

**ADMINISTRACIÓN LÓGICA DE LA RED PROPONIENDO MEJORAS
TÉCNICAS E IMPLEMENTANDO POLÍTICAS DE SEGURIDAD Y PLANES DE
CONTINGENCIA.**

HERNÁN MAURICIO ATUESTA BERRIO

**UNIVERSIDAD CATÓLICA POPULAR DEL RISARALDA
PROGRAMA DE INGENIERÍA DE SISTEMAS Y TELECOMUNICACIONES
PRACTICAS PROFESIONALES
PEREIRA
2009**

**ADMINISTRACIÓN LÓGICA DE LA RED PROPONIENDO MEJORAS
TÉCNICAS E IMPLEMENTANDO POLÍTICAS DE SEGURIDAD Y PLANES DE
CONTINGENCIA.**

HERNÁN MAURICIO ATUESTA BERRIO

INFORME DE PRÁCTICA PROFESIONAL

**Tutor
CÉSAR AUGUSTO TABARES ISAZA**

**UNIVERSIDAD CATÓLICA POPULAR DEL RISARALDA
PROGRAMA DE INGENIERÍA DE SISTEMAS Y TELECOMUNICACIONES
PRACTICAS PROFESIONALES
PEREIRA
2009**

CONTENIDO

| | |
|---|----|
| INTRODUCCIÓN | 9 |
| 1.PRESENTACIÓN GENERAL DE LA EMPRESA..... | 10 |
| 1.1 RESEÑA HISTÓRICA | 10 |
| 1.2 MISIÓN..... | 13 |
| 1.3 VISIÓN | 14 |
| 1.4 VALORES CORPORATIVOS..... | 14 |
| 1.5 POLÍTICAS CORPORATIVAS | 14 |
| 1.6 POLÍTICAS DE CALIDAD | 14 |
| 1.7 ORGANIGRAMA | 15 |
| 2. DIAGNÓSTICO..... | 16 |
| 2.1 SERVIDOR DE COODESURIS..... | 16 |
| 2.1.1 Estado Directorio Activo | 16 |
| 2.1.2 Estado Archivos Compartidos | 16 |
| 2.1.3 Estado de las Funciones de Mantenimiento al Servidor..... | 17 |
| 2.1.4 Estado de las Copias de Seguridad | 18 |
| 2.2 RED DE COODESURIS | 19 |
| 2.2.1 Estado de las Estaciones de Trabajo | 19 |
| 2.2.2 Estado del Antivirus Kaspersky | 20 |
| 2.2.3 Estado de las Políticas de seguridad informática | 20 |
| 2.2.4 Estado del Firewall | 21 |
| 2.3 MEJORAS TÉCNICAS Y TECNOLÓGICAS EN LA OPERACIÓN..... | 21 |
| 2.3.1 Estado Técnico del servidor | 21 |
| 2.3.2 Estado de la Conexión a las farmacias | 23 |
| 2.3.3 Estado de la Página Web | 23 |
| 3. EJES DE INTERVENCIÓN..... | 24 |
| 4. JUSTIFICACIÓN DE LOS EJES..... | 25 |

| | |
|---|----|
| 4.1 ADMINISTRACIÓN DEL SERVIDOR DE COODESURIS | 25 |
| 4.1.1 Directorio Activo de Windows 2003 Server | 25 |
| 4.1.2 Compartir archivos en la Red de Coodesuris | 26 |
| 4.1.3 Funciones de Mantenimiento al servidor | 27 |
| 4.1.4 Plan de Copia de seguridad | 27 |
| 4.2 ADMINISTRACIÓN DE LA RED..... | 29 |
| 4.2.1 Estaciones de trabajo y sus recursos | 29 |
| 4.2.2 Antivirus Kaspersky | 31 |
| 4.2.3 Herramienta Wireshark..... | 32 |
| 4.2.4 Firewall | 33 |
| 4.2.5 Políticas de seguridad en Coodesuris | 33 |
| 4.3 MEJORAS TÉCNICAS Y TECNOLÓGICAS EN LA OPERACIÓN..... | 34 |
| 4.3.1 Servidor | 34 |
| 4.3.2 Conexión de Acceso remoto | 34 |
| 4.3.3 Página web..... | 35 |
| 5. OBJETIVOS..... | 36 |
| 5.1 OBJETIVO GENERAL..... | 36 |
| 5.2 OBJETIVOS ESPECÍFICOS | 36 |
| 6. PRESENTACIÓN Y ANÁLISIS DE LOS RESULTADOS..... | 37 |
| 6.1 SERVIDOR DE COODESURIS..... | 37 |
| 6.1.1 Acciones Tomadas en el Directorio Activo | 37 |
| 6.1.2 Acciones Tomadas en la administración de archivos compartidos | 43 |
| 6.1.3 Acciones Tomadas en cuanto al mantenimiento del servidor..... | 44 |
| 6.1.4 Acciones tomadas en el plan de copia de seguridad | 46 |
| 6.2 RED DE COODESURIS | 49 |
| 6.2.1 Acciones Tomadas en las estaciones de trabajo | 49 |
| 6.2.2 Acciones Tomadas kaspersky | 51 |
| 6.2.3 Acciones Tomadas Wireshark..... | 52 |

| | |
|--|----|
| 6.2.4 Acciones Tomadas en las Políticas de Seguridad..... | 53 |
| 6.2.5 Acciones Tomadas en el Firewall | 54 |
| 6.3 MEJORAS TÉCNICAS Y TECNOLÓGICAS EN LA OPERACIÓN | 55 |
| 6.3.1 Acciones Tomadas en la Mejora técnica servidor | 55 |
| 6.3.2 Acciones Tomadas en la conexión remota..... | 55 |
| 6.3.3 Acciones Tomadas en la actualización de la página web..... | 56 |
| CONCLUSIONES | 57 |
| RECOMENDACIONES..... | 58 |
| COMPLEMENTARIOS | 65 |
| REFERENCIAS | 72 |

LISTA DE FIGURAS

| | |
|---|----|
| Figura 1 Primer Listado de Usuarios Directorio Activo..... | 37 |
| Figura 2. Segundo Listado de Usuarios Directorio Activo | 38 |
| Figura 3 Cambio Nombres de Usuarios del Directorio Activo | 39 |
| Figura 4. Primer Listado de Equipos del Directorio Activo | 40 |
| Figura 5 Listado Final de Equipos del Directorio Activo | 40 |
| Figura 6 Asignación de Grupos del Directorio Activo | 41 |
| Figura 7 Asignación de Grupos del Directorio Activo | 42 |
| Figura 8 Estado Anterior de la Unidad de Red Z | 43 |
| Figura 9 Estado Actual de la Unidad de Red Z | 44 |
| Figura 10 Relación de Visitas para Actualizar Office 2007 | 50 |
| Figura 11 Relación de Visitas Actualización Service Pack | 51 |
| Figura 12 Formato Ingreso Funcionarios | 53 |
| Figura 13 Formato Salida Usuarios | 54 |

LISTA DE TABLAS

| | |
|--|----|
| Tabla 1 Descripción ejes de intervención | 24 |
| Tabla 2 Resumen Proceso de desfragmentación | 46 |
| Tabla 3 Primer Listado Copia de Seguridad Usuarios | 47 |
| Tabla 4 Segundo listado Copia de Seguridad Usuarios..... | 48 |
| Tabla 5 Estado Actual Copias de Seguridad Usuarios | 49 |

RESUMEN

Resumen

Para la Cooperativa de Entidades de Salud del Risaralda (COODESURIS) es fundamental que sus procesos no se detengan por el motivo que sea se debe seguir operando o bien tener planes de contingencia donde suplan los fallos operativos y no se reflejen los inconvenientes presentados. Ya que la administración de servicios que realiza la cooperativa a sus entidades asociadas se vería afectada de manera directa si la sede principal detiene sus actividades.

El presente informe de práctica considera la gran mayoría de puntos débiles que posee Coodesuris e interviene con implementaciones que mejoran la administración de los recursos informáticos y propone métodos para mantener el control de sus operaciones de una forma eficiente y segura.

Descriptores: Administración de Red, Seguridad, Servidor, Directorio Activo, Firewall, Políticas de Seguridad, Actualización.

Abstract

Cooperative Agencies for Health Risaralda (COODESURIS) is that its processes do not stop for whatever reason should continue to operate or have contingency plans which suit the operational failures and does not reflect the difficulties presented because management services performed by the cooperative to its partners would be directly affected if the main stops its activities.

This report considers the practice of most weaknesses Coodesuris owns and is involved with implementations that improve the management of resources and suggests ways to maintain control of its operations in an efficient and safe

Keywords: Network Administration, Security, Server, Active Directory, Firewall, Security Policy, Update.

INTRODUCCIÓN

El siguiente documento presentado como plan de práctica en la Cooperativa de Entidades de Salud de Risaralda (COODESURIS), contiene métodos, procesos, elementos teóricos y prácticos que se pueden aplicar a cualquier empresa en el área de Sistemas.

Realizar un diagnóstico acerca del estado en que se encuentran estructurados los sistemas y las telecomunicaciones en una empresa, es un trabajo que lleva bastante tiempo y se debe hacer cuidadosamente, tanto en la parte de planeación y documentación, como en la parte de ejecución, ya que cualquier decisión tomada incorrectamente puede comprometer la seguridad de la empresa en general, por tal razón es importante advertir que la seguridad en el desarrollo de un proyecto de innovación tecnológica no se puede dejar de lado, siempre se debe enmarcar como prioridad en el momento de reestructurar el método de operación de una empresa.

Son cantidad de aspectos que no se pueden omitir en el momento de planear una mejora o cambio total a un sistema empresarial, la seguridad, los planes de contingencia, la tecnología en equipos y el funcionamiento de las redes en general, forman un engranaje que crea una dependencia significativa entre un elemento y otro, pero con la gran ventaja que si todos se encuentran en un buen nivel, se obtendrán grandes beneficios del sistema implementado.

Podemos afirmar que en este presente las empresas están bastante interesadas en apuntarle a la tecnología, a la innovación, sistematizar procesos que agilicen tareas y reduzcan de manera significativa los costos. Y es en este momento donde la formación del ingeniero entra en juego y pone sus fichas proponiendo ideas, mejoras que apunten hacia la creación tecnológica, sustentada en la observación y en los criterios de necesidad de la empresa.

