizadas.
- Mantener un almacenamiento seguro y disponible de los datos de vulnerabilidades tecnológicas
- Realizar una auditoría de las tecnologías de información para identificar las debilidades de seguridad en la infraestructura informática.
- Puede contratar servicios independientes para revisar regularmente el diseño de seguridad de la aplicación. Una evaluación realizada por terceros podría descubrir otros problemas que exijan mecanismos de seguridad adicionales.
- Contratar a una organización externa para atacar los sistemas de la organización y a la red a través de Internet (es decir, pruebas de penetración).
- En caso de contratar a una empresa externa para que se encargue de esta área. Organizar una reunión con todos los contratistas correspondientes, proveedores de servicios y terceros, para comunicar los requisitos, y comprobar que dichos requisitos se han cumplido.
- Proporcionar al personal involucrado en esta tarea capacitaciones relacionadas con Gestión de vulnerabilidades, y uso de herramientas de evaluación de vulnerabilidades.
- Implementar mecanismos formales para verificar que las actividades de mitigación para esta área se cumplen, y documentar todos los procesos de verificación.

Roles y Responsabilidades:

- Se recomienda que para no sobrecargar de trabajo a la Administradora de sistemas, se contrate nuevo personal en el área de Ti, o a una empresa externa especializada que se dedique exclusivamente a monitorear e informar de las vulnerabilidades detectadas en la red de datos de Manpower.
- La actividad de creación de las políticas y procedimientos para la Gestión de vulnerabilidades será responsabilidad de la Administradora de sistemas en colaboración con el gerente de operaciones y administración.

- Las actividades de capacitación al personal de la empresa deben ser gestionadas por el Gerente de Operaciones y Administración.
- Las actividades de verificación, deberán realizarse trimestralmente y el responsable de esta actividad es el Gerente de Operaciones y Administración, tanto si es personal interno o personal externo, el que se encarga de realizar estas tareas.

3.3.5 Área: Arquitectura y Diseño de la Seguridad

Actividades de mitigación:

- Documentar los diagramas que muestran la arquitectura de seguridad en toda la empresa y la topología 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.
- Los diagramas actuales y precisos de las relaciones físicas y lógicas de las redes internas y externas tendrán que estar disponibles en todo momento.
- Diseñar controles de seguridad en sistemas y redes, nuevos y revisados.
- 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.
- Crear una directiva para actualizar estos diagramas cuando el entorno se cambie.
- Actualizar el diseño de los sistemas utilizados, para incluir controles de seguridad apropiados.
- Investigar los incidentes periódicos en los sistemas utilizados y corregir los problemas de diseño que provocan estos incidentes.
- 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.
- Comprobar las actualizaciones y revisiones en un entorno de laboratorio antes de su instalación definitiva.

- Poner en práctica un proceso formal de gestión de configuraciones y de 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.
- Definir los roles y responsabilidades del personal involucrado en estas tareas.
- Se recomienda que los miembros de TI delegados en esta área asistan a cursos de entrenamiento en el diseño de sistemas y redes seguras.
- A continuación se entrega una lista de recomendaciones sobre las principales actividades que se deben realizar sobre la red de la empresa:
    - Implementar un firewall que soporte VPN para que los usuarios puedan realizar acceso remoto a través del internet
    - Instalar un servidor proxy para proteger las direcciones IP de la red de datos.
    - Implementar un sistema inspector de contenido web, para optimizar el uso del ancho de banda de internet
    - Implementar un sistema de detección de intrusos basado en Host, para detectar anomalías que indiquen un riesgo potencial, revisando las actividades en la máquina (host).
    - Implementar el servicio NAT, Network Address Translation o traducción de direcciones de red en el mismo firewall.

Roles y Responsabilidades:

- Se recomienda contratar una empresa externa especializada, que se encargue de estas tareas, caso contrario la gestión de estas actividades será responsabilidad de la Administradora de Sistemas.
- En el caso de que estas tareas las realice una empresa externa. Organizar una reunión con todos los contratistas correspondientes, proveedores de servicios y terceros, para comunicar los requisitos, para la incorporación de características de seguridad apropiadas en los sistemas y redes, y comprobar que dichos requisitos se han cumplido.

