INFORME PRACTICAS PROFESIONALES

Gustavo Arévalo Arenas

Cartagena 15 de Junio de 2012

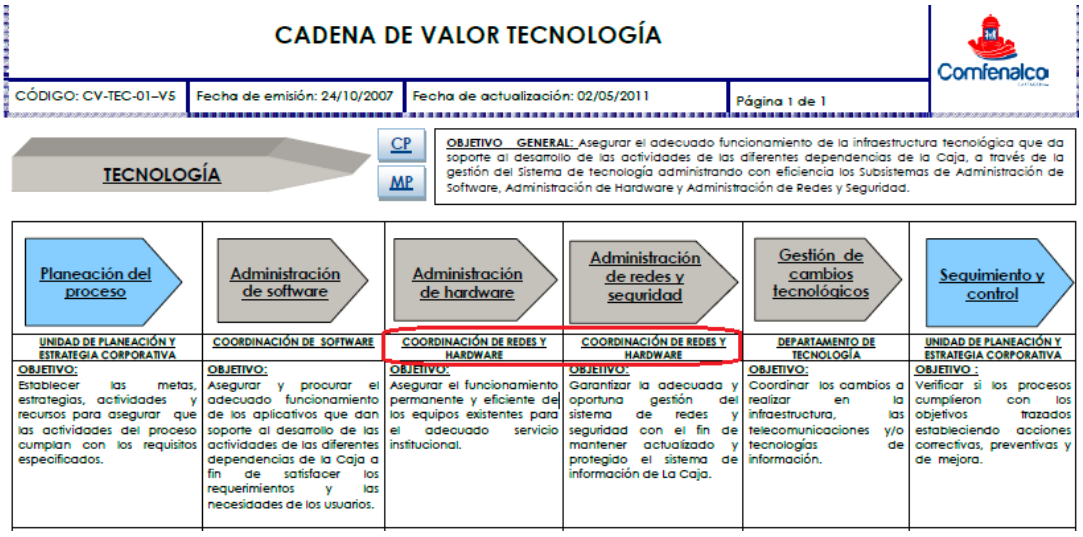
1. Información de La Empresa

El nombre completo de la organización es Caja de Compensación Familiar de Fenalco – Andi COMFENALCO CARTAGENA. El cual es una corporación civil de carácter privado, sin ánimo de lucro, de duración indefinida que cumple funciones de Seguridad Social.
Pertenece al Sistema de Subsidio Familiar, que hace parte del Sistema de Seguridad Social de Colombia y es concebido por el Estado como mecanismo de redistribución de los ingresos en un país que exhibe grandes desigualdades desde el punto de vista socioeconómico.
Su misión esta enfocada a mejorar la calidad de vida de sus afiliados y de la población vulnerable mediante la prestación de servicios sociales que contribuyan al desarrollo de la región en el marco del sistema de compensación familiar.

La Caja de Compensación Comfenalco se proyecta al 2015 a ser la Caja de Compensación Familiar preferida por las empresas y trabajadores de su ámbito territorial, consolidando su proyección nacional a través de alianzas estratégicas y un portafolio de servicios innovador, generando nuevos recursos para ser reinvertidos dentro de un marco de responsabilidad social empresarial.
La página para visita es. http://www.comfenalco.com

2. Descripción del Cargo.

Actualmente, desempeño el rol de Coordinador de Redes y Hardware, cuyo propósito general es la de garantizar, la prestación de los servicios tecnológico, bajo un entorno seguro, gestionado por nuestro Sistema de Gestión de Seguridad de la Información.
La gran parte de las funciones ejercidas se muestran a través del siguiente alcance grafico.



3. Proyectos Desarrollados En la Caja de Compensación Familiar Comfenalco Cartagena.

En el año 2008, a través de nuestro ente regulador en Colombia el cual es la Súper Intendencia del Subsidio Familiar en Colombia, recibimos una recomendación donde al año 2009, se debía presentar un informe, sobre el estado de la empresa, a través de un análisis de seguridad de la información a la compañía.

Para esta tarea, y teniendo en cuenta que este análisis debía realizarlo un ente externo, realice unos términos de referencia, donde se invitaron empresas consultoras reconocidas como los son, PRICE, KPMG, DELOITTE, ETEK, Ernest & Young. En la cual se solicito un GAP ANALYSIS, y la realización de ethical hacking interno y Externo, de los activos de la información de la compañía.