1. PRESENTACIÓN GENERAL DE LA EMPRESA

1.1 RESEÑA HISTÓRICA

En el año 1992 mediante un proceso de motivación y sensibilización, el doctor Javier de Jesús Taborda Quintero, Jefe de la División Financiera del entonces Servicio Seccional de Salud y el doctor Luís Emilio Zuluaga Trujillo, funcionario de la Superintendencia Nacional de Salud con sede en Pereira, logran encaminar acciones por parte de los gerentes de los hospitales, para crear un ente que asumiera parte de las funciones que el Servicio Seccional de Salud no seguiría desarrollando, tales como las adquisiciones de los insumos hospitalarios.

Fue así como mediante ordenanza No. 021 del 22 de Diciembre de 1992 y sancionada por el entonces Gobernador doctor Roberto Gálvez Montealegre, el 12 de enero de 1993 se faculta la creación de la Cooperativa de Entidades de Salud de Risaralda identificada con la sigla "Coodesuris", la cual con base en la solidaridad y ayuda mutua, desarrollaría programas de adquisición de insumos bajo economías de escala, consecuencial con la emisión de la Ley 100 de 1990 que modificó el Sistema Nacional de Salud.

El día 26 de marzo de 1993, se realiza la Asamblea de fundación con los 13 hospitales de los municipios del departamento, el hospital Mental y el servicio Seccional de Salud del Risaralda, suscribieron un capital de \$49'200.000 y nombraron como Gerente al doctor Luís Emilio Zuluaga Trujillo.

Mediante la resolución No. 1284 del 21 de mayo de 1993, tras asamblea de fundadores constituida por representantes legales de las Entidades Asociadas, se autoriza la conformación de la estructura directiva la Asamblea General como órgano máximo de Administración, el Consejo de Administración integrado por cuatro Asociados y tres suplentes como el órgano permanente de Administración subordinado a las directrices y políticas de la Asamblea General, y por último el Gerente como representante legal de la Cooperativa, ejecutor de las decisiones de

la Asamblea General y el Consejo de Administración y como canal de comunicación de ésta con los asociados y con terceros.

A partir del 18 de Junio de 1993, se inician las actividades comerciales en una improvisada oficina en el Servicio Seccional de Salud; bajo el proceso de compra conocido como “Justo a Tiempo”, en donde sólo cuando la Entidad Asociada requería algún insumo se realizaba la compra ante el laboratorio o el proveedor en la cantidad requerida.

En los años siguientes Coodesuris acompañó a los hospitales en los difíciles años de crisis que golpearon al sector salud, apalancando la adquisición de insumos con importantes plazos de pago mientras lograban un mayor fortalecimiento económico.

Sin embargo, los cambios importantes de la cooperativa fueron paulatinos al desarrollo de sus asociados, por ello a medida que se generaron requerimientos por parte de ellos, fue necesaria la incorporación de un mayor número de funcionarios y la implementación de nuevas estrategias para la cooperativa que permitieran prestar un mejor servicio a sus Entidades Asociadas.

Coodesuris continuó con su avance, implementando procesos a la vanguardia de la gestión administrativa de grandes empresas y de este proceso nació la idea de implementar el sistema Outsourcing, enfocado a la administración de ciertas tareas que no son propiamente la razón de ser de los hospitales, inicialmente con el suministro de medicamentos y posteriormente a los demás grupos de inventario (dispositivos médicos, imagenología, papelería, impresión y duplicación, aseo, uso doméstico y odontología) dando lugar a la eliminación del “Justo a Tiempo”, haciéndose necesario el mantener un stock de inventario disponible.

Tal idea fue pionera en su campo y fue así como el entonces Ministerio de Salud decidió apoyar financieramente a los hospitales asociados para facilitar su ingreso al modelo, lo que permitió que Coodesuris aumentara sus recursos y tuviera la

oportunidad de ofrecer mayores beneficios económicos para las Entidades Asociadas a través de sus excedentes.

Cabe anotar que el proceso de compra de insumos se estipuló mediante el acompañamiento de los funcionarios de los hospitales, los cuales seleccionan los insumos de acuerdo a la calidad, economía y oportunidad que brindan las empresas o laboratorios para beneficio de las Entidades Asociadas y sus usuarios; en la actualidad se continúa con esta importante gestión.

Desde el 1 de Agosto de 2003 llega a la Gerencia el doctor Miguel Ángel Rendón Moncada, el cual perfecciona el modelo e inicia en compañía de los organismos directivos, cambios importantes en la estructura económica, social y organizacional, logrando así un reconocimiento y posicionamiento de la cooperativa a nivel nacional. Para ello fue necesario el posicionamiento de la cooperativa como unidad de negocios que no sólo beneficia a sus asociados de manera comercial evitando el desgaste administrativo en la compra y venta de insumos, sino también reinvertiendo sus excedentes en los hospitales y su comunidad.

Debido al aumento de la demanda de insumos con las Entidades Asociadas, y su compromiso para el apoyo de la estrategia Outsourcing, Coodesuris fortaleció su proceso comercial y técnico, aumentando su stock de inventario, adoptando un mayor orden en la entrega de insumos a los hospitales y usuarios, programando los pedidos y realizando a través de sus Químicos Farmacéuticos un acompañamiento continuo a las farmacias de los hospitales para supervisar el proceso de calidad en el almacenamiento, dispensación y venta al usuario.

En el año 2004, dada la finalización de la vigencia del Plan de Desarrollo anterior, se diseñó una plataforma estratégica, que involucró al talento humano de la Cooperativa y de los hospitales asociados, acorde a la nueva estructura y requerimientos, con un enfoque totalmente dirigido hacia la satisfacción del hospital asociado, materializado en su nuevo eslogan: “Somos parte de su institución”, y del cliente interno.

Dicho eslogan enmarca la nueva filosofía de la Cooperativa, la cual busca cambiar el concepto de “Proveedor”, que tienen los hospitales asociados, por el de unidad funcional de apoyo.

Igualmente, convencido de la necesidad de continuar con el proceso de mejoramiento brinda todo su apoyo a la implementación del Sistema de Gestión de la Calidad, el cual obtiene su certificación en junio del año 2005 por el ente certificador Bureau Veritas Quality International.

Debido al buen comportamiento financiero de la cooperativa, el Consejo de Administración en el año 2006 tomó la decisión de impactar directamente las finanzas de los asociados a través de una bonificación que fue distribuida equitativamente de acuerdo a compras y oportunidad en los pagos, una vez más Coodesuris manifestaba la importancia de mantener el outsourcing y los grandes beneficios económicos que se generaban debido a la negociación.

A partir del año 2007 se generaron grandes beneficios enfocados a las Entidades Asociadas como la adquisición de una nueva planta física que permitió adecuar las oficinas y mejorar el proceso de almacenamiento cumpliendo con la Política de Salud ocupacional y seguridad Industrial.

Gracias a esto, Coodesuris permanecerá en un proceso de mejoramiento continuo y ampliación de sus servicios, para contribuir al desarrollo de sus entidades asociadas y el beneficio de su comunidad.

1.2 MISIÓN

Coodesuris es una Administradora Pública Cooperativa que presta servicios de apoyo hospitalario, especializada en el suministro de insumos, con criterios de calidad, oportunidad, eficiencia y economía, contribuyendo a la competitividad de las entidades asociadas para que ellos generen en la comunidad un alto impacto social.

1.3 VISIÓN

COODESURIS 2010. Mantendrá su solidez financiera con reconocimiento en el mercado nacional, por medio de sistemas de gestión apoyados en tecnología e infraestructura adecuada y talento humano idóneo, generando impacto social en sus asociados y comunidad.

1.4 VALORES CORPORATIVOS

- ✓ Responsabilidad.
- ✓ Lealtad.
- ✓ Compromiso.
- ✓ Honestidad.
- ✓ Pertenencia.
- ✓ Respeto

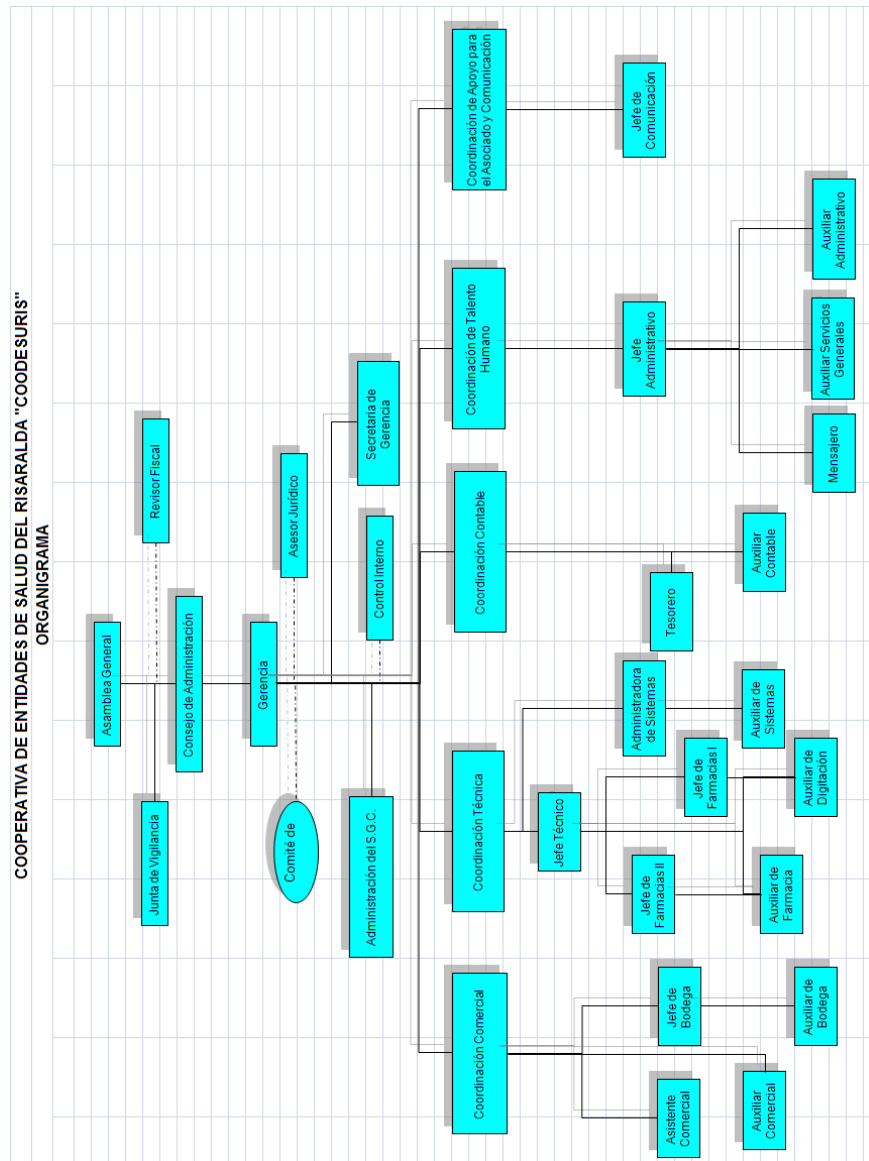
1.5 POLÍTICAS CORPORATIVAS

- ✓ Transparencia.
- ✓ Calidad.
- ✓ Responsabilidad social.
- ✓ Competitividad.
- ✓ Desarrollo del talento humano.
- ✓ Oportunidad.