- Las actividades de supervisión están a cargo del Gerente de Operaciones y Administración. Todo cambio en la arquitectura debe ser aprobado por el comité técnico.
- Las actividades de capacitación, están a cargo del Gerente de Operaciones y Administración.

4. CAPÍTULO IV: CONCLUSIONES Y RECOMENDACIONES

En este capítulo presentamos las conclusiones y recomendaciones a las que llegamos una vez concluido el proceso de evaluación de riesgos y diseño del plan de seguridad.

4.1 CONCLUSIONES

a) Cumplimos con el principal objetivo del proyecto que era realizar un análisis de riesgos, y desarrollar un plan de seguridad para la información de la empresa Manpower.
b) Realizamos la evaluación utilizando las herramientas MSAT Y OCTAVE –S y a partir de los resultados obtenidos diseñamos el plan de seguridad para Manpower.
c) Confirmamos que los activos críticos más importantes para los procesos de negocio de la empresa son el sistema gestor y los servidores de base de datos y correo electrónico.
d) Determinamos que la información sensible que maneja la empresa, son los datos que se procesa en el sistema gestor, correos electrónicos y la información de clientes y proveedores.
e) Para utilizar 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. 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) Si el equipo conoce los procesos de la empresa, el tiempo que toma desarrollar la evaluación con MSAT es significativamente más corto respecto al tiempo que toma la evaluación con OCTAVE -S.
g) MSAT y OCTAVE -S utilizan estados de alerta para determinar el nivel de criticidad de un área en particular. Con OCTAVE -S analizamos 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. MSAT hace su valoración de riesgo basándose en las respuestas del cuestionario.

h) Durante la evaluación con MSAT detectamos riesgos en las áreas de infraestructura, aplicaciones, operaciones y personal. A partir de esta evaluación obtuvimos pautas para recomendar las actividades de mitigación y minimizar los riesgos encontrados en cada una de las áreas mencionadas.
i) Con OCTAVE –S obtuvimos un listado de los activos importantes de Manpower, 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.
j) Con OCTAVE -S, para determinar los activos críticos, es necesario tener en cuenta el nivel de importancia que estos tienen para los procesos de negocio de la institución.
k) 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.
l) OCTAVE -S se centra únicamente en las áreas que considera más críticas, de otro modo tomaría demasiado tiempo hacer un plan para todas las áreas de seguridad. Determinamos que las áreas más críticas, y que necesitan un plan de seguridad con más urgencia son las áreas de Gestión de la Seguridad, Monitoreo y Auditoría de Seguridad Física, Gestión de Vulnerabilidades, y Arquitectura y Diseño de la Seguridad.
m) OCTAVE -S no solo es reactivo, también es proactivo. 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.
n) Con OCTAVE –S, incluso realizando una evaluación parcial, obtendremos información útil para mejorar la postura de la seguridad de la empresa.

o) 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.
p) 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.

4.2 RECOMENDACIONES

a) Recomendamos implementar, controlar y monitorear las actividades sugeridas en el plan de seguridad propuesto en el presente proyecto, con el fin de eliminar vulnerabilidades encontradas y disminuir la probabilidad de ocurrencia de los riesgos a futuro.
b) Es necesario que Manpower 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) Recomendamos 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 amenazas y las tecnologías 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) Recomendamos realizar evaluaciones periódicas de seguridad, ya sea por personal interno o externo a la empresa. Estas evaluaciones ayudaran 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.

e) Recomendamos revisar periódicamente las políticas y procedimientos, ya que la tecnología tiene avances constantemente y por ende aparecen riesgos que deben ser mitigados para evitar problemas futuros.
f) Recomendamos 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.
g) Recomendamos 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.
h) Recomendamos 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.

5. GLOSARIO DE TÉRMINOS

El glosario presenta los términos y conceptos utilizados en el presente proyecto de titulación. Las definiciones propuestas son tomadas del documento completo que proporciona MSAT, así como también del libro OCTAVE®-S Implementation Guide, Version 1.0.

Activos: Se considera como activo a algo que representa un valor para la empresa. Los activos de tecnología de la información son la combinación de los activos físicos y lógicos, y se agrupan en las siguientes clases específicas: información, sistemas, servicios y aplicaciones y personas.