El proyecto se le adjudico a PWC, y el rol desempeñado fue el de Gerente de Proyecto.

Este proyecto, arrojo unos resultados, para lo cual se realizo un plan de mitigación inicial a las vulnerabilidades encontradas.
En esta fase posterior al análisis, al ser una tarea, que esta bajo mi responsabilidad en la Cadena de Valor de Tecnología, fue necesario de mi parte analizar, los hallazgos encontrados, y generar un plan de acción para su mitigación.

Con referencia a los hallazgos del GAP, tecnología sugiere a la organización, la implantación de un sistema de gestión de Seguridad de la información, el cual es acogido positivamente.

3.1 Implantación del Sistema de Gestión de Seguridad de la Información, basado en la norma ISO 27001.

Se realizo el proceso de implantación del Sistema de Gestión de Seguridad de Información de la Compañía, dentro de los roles desempeñados se encuentra lo siguiente.

Elaboración de Políticas de Seguridad:

- Políticas de Control de Acceso.
- Políticas de Adquisición, Mantenimiento y Desarrollo de Sistemas de Información.
- Políticas Relacionadas con la Gestión de Continuidad de Negocio.
- Políticas Gestión de Activos.

Elaboración de los Estándares de seguridad:

- Estándar de Acceso Remoto.
- Estándar de Centro de Computo.
- Estándar Firewall.
- Estándar r de Servidores Linux.
- Estándar de Servidores Windows 2003 y 2008 SERVER.
- Estándar de Switch.
- Estándar de Wireless.

En esta fase después del análisis y realizar la documentación, se empezó a generar un plan para la aplicación de los estándares y políticas, dentro del enfoque tecnológico.

Seguido a esto se genera un Comité de Seguridad de la Información, y se crea el rol dentro de la compañía de Oficial de Seguridad de la información, y se empieza con su expansión a todos los procesos de la organización, especialmente fortaleciendo los conocimientos en seguridad de la información, con campañas de sensibilización y conocimiento del sistema de Gestión.

Finalizada esta fase, se realizan procesos de monitoreo y escaneo de vulnerabilidades dentro de la compañía a través de un SOC, contratado con la compañía PWC, se implemento una herramienta llamada OSSIM, y mensualmente nos entregan un informa, sobre las vulnerabilidades, los incidentes, y la gestión de seguridad de manera genera.

Dentro de mis funciones esta el analizar estos informe y generar planes de acción para que estos hallazgos, sean documentados y aplicados un plan de mitigación a la vulnerabilidad.
Dentro de este proceso, también se genero análisis de riesgos y de impacto a través de un BIA, con la cual se identifico, los activos críticos para los cuales era necesario generar un proceso de respaldo y contingencia.

Dentro de este proceso, las áreas ayudaron a la definición de los RTO y RPO, donde se identifico los procesos con su nivel de criticidad, esto dio como resultado, la implantación de un plan de continuidad de negocio, y dentro de este proyecto fui el encargado de analizar los tiempos esperados por la organización versus, nuestra situación actual tecnológica.

Teniendo en cuenta estos resultados, realice el Diseño de la Solución Tecnológica del Plan de Continuidad de Negocio de la Caja de Compensación Comfenalco, el cual fue aprobado por la dirección, y se convirtió en uno de los grandes pilares del Plan.

La solución consiste, en la implementación de un Centro de Computo Alterno, aprovechando que nuestra infraestructura se encuentra basada en Tecnología

VMWARE. Dimensione servidores que se usuaria como servidores de respaldo, se diseño la automatización del proceso de Replicación de Maquinas Virtuales de manera completa, con una periocidad de tiempo que supla las necesidades de los RTO y RPO, se realizo ajustes de Networking, donde se extendió las VLAN, a lo largo de las sedes y el Centro Alterno, con el objetivo, que al existir una Contingencia, se enciendan los servidores de contingencia, sin realizar cambios en el direccionamiento y el nombre, dejando que este proceso sea prácticamente transparente.

A la fecha se han realizado tres pruebas, de continuidad, parciales y completa, entregando resultados totalmente positivos.