1.6 POLÍTICAS DE CALIDAD

La administración de los servicios farmacéuticos y de almacén de nuestras entidades asociadas y la comercialización de insumos hospitalarios a no asociados; se fundamenta en la mejora continua de nuestro sistema de gestión de calidad, a través de alianzas estratégicas, apoyo técnico y tecnológico, comunicación efectiva y talento humano comprometido y calificado que interactúa en un adecuado clima organizacional, generando valores agregados e impacto social.

1.7 ORGANIGRAMA



2. DIAGNÓSTICO

2.1 SERVIDOR DE COODESURIS

2.1.1 Estado Directorio Activo

Las bases de datos del directorio activo se encuentran desactualizadas, con información obsoleta acerca de los funcionarios de la cooperativa y los componentes de red.

La búsqueda de un equipo o persona se torna difícil debido a los nombres que identifican los componentes del directorio activo, la información en muchos aspectos es redundante y le falta estructuración.

Los usuarios y equipos pertenecen a grupos con privilegios sin ningún orden, estructura o política de seguridad establecida. En pocas palabras no es lógica la configuración del directorio activo.

Las contraseñas asignadas a los usuarios no corresponden a ningún tipo de estándar ni política, son inseguras y poco administrables por parte de la administración de sistemas de la cooperativa.

2.1.2 Estado Archivos Compartidos

COODESURIS trabaja sobre una red local, donde los equipos están en red para compartir impresoras y otros recursos, el servidor tiene unos discos y carpetas compartidas abiertas a cualquier tipo de usuario ya que no existen permisos establecidos.

Los espacios donde se almacenan las copias de seguridad tanto de los usuarios (en la unidad H:) como de los archivos globales que maneja la cooperativa (en la unidad K:). No poseen ninguna restricción o política de seguridad.

Existe un espacio designado para compartir archivos entre los funcionarios llamado “Unidad de Red Z:”, teniendo en cuenta que los funcionarios suben todo tipo de archivos a este espacio no se tienen políticas de control o administración que mantengan este espacio depurado.

2.1.3 Estado de las Funciones de Mantenimiento al Servidor

Básicamente en Coodesuris existe un manual en el cual se planea el mantenimiento preventivo y correctivo para las estaciones de trabajo con un tiempo de periodicidad estipulado, lo escrito en este manual no se puede aplicar para el servidor por ser un equipo más robusto, con mayor grado de responsabilidad y con mayor desempeño ante las otras maquinas.

No existe un manual a seguir para el mantenimiento del servidor ni mucho menos una programación definida.

El estado del servidor manifestaba que:

- Falta Hacer un Escaneo de discos a bajo nivel.
- Después de realizar el seguimiento correspondiente se evidenció que los discos del servidor se encontraban de la siguiente forma:

El servidor contiene 3 discos de 146 GB, distribuidos de la siguiente forma:

- ✓ 2 discos con 2 particiones cada uno
- ✓ 1 disco con 1 partición

Para un total de 5 Volúmenes.

En el proceso de observación se halló que 2 de los volúmenes del servidor se encuentran con un alto porcentaje de fragmentación.

Se halló una partición de un disco no formateado, por otra parte el disco C: / presenta poco espacio.

No se está haciendo un uso eficiente de los discos y no se han establecido métodos de control.

- Falta Revisar la correcta configuración de los servicios disponibles
- Falta Analizar y controlar los logs
- Falta Establecer tareas de Disk Cleanup.
- Falta Establecer un Registry Cleanup.
- Falta Mantenimiento en la Limpieza de Temporales.

2.1.4 Estado de las Copias de Seguridad

En Coodesuris se manejan 2 tipos de copia:

- ✓ Copia Global
- ✓ Copia de Usuarios

La copia global abarca todos los datos de los Programas utilizados por la Cooperativa que son (Alfa, Novasoft), y otras carpetas que se describen a continuación:

- ✓ Datvis3
- ✓ Farmacia
- ✓ Planes
- ✓ Calidad
- ✓ S.G.C ISO 9001

La copia de Usuarios se realiza los viernes de cada semana contiene información que los mismos usuarios almacenan, debido a esto la administración de sistemas pierde el control de estas copias y las copias alcanzan tamaños bastante grandes para ser manejadas en medios extraíbles.

Sólo la copia global se realiza diariamente y se almacena en la unidad (K) del servidor, esta unidad se encuentra compartida y sin restricciones por ende cualquier tipo de usuario tiene control total sobre las copias de seguridad.

Actualmente las copias de seguridad dependen del sistema de tareas programadas de Windows Server y el programa Winzip en su versión 11.

Gran parte de las veces que se realizan las copias de seguridad, muestra un informe de error al finalizar, al cual se le debe hacer seguimiento.

2.2 RED DE COODESURIS

2.2.1 Estado de las Estaciones de Trabajo

Las máquinas cliente con las que cuenta Coodesuris poseen muy buenas características en cuanto a rendimiento se refiere sin dejar de lado que son programados sus respectivos mantenimientos.

En las labores de mantenimiento falta anexar el proceso de reconfigurar servicios y deshabilitar el inicio predeterminado en el cual se cargan aplicaciones en memoria que no son innecesarias para el desempeño laboral.

No existe un método masivo de distribución de Actualizaciones.

Las actualizaciones del Service pack de Windows no se encuentran al día, de 25 equipos con el que cuenta la Sede principal de la cooperativa tan sólo 3 de ellos poseen la última versión.

También se evidenció que de 25 equipos que operan en la cooperativa 11 se encuentran con la versión de office 2003, la cual no está licenciada.

2.2.2 Estado del Antivirus Kaspersky

No hay una persona designada para la administración de la consola de Kaspersky que agregue a la red lógica los nuevos equipos detectados en la red local e instale en ellos las aplicaciones necesarias, de forma regular.

Se evidenciaron algunos equipos en la cooperativa que no se encontraban en la base de datos y otros que sí pero se encontraban desactualizados y en espera que se les realizara un escaneo completo para así entrar a la red lógica como equipos seguros.

No existe un seguimiento a los informes, avisos y mensajes que genera el antivirus en caso de novedades en la red.

Falta vigilancia en los espacios disponibles en el servidor para almacenar envíos desde los clientes y así como la memoria libre disponible en el servidor para procesar los datos enviados.

No se Hacen copias de seguridad periódicas de los datos del sistema de administración.

No se realizan mantenimientos de depuración de información a las bases de datos de la consola de administración.

2.2.3 Estado de las Políticas de seguridad informática

Actualmente en Coodesuris no existe ningún mecanismo ni documento que sustente las PSI, puesto que no se ha hecho la labor de crear políticas, aún no se tiene la conciencia de que la organización desde sus inicios ha crecido en forma considerable y poco a poco se sale de las manos, creando vulnerabilidades si no se toman medidas de aseguramiento.

El hecho de que no exista un documento que aplique políticas no quiere decir que no se maneje algún tipo de seguridad, lo único que pasa es que la seguridad manejada no tiene un orden específico, una estructura, por ejemplo se hace realmente difícil contemplar cuándo y en qué momento se deben renovar las contraseñas, quien ha perdido su contraseña, para asignar una nueva contraseña no se tiene un estándar y difícilmente un nivel de seguridad por usuarios.

2.2.4 Estado del Firewall

El firewall con el que trabaja Coodesuris provee una interfaz web para su respectiva administración.

En la evaluación que se realizó se evidenció que no se encuentran registros de cada uno de los hechos ocurridos en el firewall y por ende no se realiza seguimiento.

No existe una persona seleccionada encargada de la administración del firewall que cumpla con las obligaciones de atención que este requiere.

2.3 MEJORAS TÉCNICAS Y TECNOLÓGICAS EN LA OPERACIÓN

2.3.1 Estado Técnico del servidor

Como primera instancia la mejora que requiere el servidor es de carácter físico, donde centralmente se entraron a evaluar tres aspectos que garanticen el trabajo y planes de contingencia para la cooperativa. Los cuales se relacionan a continuación:

- Anexo de fuente de poder
- Discos Duros
- Arreglo de Discos
- Memoria RAM

Usualmente un servidor se encuentra encendido las 24 horas del día durante los 365 del año, aunque son máquinas resistentes y se encuentran en una habitación con refrigeración externa la **fuentes de poder** que traen por defecto no es suficiente si se requiere manejar planes de contingencia, debido a las exposiciones que ésta maneja como alimentador central de energía, es por tal razón que se considera instalar una **Fuente de poder redundante**, y así garantizar que las operaciones continúen con normalidad en caso de falla de alguna de las dos fuentes, a simple vista invertir en una fuente de poder adicional no se toma como consideración en el momento de actualizar pero de nada vale tener una máquina con las mejores características en cuanto a velocidad, procesamiento y rendimiento si se tiene la vulnerabilidad de fallo en la alimentación de energía.

En los **Discos Duros** se almacena toda la información que representan un alto porcentaje de las operaciones y el funcionamiento de la cooperativa, el almacenamiento se queda corto a medida que la cooperativa crece por tal razón es preciso incrementar la capacidad y no sufrir por falta de espacio en discos. Estos discos son vulnerables a fallas debido al uso frecuente que se les da en cada acceso realizado por los funcionarios, bien sea en consultas de información o como peticiones hechas al sistema, cabe rescatar que existen métodos como planes de contingencia en caso de falla de los discos como lo son los Arreglos de Discos donde se tiene toda la información de un disco almacenada en otro en tiempo real creando un espejo constante y en caso de fallo de cualquiera de los dos discos, siguen su curso normal y no afecta las actividades laborales, es por tal razón que se debe considerar la implementación de éste método en Codesuris, donde actualmente no se cuenta con ningún tipo de respaldo.