Categoría de los Activos

- Información: Datos documentados (impresos o electrónicos) u otra propiedad intelectual utilizada para cumplir con la misión de la empresa
- Sistemas: Representa la combinación de información, software, y activos de hardware que procesan y almacenan información. Cualquier host, cliente o servidor puede ser considerado como un sistema.
- Servicios y aplicaciones: Son las aplicaciones de software y servicios (sistemas operativos, aplicaciones de bases de datos, software de red, aplicaciones de oficina, aplicaciones personalizadas, etc) que procesan, almacenan o transmiten la información.
- Personas: Las personas de una empresa que poseen habilidades únicas, conocimientos y experiencias, son difíciles de reemplazar.

Amenaza: Representa un indicador de un potencial evento no deseable. Una amenaza hace referencia a una situación en la que una persona podría hacer algo indeseable (iniciar un ataque de denegación de servicio contra el servidor de correo de la empresa), o un fenómeno natural que podría causar un resultado no deseado (un incendio dañaría el hardware de tecnología de la información de la empresa).

Aplicaciones: Software informático que proporciona funcionalidad al usuario final. Requiere la existencia de un sistema operativo en el que pueda ejecutarse.

Áreas de Práctica de Seguridad: Grupos de prácticas que son estratégicas u operacionales. Las Áreas de Prácticas de Seguridad Estratégicas son típicamente amplias y tienden a afectar a todos los riesgos de todos los activos críticos por igual (por ejemplo, documentando un conjunto de políticas de seguridad para la empresa). Las Áreas de Prácticas de Seguridad Operacionales se enfocan en las áreas del día a día y pueden ser dirigidos hacia la mitigación de riesgos específicos de activos específicos (por ejemplo, control de un sistema específico para las cuentas por defecto).

Características: Una cualidad o atributo de una área de práctica de seguridad. Cada área de práctica de seguridad incluye múltiples características.

Catalogó de prácticas: Es una colección estratégica y operativa de buenas prácticas de seguridad que una empresa puede utilizar para administrar su seguridad.

Clase de componentes clave: Son las categorías de dispositivos y redes usadas, que acceden a un sistema de interés. Estos dispositivos y redes son parte de o están relacionados al sistema de interés. Cuando los usuarios acceden legítimamente al activo crítico, ellos acceden a componentes de esta clase. Actores amenaza también acceden a componentes de esa clase cuando los actores deliberadamente victimizan a un activo crítico.

Criterio de evaluación de Impacto: Es un conjunto de medidas cualitativas frente a los cuales se evalúa el efecto de cada riesgo en la misión y los objetivos de negocio de la empresa. Los criterios de evaluación de impacto definen los rangos de los impactos (alto, medio y bajo) para la empresa.

Enfoque: La forma en que una empresa aborda una característica de una área de práctica de seguridad.

Estado de semáforo: El estado de semáforo se basa en el rendimiento de la empresa con las áreas de práctica de seguridad. Los siguientes colores son asignados a un área basada en el rendimiento percibido en esa área:

- Verde: La empresa está llevando a cabo las prácticas de seguridad en el área de una manera correcta, no hay necesidad real de mejora.

- Amarillo: La empresa está llevando a cabo las prácticas de seguridad solo hasta cierto punto, hay espacio para la mejora.
- Rojo: La empresa no está llevando a cabo las prácticas de seguridad en el área, existe un amplio margen de mejora.

Estrategias de Protección: Define la estrategia general empleada por una empresa para iniciar, implementar y mantener su seguridad interna. Está estructurada de acuerdo a las áreas de prácticas de seguridad. Una estrategia de protección define como una empresa tiene la intención de aumentar o mantener el nivel de seguridad existente. Su objetivo es proporcionar una dirección a los futuros esfuerzos de la seguridad de la información en lugar de encontrar una solución inmediata a todas las preocupaciones y vulnerabilidades de seguridad.

Impacto: Es el efecto de una amenaza sobre la misión y los objetivos de negocio de una empresa.

Índice de defensa en profundidad (DiDI): Medida de las defensas de seguridad utilizadas en el personal, los procesos y la tecnología para contribuir a reducir los riesgos identificados en una empresa.

Infraestructura: Funcionalidad de red, así como su administración y mantenimiento para ofrecer compatibilidad con la defensa de red, respuesta frente a incidentes, disponibilidad de red y análisis de errores. Incluye compatibilidad con los procesos empresariales internos y externos, y acerca de cómo se crean e implementan los hosts.