Como último aspecto tenemos la **Memoria RAM**, este elemento es en cierto modo uno de los menos importantes en cuanto a la planeación de contingencias, pero sí es uno de los más importantes en cuanto al rendimiento de la máquina se refiere ya que cualquier proceso que se ejecute en el servidor se monta sobre la Memoria RAM y de acuerdo a la capacidad que esta tenga el proceso puede darse de manera más eficiente o demorada.

2.3.2 Estado de la Conexión a las farmacias

Coodesuris realiza unas labores de administración en las farmacias de los hospitales del departamento de Risaralda, con las cuales mantiene una constante comunicación vía web para la transferencia de información y vía telefónica para la solución de inconvenientes, asesorías u otros datos que se requieran.

Tener una conexión de acceso remoto con las diferentes farmacias beneficiaría de forma significativa los procesos que trabaja la cooperativa, claro está todo depende del tipo de conexión que se implemente, ya que una de las desventajas que puede traer todo esto es la falta de seguridad a la que se expone la información.

2.3.3 Estado de la Página Web

La página web de la cooperativa se encuentra almacenada con el dominio de Coodesuris.com este plan provee un espacio total de 200 MB, de las cuales sólo 2MB se encuentran libres, por lo tanto nos da para sacar la conclusión que el espacio asignado es muy poco para las operaciones que maneja Coodesuris por medio de su página web. Uno de los factores afectados por el poco espacio son las cuentas de correo, éstas requieren una cantidad mínima para operar, pero lastimosamente la cantidad que se le puede asignar a cada cuenta en Coodesuris está por debajo de ese límite, así que éstas con frecuencia presentan diversas fallas. Por otra parte como se trata de una web administrable, el personal de comunicación carga en la página web contenido de interés general el cual en ocasiones no se puede hacer por las mismas razones de espacio.

El motivo de falta de espacio impide que las actividades que se realizan por medio de la página web se ejecuten de una forma eficiente por tal razón es necesario buscar otras soluciones u alternativas.

3. EJES DE INTERVENCIÓN

| Eje | Destinatario | Descripción |
|--|---|--|
| Administración del Servidor de Coodesuris | Funcionarios y administración de sistemas | Mejora en la administración y Manejo de los componentes de red, desarrollo de políticas de seguridad que puedan ser aplicadas y así obtener un incremento en la seguridad de la empresa. |
| Administración de la Red | Funcionarios y Administración de sistemas | Incrementar las técnicas dirigidas a mantener una red operativa, eficiente, segura, constantemente monitoreada y con una planeación adecuada propiamente documentada. |
| Mejoras Técnicas y Tecnológicas en la operación. | Funcionarios y Administración de sistemas | Implementación de planes de contingencia que soporten fallos operativos haciendo uso de la tecnología existente, disminuyendo los procesos y tiempos de respuesta |

Tabla 1 Descripción ejes de intervención

4. JUSTIFICACIÓN DE LOS EJES

4.1 ADMINISTRACIÓN DEL SERVIDOR DE COODESURIS

4.1.1 Directorio Activo de Windows 2003 Server

Hoy en día, los ordenadores existentes en cualquier organización se encuentran formando parte de redes, de forma que pueden intercambiar información. Desde el punto de vista de la administración de sistemas, la mejor forma de aprovechar esta característica es la creación de un *dominio* de sistemas, en donde todos los procesos administrativos y de seguridad se encuentren *centralizados* en uno o varios servidores, facilitando así la labor del administrador. Windows 2003 utiliza el concepto de **directorio** para implementar dominios de sistemas.

En el ámbito de las redes de ordenadores, el concepto de *directorio* (o almacén de datos) es una estructura jerárquica que almacena información sobre objetos en la red, normalmente implementada como una base de datos optimizada para operaciones de lectura y que soporta búsquedas de grandes datos y con capacidades de exploración.

Active Directory es el servicio de directorio de una red de Windows 2003. Este servicio almacena información acerca de los recursos de la red y permite el acceso de los usuarios y las aplicaciones a dichos recursos, de forma que se convierte en un medio de organizar, controlar y *administrar* centralizadamente el acceso a los recursos de la red.

Los equipos de la red son los *clientes* de dicho servicio de directorio, con lo que reciben toda la información almacenada en los controladores. Esta información incluye no sólo las cuentas de usuario, grupo, equipo, etc., sino también los perfiles de usuario y equipo, directivas de seguridad, servicios de red, etc. El Directorio Activo se convierte así en la herramienta fundamental de administración de toda la organización.

Una de las ventajas fundamentales del Directorio Activo es que separa la estructura *lógica* de la organización (dominios) de la estructura *física* (topología de red). Ello permite, por una parte, independizar la estructuración de dominios de la organización de la topología de la(s) red(es) que interconectan los sistemas; y, por otra parte, permite administrar la estructura física explícitamente cuando es necesario, de forma independiente de la administración de los dominios.¹

4.1.2 Compartir archivos en la Red de Coodesuris

En una red se puede compartir la información y los recursos. Gracias a esta facilidad contamos con una serie de ventajas:

- ✓ Podemos compartir los periféricos caros, como pueden ser las impresoras. En una red, todos los ordenadores pueden acceder a la misma impresora.
- ✓ La transferencia de archivos a través de la red elimina el tiempo que se pierde copiando archivos en un medio extraíble y luego en otro PC. Además, hay menos restricciones en el tamaño del archivo que se transfiere.
- ✓ Se Puede centralizar programas informáticos clave, como son los de finanzas y contabilidad. A menudo, los usuarios tienen que acceder al mismo programa para trabajar en él simultáneamente. Un ejemplo de lo anterior sería el sistema Novasoft que maneja Coodesuris, en el que es importante evitar que los despachos se efectúen dos veces.

¹ Just another WordPress.com weblog. Windows server 2003: Dominios windows server y directorio activo. (Sitio de internet). Disponible en: <http://admonredes.wordpress.com/dominios-windows-server-y-directorio-activo/> Consultado: 17 de abril de 2009

- ✓ Se puede utilizar un programa informático para hacer copias de seguridad de archivos automáticamente, con lo que se ahorra tiempo y se garantiza que todo el trabajo ha quedado guardado²

4.1.3 Funciones de Mantenimiento al servidor

El mantenimiento de servidores es tanto o más importante que el mantenimiento de la red pero no se pasa por alto por motivos obvios. Esto significa que a pesar de que muchas empresas no realizan un mantenimiento de su red, por lo general sí realizan un mantenimiento en sus servidores, aunque en forma mínima. Cuando decimos por lo general no significa que siempre se realice, hay algunas empresas que aún no son conscientes de la importancia del mantenimiento de sus servidores, porque creen ciegamente que los servidores al no ser utilizados por usuarios de forma directa, no caen en las problemáticas de otras computadoras o sistemas.

Dependiendo de los sistemas dentro de la empresa será el tipo de mantenimiento y la regularidad del mismo. Algunos sistemas requieren menos mantenimiento que otros, algunos sistemas tienen más flexibilidad y escalabilidad que otros, esta distinción es lo que permite a las empresas además elegir cuál de estos sistemas le entregará mejores resultados, tomando en cuenta también el tipo de servicios que requieren, por supuesto.³

4.1.4 Plan de Copia de seguridad

Crear un plan de copia de seguridad y restablecimiento de la información constituye una parte crítica de cualquier implementación en una empresa. Para crear un plan es preciso conocer el tamaño y el alcance de la actividad, designar a

² Campus Virtual UM. Open Course Ware. Facultad de Ingeniería. Redes. (Sitio de Internet). Disponible en: http://ocw.virtualum.edu.co/ocwum/facultad-de-ingenieria-1/redes-i/redes-i/doc/Que_es_una_Red1.doc.

Consultado: 23 de abril de 2009

³ Allele Mantenimiento de redes y Servidores. Mantenimiento de servidores. Disponible en: <http://www.allele.com.ar/mantenimiento-de-servidores.php> Consultado: 20 de Abril 2009

una persona o un equipo de personas que realicen las copias de seguridad, determinar una estrategia de almacenamiento de dichas copias y estudiar qué software de copia de seguridad es el que mejor responde a las necesidades de la organización. También debe planear la comprobación de la integridad de las copias de seguridad por medio de restablecimientos de prueba regulares.

Existen varios factores que hay que tener en cuenta al planear las copias de seguridad de un Servidor; por ejemplo, cuándo programarlas, qué datos incluir en ellas y cómo almacenarlas. No todos los factores desembocarán en las mismas conclusiones, pero un estudio detallado del conjunto orientará durante la creación de un plan de copia de seguridad que satisfaga las necesidades actuales de la organización.

Considerar quién será responsable de las copias de seguridad de los equipos críticos. ¿Será una persona sola o un equipo? Si las copias de seguridad de los equipos críticos se van a efectuar fuera del horario laboral, puede ser conveniente automatizarlas. Sin embargo, en ese caso deberá haber alguien que se asegure de que las copias de seguridad automatizadas se han realizado correctamente. Si necesita restablecer un servidor repentinamente a partir de la copia de seguridad, ¿hay alguna manera de ponerse en contacto con estas personas fuera del horario laboral normal? Si una persona no está disponible, ¿hay alguien más que pueda realizar una copia de seguridad de los datos o restablecerlos? ¿Existe algún documento de recuperación de desastres? ⁴

⁴ Centro de desarrollo de Team Foundation Server. Biblioteca. Herramientas y lenguajes de desarrollo. Visual Studio 2005. Documentación de Visual Studio Team System. Documentación de Team Foundation. Administradores de Team Foundation. Planeamiento de Team Foundation Server. Plan de mantenimiento del servidor. Plan de copia de seguridad y restablecimiento. (Sitio de Internet) Disponible en: [http://msdn.microsoft.com/es-es/library/ms316430\(VS.80\).aspx](http://msdn.microsoft.com/es-es/library/ms316430(VS.80).aspx) Consultado 17 de abril de 2009

4.2 ADMINISTRACIÓN DE LA RED

4.2.1 Estaciones de trabajo y sus recursos

Una estación de trabajo es una computadora que facilita a los usuarios el acceso a los servidores y periféricos de la red. Para una posible comunicación tienen una tarjeta de red y está físicamente conectada por medio de cables u otros medios no guiados con los servidores. Los componentes para servidores y estaciones de trabajo alcanzan nuevos niveles de rendimiento informático, al tiempo que ofrecen fiabilidad, compatibilidad, escalabilidad y arquitectura avanzada ideales para entornos multiproceso.

¿Por qué es necesario optimizar los recursos lógicos?

En la actualidad existen gran cantidad de métodos y herramientas para optimizar nuestros computadores, cabe resaltar que no todos son 100% confiables, y se debe tener un conocimiento previo para no causar daños traumáticos en el transcurso de los cambios.

Muchos programas que se instalan o procesos que se han ejecutado se cargan en memoria y ocupando espacio así ya no se empleen, desmejorando notablemente el rendimiento y la producción de nuevas operaciones.

Por otra parte tenemos los Servicios de Windows XP que se pueden calificar como pequeños programas controladores que se ejecutan en segundo plano y que controlan una tarea muy específica en el sistema, no todos los servicios son necesarios para el funcionamiento básico y por esta razón se deben desactivar, logrando una mejora en el rendimiento.

¿Por qué es importante tener las estaciones de trabajo actualizadas?

La administración de actualizaciones es el proceso de control de la implementación y mantenimiento de las versiones de software provisionales en los entornos de producción. Ayuda a mantener la eficacia operativa, solucionar las

vulnerabilidades de seguridad y mantener la estabilidad de su entorno de producción.

Si la cooperativa no puede determinar ni mantener un nivel conocido de confianza en sus sistemas operativos y software de aplicación, puede presentar varias vulnerabilidades de seguridad; si se aprovechan, se puede producir la pérdida de beneficios y de propiedad intelectual. Para reducir esta amenaza se debe disponer de sistemas configurados correctamente, usar el software más reciente e instalar las actualizaciones de software recomendadas.

Se deben tener en cuenta las áreas siguientes al determinar las posibles repercusiones financieras de una administración deficiente de las actualizaciones:

➤ Tiempo de inactividad

¿Cuál es el costo del tiempo de inactividad de equipos en su entorno?
¿Qué sucedería si se interrumpen sus sistemas empresariales críticos? Determine el costo de la pérdida de productividad de los usuarios finales, la pérdida de transacciones en sistemas críticos y la pérdida de negocio durante un incidente. La mayoría de ataques provocan tiempo de inactividad, ya sea por el propio ataque o por la corrección correspondiente que se necesitará para la recuperación. Algunos ataques han dejado los equipos inactivos durante varios días.

➤ Tiempo de corrección

¿Cuál es el costo de corregir un problema extendido en su entorno?
¿Cuánto cuesta reinstalar un equipo? ¿Y si se tuvieran que reinstalar todos los equipos? Muchos ataques de seguridad requieren la reinstalación completa para garantizar que no haya oportunidad de ataque (que pudiera aprovecharse en un futuro).

➤ Integridad dudosa de los datos

Si la integridad de los datos se ve dañada debido a un ataque, ¿cuál es el costo de recuperar los datos de la última copia de seguridad correcta o de confirmar la exactitud de los mismos con los clientes y socios?⁵

4.2.2 Antivirus Kaspersky

Tener el control centralizado de las principales tareas administrativas y ofrecer un completo control, del sistema antivirus, siendo compatible con todas las configuraciones de red que utilicen el protocolo TCP/IP. Son unas cuantas tareas que se pueden ejecutar con una buena administración del antivirus.

Las principales bondades que ofrece Kaspersky se describen a continuación:

- Distribuir y eliminar de forma remota aplicaciones Kaspersky Lab en y desde los equipos de red.
- Administrar eficazmente las claves de licencia. La Administración de Kaspersky permite instalar de forma centralizada claves de licencia para todas las aplicaciones Kaspersky Lab, supervisar la correspondencia entre el número de usuarios con licencia y las aplicaciones Kaspersky Lab instaladas en la red, así como controlar las fechas de caducidad de las licencias.
- Actualizar automáticamente la base antivirus. Puede actualizar la base antivirus de forma centralizada para todas las aplicaciones, sin tener que conectar directamente cada equipo a los servidores de actualización. Puede planificar que la actualización se realice automáticamente, a una hora

⁵ Microsoft. Support TechNet Security. Proceso de Administración de Revisiones. (Sitio de internet). Disponible en: <http://www.microsoft.com/spain/technet/security/guidance/patchmanagement/default.msp> Consultado 3 de Mayo de 2009.

determinada, para mantener siempre actualizada su protección y supervisar el proceso de actualización en los equipos cliente.

- Recopilar informes de todas las instalaciones. Las funciones mejoradas de creación de informes de La Consola de Administración de Kaspersky permiten obtener las estadísticas sobre las operaciones de todas las instalaciones y crear informes a partir de las estadísticas más recientes.
- Mediante un sistema de notificaciones de eventos específicos sobre el funcionamiento de la aplicación y el envío de notificaciones. Es posible especificar el conjunto de eventos que requieren notificación. Estos eventos producidos durante el funcionamiento de la aplicación pueden ser, por ejemplo, la detección de un virus, un fallo en la actualización o un nuevo equipo que aparece en la red.⁶

4.2.3 Herramienta Wireshark

Wireshark es un analizador de red con el que podemos tener una visión del tráfico que pasa por nuestra red. Hay que decir que este tipo de programas puede llegar a ser muy útil para detectar tráfico innecesario y solucionar problemas en redes de comunicaciones, para desarrollo de software y protocolos. Aunque también la gente lo puede utilizar para cosas no tan productivas.

Todo administrador de red debe contar con un analizador y así detectar posibles inconvenientes que puedan llegar a colapsarla o desmejorar su tráfico. En la red existen cantidades de usuarios maliciosos que su única finalidad es violar sistemas y consumir sus recursos, generando dolores de cabeza a los administradores de la red, es en ese momento donde Wireshark nos ayuda a encontrar operaciones sospechosas en el tráfico y paquetes que puedan llegar a causar algún daño.

⁶ Kaspersky Lab's Official Sites. Kaspersky Lab documentation. (Sitio de Internet). Disponible en: http://downloads.kaspersky-labs.com/docs/spanish/kasp6.0_ak_deployguidees.pdf Consultado 14 de junio de 2009

4.2.4 Firewall

Un Firewall en Internet es un sistema o grupo de sistemas que impone una política de seguridad entre la organización de red privada y el Internet. El firewall determina cual de los servicios de red pueden ser accesados dentro de esta por los que están fuera, es decir quién puede entrar para utilizar los recursos de red pertenecientes a la organización. Para que un firewall sea efectivo, todo tráfico de información a través del Internet deberá pasar a través del mismo donde podrá ser inspeccionada. El firewall podrá únicamente autorizar el paso del tráfico, y el mismo podrá ser inmune a la penetración. Desafortunadamente, este sistema no puede ofrecer protección una vez que el agresor lo traspasa o permanece en torno a este.⁷

Es importante resaltar que los Firewalls no deben simplemente instalarse y darles la espalda, todo lo contrario se les debe dar una constante administración.

4.2.5 Políticas de seguridad en Coodesuris

Las políticas de seguridad informática (PSI) surgen como una herramienta organizacional para concientizar a los colaboradores de la organización sobre la importancia y sensibilidad de la información, servicios críticos que permiten a la empresa crecer y mantenerse competitiva. Ante esta situación, el proponer o identificar una política de seguridad requiere un alto compromiso con la organización, agudeza técnica para establecer fallas, debilidades y constancia para renovar y actualizar dicha política en función del dinámico ambiente que rodea las organizaciones modernas.

No se puede considerar que una política de seguridad informática es una descripción técnica de mecanismos, ni una expresión legal que involucre sanciones a conductas de los funcionarios, es más bien una descripción de lo que deseamos proteger y él por qué de ello, pues cada política de seguridad es una invitación a cada uno de sus miembros a reconocer la información como uno de sus principales activos así como, un motor de intercambio y desarrollo en el ámbito de sus negocios. Por tal razón, las políticas de seguridad deben concluir en

⁷ Duamu. Portada. Manuales firewalls y seguridad en internet. (Sitio de Internet). Disponible en <http://www.duamu.com/re/manual/1680/id/2652/manuales-firewalls-y-seguridad-en-internet.html> Consultado 26 de Junio de 2009

una posición consciente y vigilante del personal por el uso y limitaciones de los recursos y servicios informáticos.

4.3 MEJORAS TÉCNICAS Y TECNOLÓGICAS EN LA OPERACIÓN

4.3.1 Servidor

Un gran porcentaje de las empresas desarrollan sus actividades laborales sobre equipos llamados servidores, éstos son en su mayoría el eje central de donde se ramifica toda la red de operaciones, físicamente son maquinas resistentes a fallos, veloces, y en su defecto contienen gran parte de la información manejada por la empresa. Comúnmente las aplicaciones en las empresas se trabajan de manera Cliente – servidor que significa que una parte de la información es almacenada, ejecutada y procesada en el servidor y otra parte en el cliente. Independientemente de la estructura de red y operaciones que maneje la empresa, a los servidores se les confía el desempeño, la información y los procesos internos, tanto así que si este llegase a fallar las perdidas en tiempo y dinero serian bastantes considerables.

No obstante, el crecimiento constante de las empresas, la necesidad de comunicación, la vulnerabilidad de la información en su intercambio y los avances tecnológicos tanto en hardware como en Software hacen que nuestros sistemas se vuelvan inseguros, desmejoren su rendimiento y se vean obsoletos frente a otras tecnologías.

4.3.2 Conexión de Acceso remoto

Coodesuris realiza unas labores de administración en las farmacias de los hospitales del departamento de Risaralda, con las cuales mantiene una constante comunicación vía web para la transferencia de información y vía telefónica para la solución de inconvenientes, asesorías u otros datos que se requieran.

Tener una conexión de acceso remoto con las diferentes farmacias beneficiaría de forma significativa los procesos que trabaja la cooperativa, claro está todo depende del tipo de conexión que se implemente, ya que una de las desventajas que puede traer todo esto es la inseguridad de la información.

4.3.3 Página web

Básicamente las páginas web sirven para dar a conocer especificaciones de una empresa, mostrar al mundo entero a que actividades se dedica y que servicios están dispuestos a ofrecer. Hoy en día es bastante común Adquirir un espacio en la internet para montar un sitio web, se pueden adquirir paquetes integrados que van desde diseño, cuentas de correo, subdominios entre otros, o simplemente se puede adquirir sitios sencillos con espacios de almacenamiento a la medida.

Al momento de actualizar una página web ya existente se debe tener bien claro cuál es el motivo si es por si acaso una reforma en el diseño, el aumento de espacio, el cambio de servidor (Hosting), cambio de dominio, entre muchos otros aspectos, ya que de acuerdo a lo que se quiera las características de otros componentes pueden variar.