Lugares de almacenamiento de datos: Tipos adicionales de componentes utilizados para almacenar información crítica o proporcionar servicios de soporte de datos relacionados al sistema de interés (por ejemplo, dispositivos de almacenamiento utilizados para respaldar información almacenada en un sistema de interés).

Operaciones: Las políticas, procesos, procedimientos y prácticas relacionadas con la protección.

Plan de Mitigación de Riesgos: Un plan que tiene como objetivo reducir los riesgos a un activo crítico. Los planes de mitigación de riesgos tienden a

incorporar actividades o medidas destinadas a contrarrestar las amenazas a los activos.

Los planes de mitigación de riesgos comprenden los siguientes elementos:

- *Actividades de mitigación:* Definen las actividades que el equipo de análisis recomienda implementar en un área de práctica de seguridad.
- *Justificación:* Documenta las razones para la selección de cada actividad de mitigación. La razón se debe documentar si la actividad está destinada a reconocer la amenaza, resistirla, o recuperarse de ellas.
- *Responsabilidad de mitigación:* Identifica quién debe participar en la implementación de cada actividad.
- *Soporte/apoyo adicional:* Documentar cualquier apoyo adicional que se necesite en la aplicación de cada actividad (por ejm, financiación, compromiso del personal).

Prácticas de seguridad: Son acciones que ayudan a iniciar, implementar y mantener la seguridad dentro de una empresa.

Prácticas estratégicas: Son las prácticas de seguridad que se centran en cuestiones de organización a nivel de políticas. Se incluyen temas relacionados con la empresa, así como cuestiones que requieren de la planificación y participación de toda la organización.

Prácticas operacionales: Son las prácticas de seguridad que se centran en cuestiones relacionadas con la tecnología. Se incluyen temas relacionados con la manera en que las personas utilizan, interactúan, y protegen la tecnología en el día a día.

Perfil de Amenaza: Presenta de manera estructurada una serie de amenazas a un activo crítico. El perfil de amenaza genérico es un punto de partida para crear un único perfil de amenaza para cada activo crítico.

Las amenazas son representadas usando las siguientes propiedades:

- Activo: Alguna cosa de valor para la empresa.
- Acceso: Cómo el activo es accesado por un actor (acceso a la red, acceso físico). El acceso se aplica solo a actores humanos.

- Actor: Quién o qué puede violar los requerimientos de seguridad (confidencialidad, integridad, disponibilidad) de un activo.
- Motivo: La intención de un actor (por ejemplo, deliberada o accidental). El motivo se aplica solo a actores humanos.
- Resultado: El resultado inmediato (divulgación, modificación, destrucción, pérdida, interrupción) de violar los requerimientos de seguridad de un activo.

En OCTAVE-S, las amenazas se representan visualmente en una estructura de árbol, a menudo referido como un árbol de amenaza. Hay un árbol de amenaza para cada una de las siguientes categorías de amenaza:

Categoría	**Definición**
Actores humanos con acceso a la red	Las amenazas en esta categoría son amenazas basadas en la red. Requiere la acción directa de una persona y puede ser deliberada o accidental.
Actores humanos con acceso físico	Las amenazas en esta categoría son amenazas físicas a los activos críticos de la empresa. Requiere la acción directa de una persona y puede ser deliberada o accidental.
Problemas del sistema	Las amenazas de esta categoría son problemas con los sistemas de tecnología de la información de la empresa. Algunos ejemplos son: los defectos de software, código malicioso (por ejemplo, virus, malware), y otros problemas relacionados con el sistema.
Otros problemas	Las amenazas en esta categoría son problemas o situaciones que están fuera de control de una empresa. Esta categoría de amenazas incluye desastres naturales (por ejemplo, inundaciones, terremotos) y los riesgos de interdependencia. Los riesgos de interdependencia incluyen la falta de infraestructuras críticas (por ejemplo, fuentes de energía).

Perfil de riesgos para la empresa (BRP): Medida del riesgo al que está expuesto una empresa, según el entorno empresarial y el sector en que compite.

Personal: Miembros de una empresa, así como las directivas, procesos, procedimientos y prácticas que se relacionan con su protección y la de la empresa.