5. OBJETIVOS

5.1 OBJETIVO GENERAL

Incrementar las técnicas dirigidas a mantener una red operativa, eficiente, segura, constantemente monitoreada con una planeación adecuada y propiamente documentada que soporte fallos operativos. Lo anterior se logra haciendo uso de la tecnología existente, incrementando procesos y tiempos de respuesta, siendo la seguridad el principal factor a tener en cuenta.

5.2 OBJETIVOS ESPECÍFICOS

1. Optimizar la administración del servidor, reduciendo fallos operativos e implementando mejoras de acceso a los recursos de la red.
2. Brindar una correcta administración a la red, consiguiendo el mejor rendimiento por medio de herramientas actuales que brinden mayor seguridad.
3. Asesorar a la Cooperativa en cuanto a la mejora estratégica donde se prevean contingencias y obtenga de sus procesos una mayor utilidad.

6. PRESENTACIÓN Y ANÁLISIS DE LOS RESULTADOS

6.1 SERVIDOR DE COODESURIS

6.1.1 Acciones Tomadas en el Directorio Activo

Se obtiene un listado de todos los usuarios que se encuentran registrados en el directorio activo. Ver Figura 2

| No | Nombre Inicio de Sesión de Usuario | Nombre |
|----|------------------------------------|-------------------------------|
| | Administrador | |
| 1 | Administradorcalidad | Administradorcalidad |
| 2 | Sistemas | Alba lucia Bedoya Benjumea |
| 3 | coordinadoraRH | Alexandra Arcila |
| 4 | recepcion | Ana Delia Acevedo Rios |
| 5 | comercial | Andrea Cardona |
| 6 | jefetec | Andres Alvarez |
| 7 | asiscomercial | Angelica Serna |
| 8 | aprendizsena | aprendizsena |
| 9 | Aux-sistemas | Aux-sistemas |
| 10 | aux-facturacion | Auxiliar Facturacion |
| 11 | Auxbodega | Carlos A. Echeverry |
| 12 | sistemas1 | CARLOS JHON |
| 13 | tesoreria | Claudia Patricia Alvarez |
| 14 | secretgerencia | Claudia Lopez |
| 15 | control_int | Control Interno |
| 16 | invitado | |
| 17 | coordinadoraT | Isabel Cristina Muñoz Molina |
| 18 | AUXILIAR | Isabel Patricia Izquierdo |
| 19 | comunicación | Julian Andres Zapata |
| 20 | Aux_comercial | Luz Adriana Florez |
| 21 | gerentegral | Miguel Angel Rendon Moncada |
| 22 | AUX_CONTABILIDAD | Olga Lucia Navarro |
| 23 | Pastora_C | Pastora Cañaveral |
| 24 | comunicacio1 | Practicante Comunicación |
| 25 | comunicacion2 | Practicante Comunicación |
| 26 | quimicos | Quimicos Coodesuris |
| 27 | administrativa | Rosa Cardona |
| 28 | SERVIDOR2000 | SERVIDOR2000 |
| 29 | servidor2006c | servidor2006c |
| 30 | Servidoresoporte | Servidoresoporte |
| 31 | PORSISTEMAS | TODOS |
| 32 | auxcomercia1 | Victoria Eugenia Castaño |
| 33 | auxcomercial | Viviana Andrea Builes Sanchez |

Figura 1 Primer Listado de Usuarios Directorio Activo

Por medio de observación directa e indagación a la administración de sistemas, se reorganiza la lista de usuarios identificando qué usuarios operan actualmente. Ver Figura 3

| No | Nombre Inicio de Sesión de Usuario | Nombre |
|----|------------------------------------|------------------------------|
| | Administrador | |
| 1 | Administradorcalidad | Karol Eliana Gonzales |
| 2 | Sistemas | Alba Lucia Bedoya Benjumea |
| 3 | coordinadoraRH | Alexandra Arcila |
| 4 | repcion | Ana Delia Acevedo Rios |
| 5 | comercial | Andrea Cardona |
| 6 | asiscomercial | Viviana Andrea Builes |
| 7 | Aux-sistemas | Carlos A. Huertas |
| 8 | aux-facturacion | Natalia Giraldo |
| 9 | Auxbodega | Carlos A. Echeverry |
| 10 | tesoreria | Claudia Patricia Alvarez |
| 11 | secretgerencia | Claudia Lopez |
| 12 | coordinadoraT | Isabel Cristina Muñoz Molina |
| 13 | AUXILIAR | Isabel Patricia Izquierdo |
| 14 | comunicación | Julian Andres Zapata |
| 15 | Aux_comercial | Yudi Catherine Valencia |
| 16 | gerentegral | Miguel Angel Rendon Moncada |
| 17 | AUX_CONTABILIDAD | Olga Lucia Navarro |
| 18 | Pastora_C | Pastora Cañaveral |
| 19 | comunicacio1 | Practicante Comunicación |
| 20 | comunicacion2 | Practicante Comunicación |
| 21 | administrativa | Rosa Cardona |
| 22 | auxcomercial1 | Luisa Fernanda Acosta |
| 23 | adminsistemas | Hernan Mauricio Atuesta |
| 24 | JefeBodega | Carlos Alberto Echeverry |

Figura 2. Segundo Listado de Usuarios Directorio Activo

Se reasignan nombres de inicio de sesión y contraseñas a los usuarios, cumpliendo con un estándar establecido para toda la sede principal (documento de políticas de seguridad) y se actualiza la información pertinente de los usuarios. Ver figura 4

| No | Nombre Inicio de Sesión de Usuario | Nombre |
|----|------------------------------------|------------------------------|
| | Administrador | |
| 1 | AdmiCalidad | Karol Eliana Gonzales |
| 2 | JefeSist | Alba lucia Bedoya Benjumea |
| 3 | CoordTalento | Alexandra Arcila |
| 4 | Recepcion | Ana Delia Acevedo Rios |
| 5 | Coordcomercial | Andrea Cardona |
| 6 | Asiscomer | Viviana Andrea Builes |
| 7 | AuxSistemas1 | Carlos A. Huertas |
| 8 | AuxSistemas2 | Mauricio Ramirez |
| 9 | AuxComercial3 | Natalia Giraldo |
| 10 | Auxbodega | Carlos A. Echeverry |
| 11 | Tesoreria | Claudia Patricia Alvarez |
| 12 | SecreGerencia | Claudia Lopez |
| 13 | CoordTecnica | Isabel Cristina Muñoz Molina |
| 14 | AuxContable1 | Isabel Patricia Izquierdo |
| 15 | JefeComunica | Julian Andres Zapata |
| 16 | AuxComercial1 | Yudi Catherine Valencia |
| 17 | gerentegral | Miguel Angel Rendon Moncada |
| 18 | AuxContable2 | Olga Lucia Navarro |
| 19 | CoordCont | Pastora Cañaveral |
| 20 | PractComunica1 | Practicante Comunicación |
| 21 | PractComunica2 | Practicante Comunicación |
| 22 | JefeAdmon | Rosa Cardona |
| 23 | AuxComercial2 | Luisa Fernanda Acosta |
| 24 | PracSistemas | Hernan Mauricio Atuesta |
| 25 | JefeBodega | Carlos Alberto Echeverry |

Figura 3 Cambio Nombres de Usuarios del Directorio Activo

Con el fin de reorganizar la base de datos de los equipos, se obtiene la primera lista de equipos del directorio activo. Ver figura 5

| No | Nombre | Tipo | No | Nombre | Tipo | No | Nombre | Tipo |
|----|-----------------|--------|----|-----------------|--------|----|-----------------|--------|
| 1 | ADMINISTRATIVA | Equipo | 23 | CALIDAD | Equipo | 45 | JEFESISTEMAS | Equipo |
| 2 | ADMONSISTEMAS | Equipo | 24 | CALIDAD1 | Equipo | 46 | JEFETEC | Equipo |
| 3 | APRENDICES | Equipo | 25 | CLIENTE | Equipo | 47 | PORTATILQF | Equipo |
| 4 | APRENDIZ | Equipo | 26 | COMERCIAL | Equipo | 48 | QUIMICABOGO | Equipo |
| 5 | APRENDIZSENA | Equipo | 27 | COMERCIAL3 | Equipo | 49 | QUIMICO1 | Equipo |
| 6 | APRESENASIST | Equipo | 28 | COMUNICACION | Equipo | 50 | QUIMICOS | Equipo |
| 7 | ASISADTVA | Equipo | 29 | COMUNICACION_1 | Equipo | 51 | RECEPCION | Equipo |
| 8 | ASISCOMERCIAL | Equipo | 30 | COMUNICACION2 | Equipo | 52 | RECURSO_HUMANO | Equipo |
| 9 | AUX-FACTURACION | Equipo | 31 | COMUNICACION3 | Equipo | 53 | RRHH | Equipo |
| 10 | AUX-SISTEMAS | Equipo | 32 | COMUNICADORAS | Equipo | 54 | SANTA_MONICA | Equipo |
| 11 | AUX_COMERCIAL | Equipo | 33 | CONTABILIDAD | Equipo | 55 | SECRETGERENCIA | Equipo |
| 12 | AUX_CONTABILIDA | Equipo | 34 | CONTROL_INT | Equipo | 56 | SERVIDOR2006C | Equipo |
| 13 | AUX_SISTEMAS | Equipo | 35 | CODESUR-051A5B | Equipo | 57 | SERVIDORSOPORTE | Equipo |
| 14 | Auxbodega | Equipo | 36 | CODESUR-3GL1LY | Equipo | 58 | SISTEMAS | Equipo |
| 15 | AUXCOMERCIAL | Equipo | 37 | CODESUR-60CMKG | Equipo | 59 | SISTEMAS_PROVI | Equipo |
| 16 | AUXCOMERCIAL1 | Equipo | 38 | CODESUR-D1DC19 | Equipo | 60 | SISTEMAS1 | Equipo |
| 17 | AUXCONTAB | Equipo | 39 | COORCONTABLE | Equipo | 61 | SISTEMASSENA | Equipo |
| 18 | AUXCONTABILIDAD | Equipo | 40 | COORD_COMERCIAL | Equipo | 62 | TESOPROVI | Equipo |
| 19 | AUXILIAR1 | Equipo | 41 | COORDINADORA_TE | Equipo | 63 | TESORERIA | Equipo |
| 20 | AUXILIARSISTEMA | Equipo | 42 | COORDINADORATEC | Equipo | 64 | THE_WOLF | Equipo |
| 21 | AUXSISTEMAS | Equipo | 43 | FACTURACION | Equipo | | | |
| 22 | BELEN | Equipo | 44 | FARMACIAS | Equipo | | | |