Puntos de accesos: Interfaces que directa o indirectamente permiten el acceso al sistema de interés. Estas interfaces se agrupan de acuerdo a las siguientes categorías:

- Componentes del sistema de interés.
- Sistema de acceso de personas.
- Puntos de acceso intermedios.
- Interfaces y datos de almacenamiento de otros lugares.
- Otros sistemas.

Puntos intermedios de acceso: Redes utilizadas para transmitir la información y aplicaciones del sistema de interés para las personas.

Requerimientos de Seguridad: Son declaraciones que describen las cualidades de los activos de información y que son importantes para la empresa. Los requerimientos de seguridad más comunes son: la confidencialidad, integridad y disponibilidad.

- **Confidencialidad:** Es la necesidad para mantener información confidencial, sensible o personal, inaccessible o privada para cualquier persona que no esté autorizada para verla.
- **Integridad:** Es la autenticidad y completitud de una activo.
- **Disponibilidad:** Cuándo o con qué frecuencia un activo debe estar listo para su utilización.

Riesgo: La posibilidad de sufrir daños o pérdidas. El riesgo se refiere a una situación en la que una persona puede hacer algo indeseable o un fenómeno natural puede causar un resultado no deseado, lo que resulta en un impacto negativo o consecuencia.

Un riesgo se compone de:

- Un evento
- Incertidumbre
- Una consecuencia

En la seguridad de la Información, un evento básico es una amenaza.

Hay incertidumbre en torno a si una amenaza se produce y si la empresa está lo suficientemente protegida contra el actor amenaza. La incertidumbre es a menudo representada usando la probabilidad de ocurrencia o probabilidad.

La consecuencia que en definitiva importa en el riesgo de la seguridad de la información es el impacto resultante en la empresa debido a una amenaza. El impacto describe cómo una empresa puede verse afectada basado en los siguientes resultados de amenazas:

- Divulgación.
- Modificación.
- Perdida/Destrucción.
- Interrupción.

Rutas de acceso a la red: Son las formas en que los sistemas, dispositivos, información o servicios pueden ser accedidos a través de la red de la empresa.

Sistemas de acceso de personas: Tipos de componentes que las personas (por ejemplo, usuarios, atacantes) utilizan para acceder a un sistema de interés. Estos componentes constituyen los puntos de acceso que se originan interna o externamente a los sistemas y redes de una empresa.

Sistemas de interés: Son el o los sistemas que están más estrechamente ligados a un activo crítico, por ejemplo:

- El sistema en donde “vive” el activo.
- El sistema que ofrece a los usuarios acceso legitimo a un activo crítico.
- El sistema que permite acceso a un actor amenaza al activo crítico.

Tareas: Una actividad que debe ser completada como parte de una área de práctica de seguridad operacional.

Valor de Impacto: Una medida cualitativa del impacto de un riesgo específico para la empresa, esta medida puede ser cualquiera de los siguientes rangos: alto, medio o bajo.

Valor de Probabilidad: Una medida cualitativa de la probabilidad de una amenaza (alta, media, baja).

Vulnerabilidades Organizacionales: Representan debilidades en las políticas de la organización y/o en las prácticas que pueden resultar en acciones no autorizadas.

Zona desmilitarizada (DMZ): Parte de la red separada de la red interna mediante un cortafuegos y conectada a Internet a través de otro cortafuegos.

6. ANEXOS

Anexo A: Se encuentra en formato digital en el cd en la siguiente ruta: */ANEXOS/Anexo A/Informe resumido MSAT.*

Anexo B: Se encuentra en formato digital en el cd en la siguiente ruta: */ANEXOS/Anexo B/Informe completo MSAT.*

Anexo C: Se encuentra en formato digital en el cd en la siguiente ruta: */ANEXOS/Anexo C/Hojas de trabajo OCTAVE –S.*

7. BIBLIOGRAFIA

LIBROS:

- ALBERTS, Christopher, DOROFEE, Audrey, STEVENS, James, WOODY, Carol, “Lista de documentos guía del método OCTAVE-S”, Carnegie MellonUniversity, Software EngineeringInstitute, Pittsburgh, PA, Enero 2005.