Figura 4. Primer Listado de Equipos del Directorio Activo

Se recurre a visitar cada estación de trabajo, y de esta forma definir que equipos conforman la red de Codesuris verificando que se encuentren activos. Ver figura 6

| No | Nombre | Tipo |
|----|-----------------|--------|
| 1 | CALIDAD | Equipo |
| 2 | JEFESISTEMAS | |
| 3 | RRHH | Equipo |
| 4 | RECEPCION | Equipo |
| 5 | COORD_COMERCIAL | Equipo |
| 6 | ASISCOMERCIAL | Equipo |
| 7 | SISTEMAS | Equipo |
| 8 | AUX-FACTURACION | Equipo |
| 9 | Auxbodega | Equipo |
| 10 | TESORERIA | Equipo |
| 11 | SECRETGERENCIA | Equipo |
| 12 | COORDINADORA_TE | Equipo |
| 13 | AUXCONTAB | Equipo |
| 14 | JEFECOMUNICA | Equipo |
| 15 | AUXCOMERCIAL | Equipo |
| 17 | AUX_CONTABILIDA | Equipo |
| 18 | COORCONTABLE | Equipo |
| 19 | COMUNICACION_1 | Equipo |
| 20 | COMUNICACION4 | Equipo |
| 21 | ASISADTVA | Equipo |
| 22 | AUXCOMERCIAL1 | Equipo |
| 23 | JEFESISTEMAS1 | Equipo |
| 24 | JEFEBODEGA | Equipo |

Figura 5 Listado Final de Equipos del Directorio Activo

Tanto a usuarios como equipos se les ubica en grupos de acuerdo a sus privilegios y funciones empleadas en la cooperativa. Ver figura 7 – 8

| Administradores | Grupo de Seguridad- Dominio Local | Los administradores tienen acceso completo y sin restricciones al equipo o dominio | | | |
|---------------------------------|------------------------------------|---|----------------------|--|--|
| Administradores Antiguos | Administradorcalidad | Administradores Actuales | Administrador | | |
| | Alexandra Arcila | | Admins del dominio | | |
| | Andrea Cardona | | Equipos del dominio | | |
| | Angelica Serna | | Alba lucia Bedoya | | |
| | Aux-facturacion | | Aux-sistemas1 | | |
| | Claudia Alvarez | | PractSistemas | | |
| | Isabel Patricia Izquierdo | | | | |
| | Luz Adriana Florez | | | | |
| | Olga lucia Navarro | | | | |
| | Pastora Cañaveral | | | | |
| | Practicante Comunicación 2 | | | | |
| Admins. Del dominio | Grupo de Seguridad - Global | Los miembros de este grupo controlan el dominio por completo, por tal razón se deben agregar los miembros con cautela | | | |
| Antiguos | | | | | |
| | Administradorcalidad | | ASISADTVA | | |
| | Andrea Cardona | | ASISCOMERCIAL | | |
| | Angelica Serna | | AUX_CONTABILIDAD | | |
| | Aux Facturacion | | AUXBODEGA | | |
| | Claudia Alvarez | | AUXCONTAB | | |
| | Invitado | | AUXILIAR FACTURACION | | |
| | Isabel Cristina Muñoz | | COMUNICACIÓN | | |
| | Isabel Patricia Izquierdo | | COMUNICACIÓN_1 | | |
| | Luz Adriana Florez | | COORCONTABLE | | |
| | Olga lucia Navarro | | JEFESISTEMAS | | |
| | Pastora Cañaveral | | QUIMICOS | | |
| | | | RECEPCION | | |
| | | | SECRETGERENCIA | | |
| | | | TESORERIA | | |
| Actuales | | | | | |
| | Administrador | | | | |
| Equipos del Dominio | Grupo de seguridad - Global | Este grupo contiene todos los servidores y estaciones de trabajo unidos al dominio | | | |
| Antiguos | | | | | |
| | Administradorcalidad | | | | |
| | Andrea Cardona | | | | |
| | Auxiliar Facturacion | | | | |
| | Claudia Alvarez | | | | |
| | Invitado | | | | |
| | Isabel Patricia Izquierdo | | | | |
| | Julian Andres Zapata | | | | |
| | Luz Adriana Florez | | | | |
| | Olga Lucia Navarro | | | | |
| | Pastora Cañaveral | | | | |
| | Practicante Comunicación 2 | | | | |
| Actuales | | | | | |
| | Administrador | | QUIMICOS | | |
| | ASISADTVA | | RECEPCION | | |
| | ASISCOMERCIAL | | SECRETGERENCIA | | |
| | AUX_CONTABILIDA | | TESORERIA | | |
| | AUXBODEGA | | GERENCIA | | |
| | AUXCOMERCIAL | | SISTEMAS | | |
| | AUXCOMERCIAL1 | | RRHH | | |
| | AUXCONTAB | | HP25975159401 | | |
| | AUX-FACTURACION | | ISSALTD1 | | |
| | CALIDAD | | JEFEBODEGA | | |
| | COMUNICACIÓN | | JEFESISTEMAS | | |
| | COMUNICACIÓN_1 | | JEFESISTEMAS1 | | |
| | COMUNICACION4 | | COORDINADORA_TE | | |
| | COORCONTABLE | | | | |
| | COOR_COMERCIAL | | | | |

Figura 6 Asignación de Grupos del Directorio Activo



| Usuarios del Dominio | Grpo de seguridad - Global | Todos las cuentas que se creen en el demonio son miembros de este grupo | | | |
|----------------------|--|--|------------------------------|--|--|
| Antiguos | | | | | |
| |  COMUNICACIÓN | | | | |
| | Krbtgt | | | | |
| | Invitado | | | | |
| Actuales | Administrador | | Isabel Cristina Muñoz Molina | | |
| | Administradorcalidad | | Isabel Patricia Izquierdo | | |
| | Alba lucia Bedoya Benjumea | | Julian Andres Zapata | | |
| | Alexandra Arcila | | Luz Adriana Florez | | |
| | Ana Delia Acevedo Rios | | Miguel Angel Rendon Moncada | | |
| | Andrea Cardona | | Olga Lucia Navarro | | |
| | Angelica Serna | | Pastora Cañaveral | | |
| | Aux-sistemas | | Practicante Comunicación 1 | | |
| | Auxiliar Facturacion | | Practicante Comunicación 2 | | |
| | Carlos A. Echeverry | | Quimicos Coodesuris | | |
| | Carlos Alberto Echeverry | | Rosa Cardona | | |
| | Claudia Patricia Alvarez | | Victoria Eugenia Castaño | | |
| | Claudia Lopez | | Viviana Andrea Builes | | |
| | Hernan Mauricio Atuesta | | | | |
| Usuarios | Grupo de Seguridad - Dominio Local | Los usuarios no pueden hacer cambios accidentales o intencionados en el sistema. Pueden ejecutar aplicaciones certificadas pero no la mayoría de las heredadas | | | |
| Antiguos | | | | | |
| | Administradorcalidad | | | | |
| | Andrea Cardona | | | | |
| | Claudia alvarez | | | | |
| |  COMUNICACIÓN | | | | |
| | Isabel Patricia Izquierdo | | | | |
| | Luz Adriana Florez | | | | |
| | Olga lucia Navarro | | | | |
| | Pastora Cañaveral | | | | |
| Actuales | | | | | |
| | Admins. Del dominio | | | | |
| | INTERACTIVE | | | | |
| | Invitado | | | | |
| | Usuarios autenticados | | | | |
| | Usuarios del dominio | | | | |

Figura 7 Asignación de Grupos del Directorio Activo

6.1.2 Acciones Tomadas en la administración de archivos compartidos

- ✓ Por seguridad se inhabilita la acción de compartir algunos discos y carpetas del servidor
- ✓ Se redistribuye la forma de compartir archivos en el espacio designado por la administración de sistemas. Ver figura 9 -10

Fecha: Marzo 28 de 2009

Z: /...

| |
|------------------|
| Alba |
| Alexa |
| Carlos Htas |
| Claudia Lopez |
| Comercial |
| Diana |
| Viviana |
| Auxcomercialvivi |
| Comunicación |
| Andrea |
| Claudia |
| Julianita |
| Gerencia |
| Karol |
| Pastora |
| Rosa |
| Rubio |
| Angela |
| Alejo |
| Ana Bienestar |
| ELIANA |

Z: /Alba/...

| |
|------------------|
| \Jhon |
| \Karina |
| \Leonardo |
| \Nicolas |
| \Paty |
| \Sebastian |
| \Secretaria |
| \Alba |
| \Sistemas |
| \Criss |
| \Claudia Alvarez |
| \Viviana Builes |
| \Andres Quimico |
| \Olga |

Espacio Total: 18.5 GB

Figura 8 Estado Anterior de la Unidad de Red Z

| |
|-------------------|
| \\Jhon |
| \\Karina |
| \\Leonardo |
| \\Nicolas |
| \\Paty |
| \\Sebastian |
| \\Secretaria |
| \\Alba |
| \\Sistemas |
| \\Criss |
| \\Claudia Alvarez |
| \\Viviana Builes |
| \\Andres Quimico |
| \\Olga |

Fecha: Mayo 15 de 2009

Espacio Total: 8.89 GB

Figura 9 Estado Actual de la Unidad de Red Z

- ✓ Se depura la información y además se crea una tarea mensual de depuración para el espacio de compartir archivos de los usuarios.

6.1.3 Acciones Tomadas en cuanto al mantenimiento del servidor

- ✓ Se procedió a depurar los archivos temporales de internet, historial, cookies y programas ejecutados y se consiguió aumento de espacio.
- ✓ Se re direccionan los archivos temporales que almacenaba el programa Winzip durante las copias de seguridad ya que por falta de espacio en disco C: presentaba errores al realizar la copia.
- ✓ Se depura la Información del disco H: y así se consiguió más espacio libre.