- INTRODUCCION A OCTAVE

  ALBERTS, Christopher, DOROFEE, Audrey, STEVENS, James, WOODY, Carol, “introducción al enfoque OCTAVE-S”, Programa de supervivencia de sistemas en red, Carnegie MellonUniversity, Software EngineeringInstitute, Pittsburgh, PA, Agosto 2003.

- ALBERTS, Christopher, DOROFEE, Audrey, STEVENS, James, WOODY, Carol, “Vision General de OCTAVE”, Carnegie Mellon University, Software Engineering Institute, Pittsburgh, PA, 2003.

- ALBERTS, Christopher, DOROFEE, Audrey, “Criterios de OCTAVE”, Carnegie Mellon University, Software Engineering Institute, Pittsburgh, PA, Diciembre 2001.

- ALBERTS, Christopher, DOROFEE, Audrey, ALLEN, Julia H.,“Catálogo de Prácticas OCTAVE”, Versión 2, Carnegie Mellon University, Software Engineering Institute, Pittsburgh, PA, Octubre 2001.

- ALBERTS, Christopher, DOROFEE, Audrey, WOODY, Carol, “Seguridad de la información en pequeñas organizaciones”, Carnegie MellonUniversity, Software EngineeringInstitute, Pittsburgh, PA, Enero 2005.

LISTA DE DOCUMENTOS GUIA DEL METODO OCTAVE-S

V01_octave_s_intro v1.doc, introducción al método;
v02_preparation v1.doc, preparación antes de la evaluación;
v03_guidelines v1.doc, normas de aplicación de la evaluación;
v04_org_ws v1.doc, hojas de trabajo organizacionales;
v05_info_asset_ws v1.doc, hojas de trabajo de información de activos críticos;
v06_sys_asset_ws v1.doc, hojas de trabajos de activos críticos de sistemas;
v07_app_asset_ws v1.doc, hojas de trabajo de activos críticos de aplicaciones;
v08_ppl_asset_ws v1.doc, hojas de trabajo de activos críticos de personas;
v09_P1_strat_ws v1.doc, hojas de trabajo de planes y estrategias;
v10_example v1.doc, escenario completo de ejemplo.

PÁGINAS WEB:

- OCTAVE.
  http://www.cert.org/octave/
  Septiembre 2008
- OCTAVE-S
  http://www.cert.org/octave/octaves.html
  Septiembre 2008
- GUIA DE IMPLEMENTACION OCTAVE-S
  http://www.sei.cmu.edu/library/abstracts/reports/04hb003.cfm
  Noviembre 2011
- HERRAMIENTA DE EVALUACION MSAT
  http://technet.microsoft.com/es-es/security/cc185712
  Noviembre 2011
- Herramienta de Evaluación de Seguridad de Microsoft (MSAT)
  http://technet.microsoft.com/es-es/library/cc185712.aspx
  Enero 2013

TEMAS DE TESIS:

- ANDRADE RAMOS, Manuel Raúl. Análisis de Riesgos y Diseño de un plan de seguridad de información para el instituto geofísico de la Escuela Politécnica Nacional. Proyecto de titulación. EPN. 2006.

- PARREÑO PONTÓN, Sandra Tamara, SUNTAXI OÑA, Gabriela Lorena. Auditoría de la seguridad de la información de la Empresa Transportes Noroccidental. Proyecto de titulación. EPN. 2010.

- PAZMIÑO NARANJO, Pablo Daniel. Análisis de los riesgos y vulnerabilidades de la red de datos de Escuela Politécnica Nacional. Proyecto de titulación. EPN. 2007.

- GALLARDO PIEDRA, María Cristina, JACOME CORDONES, Paul Orlando, Análisis de riesgos informáticos y elaboración de un plan de contingencia TI para la empresa eléctrica Quito S:A:, Proyecto de titulación. EPN. 2011.

- CUASCOTA PAZMIÑO, José Luis, SIMBA SANCHEZ, German Roberto, Análisis, diseño y prototipo de una red VoIP empresarial, Proyecto de titulación. EPN. 2011.

- LOPEZ Aida, BENITEZ Cesar, GUTIERREZ Raúl, ZAVALA José, Proyecto de seguridad en sites del servicio de administración y enajenación de bienes (SAE), Maestría en gestión de tecnologías de información, SAE, DICIEMBRE 2009.