- ✓ Se realiza un Scandisk a todos los discos del servidor, con el fin de corregir errores y mejorar el acceso al sistema.
- ✓ Se hace el proceso de limpiar entradas del registro antiguas.
- ✓ Se instaló una herramienta de uso libre (Freeware) en el servidor, para realizar todo tipo de limpieza del disco, registro, archivos temporales y otras utilidades que ayudan a mantener el buen funcionamiento de las operaciones.
- ✓ Se realiza una desfragmentación de todos los volúmenes contenidos en los discos del servidor

Desfragmentación de Discos

| | C: | F: | H: | K: |
|---|--------------|--------------|--------------|--------------|
| Tamaño del Volumen | 29.32 GB | 107.43 GB | 136.73 GB | 107.43 GB |
| Tamaño del Cluster | 512 bytes | 4 K | 4 K | 4 K |
| Espacio Utilizado | 24.19 GB | 41.31 GB | 49.81 GB | 56.70 GB |
| Espacio Libre | 5.13 GB | 66.12 GB | 86.92 GB | 50.71 GB |
| Porcentaje de Espacio disponible | 17% | 61% | 63% | 47% |
| Fragmentación del volumen | | | | |
| Fragmentación total | 27% | 0% | 16% | 0% |
| Fragmentación del archivo | 55% | 0% | 41% | 0% |
| Fragmentación del espacio disponible | 0% | 0% | 3% | 0% |
| Fragmentación del archivo | | | | |
| Cantidad de archivos | 69.939 | 97.725 | 11.740 | 31.319 |
| Tamaño promedio de archivo | 732 KB | 451 KB | 227 KB | 2 MB |
| Cantidad de archivos fragmentados | 5.609 | 0 | 2.185 | 0 |
| Cantidad de fragmentos en exceso | 166.735 | 0 | 85.692 | 0 |

| | | | | |
|--|-------|---------|---------|---------|
| Promedio de fragmentos por archivo | 3.60 | 0.99 | 1.80 | 0,99 |
| Fragmentación del archivo de paginación | | | | |
| Tamaño del archivo de paginación | 2 GB | 0 bytes | 0 bytes | 0 bytes |
| Cantidad de fragmentos | 5 | 0 | 0 | 0 |
| Fragmentación de carpetas | | | | |
| Cantidad de carpetas | 5006 | 1774 | 136 | 439 |
| Carpetas fragmentadas | 156 | 12 | 11 | 1 |
| Exceso de fragmentos de carpetas | 2.473 | 96 | 0 | 0 |

Tabla 2 Resumen Proceso de desfragmentación

6.1.4 Acciones tomadas en el plan de copia de seguridad

- ✓ Se reasignan nombres a las carpetas de copia de seguridad para una mejor identificación.
- ✓ Se ordenan carpetas de copias de seguridad de acuerdo al área de trabajo y se eliminaron carpetas obsoletas.
- ✓ Se asignan permisos especiales a cada usuario en su carpeta de copia.
- ✓ Se restringe el permiso de cada usuario a las copias de seguridad globales, para tener acceso debe pertenecer al grupo de administradores, encabezados por los integrantes del área de sistemas.
- ✓ Se realizan visitas a cada usuario para que depuren información la cual no requiere copia de seguridad.

OBSERVACIÓN INICIAL

| Nombre carpeta | Usuario | Tamaño |
|----------------------------|---------------------------|---------|
| Administrador SGC | Karol Eliana Gonzales | 1.82 GB |
| Aprendiz Sena | Shirley | 206 KB |
| Aprendiz Sena Comercial | | 36.2 MB |
| Asistente Administrativa | Rosa Cardona | 477 MB |
| Asistente Comercial | Viviana Builes | 321 MB |
| Auxiliar Facturación | Natalia Giraldo | 19.6 MB |
| Auxiliar de Contabilidad 1 | Isabel Patricia Izquierdo | 412 MB |
| Auxiliar de Contabilidad 2 | Olga Lucia Navarro | 179 MB |
| Auxiliar de Sistemas | Carlos Alberto Huertas | 902 MB |
| Bodega | Carlos Alberto Echeverry | 54.5 MB |
| Comunicación | Julián Zapata | 18.6 GB |
| Coordinador Técnico | Isabel Cristina Muñoz | 24 MB |
| Coordinadora Comercial | Andrea Cardona | 14.4 GB |
| Coordinadora Contable | Pastora Cañaveral | 979 MB |
| Gerencia | Miguel Ángel Rendón | 1.19 GB |
| Jefe Técnico | Andrés | 2.35 GB |
| Proyectos | Alexandra Arcila | 3.29 GB |
| Recepción | Ana delia Ríos | 845 KB |
| Sistemas | Alba lucia Bedoya | 4.36 GB |
| Tesorería | Claudia Álvarez | 985 MB |

| | |
|---------------------|----------------|
| Tamaño Total | 50.4 GB |
|---------------------|----------------|

Tabla 3 Primer Listado Copia de Seguridad Usuarios

SEGUIMIENTO

| Nombre carpeta | Usuario | Tamaño |
|--------------------------|-----------------------|---------|
| Administrador SGC | Karol Eliana Gonzales | 1.66 GB |
| Asistente Administrativa | Rosa Cardona | 272 MB |
| Asistente Comercial | Viviana Builes | 335 MB |
| Auxiliar Facturación | Natalia Giraldo | 19.6 MB |

| | | |
|----------------------------|---------------------------|---------|
| Auxiliar de Contabilidad 1 | Isabel Patricia Izquierdo | 414 MB |
| Auxiliar de Contabilidad 2 | Olga Lucia Navarro | 183 MB |
| Auxiliar de Sistemas | Carlos Alberto Huertas | 245 MB |
| Bodega | Carlos Alberto Echeverry | 54.5 MB |
| Comunicación | Julián Zapata | 9.85 GB |
| Coordinador Técnico | Isabel Cristina Muñoz | 24 MB |
| Coordinadora Comercial | Andrea Cardona | 14.4 GB |
| Coordinadora Contable | Pastora Cañaveral | 1 GB |
| Gerencia | Miguel Ángel Rendón | 1.19 GB |
| Jefe Técnico | Andrés | 2.35 GB |
| Talento Humano | Alexandra Arcila | 2.86 GB |
| Recepción | Ana delia Ríos | 845 KB |
| Sistemas | Alba lucia Bedoya | 4.32 GB |
| Tesorería | Claudia Álvarez | 993 MB |

| | |
|---------------------|----------------|
| Tamaño Total | 40.2 GB |
|---------------------|----------------|

Tabla 4 Segundo listado Copia de Seguridad Usuarios

A LA FECHA

| Nombre carpeta | Usuario | Tamaño |
|----------------------------|---------------------------|---------------|
| Administrador SGC | Karol Eliana Gonzales | 401 MB |
| Asistente Administrativa | Rosa Cardona | 275 MB |
| Asistente Comercial | Viviana Builes | 343 MB |
| Auxiliar Facturación | Natalia Giraldo | 19.9 MB |
| Auxiliar de Contabilidad 1 | Isabel Patricia Izquierdo | 420 MB |
| Auxiliar de Contabilidad 2 | Olga Lucia Navarro | 190 MB |
| Bodega | Carlos Alberto Echeverry | 57.1 MB |
| Comunicación | Julián Zapata | 9.85 GB |
| Coordinador Técnico | Isabel Cristina Muñoz | 24.1 MB |
| Coordinadora Comercial | Andrea Cardona | 0 KB |
| Coordinadora Contable | Pastora Cañaveral | 1.01 GB |
| Gerencia | Miguel Ángel Rendón | 706 MB |
| Jefe Técnico | Andrés | 2.35 GB |

| | | |
|-------------------------|-------------------|---------|
| Talento Humano | Alexandra Arcila | 2.86 GB |
| Recepción | Ana delia Ríos | 856 KB |
| Administradora Sistemas | Alba lucia Bedoya | 308 MB |
| Tesorería | Claudia Álvarez | 0.98 GB |

| | |
|---------------------|----------------|
| Tamaño Total | 17.4 GB |
|---------------------|----------------|

Tabla 5 Estado Actual Copias de Seguridad Usuarios

6.2 RED DE COODESURIS

6.2.1 Acciones Tomadas en las estaciones de trabajo

- ✓ Se ejecuta la actualización del service pack de Windows mediante un archivo que contiene la versión numero tres.
- ✓ Se verifican los seriales con los que fueron instaladas las copias del office,
- ✓ Se instala por medio del Cd original, la copia de Office 2007 en las máquinas que aún no lo tenían.
- ✓ Se procede a reconfigurar los servicios de inicio de las estaciones de trabajo
- ✓ Se eliminan los elementos de inicio en cada esta de trabajo que ocupaba espacio innecesario en la memoria.
- ✓ Se activaron mensajes de alerta y de aviso en las maquinas cliente para difundir mensajes de manera más rápida proveniente del área de sistemas.

- ✓ Se realizan visitas para recolección de información y programación de actualizaciones de Office 2003 a Office 2007. Ver Figura 11


| Office 2003 | Office 2007 | Programa de Visitas para la Instalación de Office 2007 | | | | | |  |
|-------------|-------------|--|------------------------------|---------------|------------|-------------------|-------------|---|
| | | Area | Nombre | Fecha (d/m/a) | Hora | Firma Funcionario | Responsable | |
| | | Administradorcalidad | Karol Eliana | 26/05/2009 | 09:50 a.m. | | | |
| | | Sistemas | Alba Lucia Bedoya Benjumea | | | | | |
| | | Practicante Sistemas | Hernan Mauricio Atuesta | | | | | |
| | | Aux-sistemas | Aux-sistemas | | | | | |
| | | coordinadoraRH | Alexandra Arcila | 22/05/2009 | 09:00 a.m. | | | |
| | | administrativa | Rosa Cardona | | | | | |
| | | repcion | Ana Delia Acevedo Rios | | | | | |
| | | comercial | Andrea Cardona | | | | | |
| | | asíscomercial | Viviana Builes | | | | | |
| | | Aux_comercial | Yudi Catherine | 27/05/2009 | 11:00 a.m. | | | |
| | | auxcomercia1 | Luisa Fernanda | 24/05/2009 | 08:00 a.m. | | | |
| | | aux-facturacion | Ntalia Giraldo | | | | | |
| | | Auxbodega | Carlos A. Echeverry | N/A | N/A | N/A | N/A | |
| | | tesoreria | Claudia Patricia Alvarez | 26/05/2009 | 08:00 a.m. | | | |
| | | secretgerencia | Claudia Lopez | 26/05/2009 | 09:30 a.m. | | | |
| | | gerentegral | Miguel Angel Rendon Moncada | | | | | |
| | | coordinadoraT | Isabel Cristina Muñoz Molina | | | | | |
| | | comunicación | Julian Andres Zapata | | | | | |
| | | comunicacio1 | Practicante Comunicación | 26/05/2009 | 02:00 p.m. | | | |
| | | comunicacion2 | Practicante Comunicación | 26/05/2009 | 11:00 a.m. | | | |
| | | AUX_CONTABILIDAD | Olga Lucia Navarro | 26/05/2009 | 10:30 a.m. | | | |
| | | Pastora_C | Pastora Cañaveral | 26/05/2009 | 08:00 a.m. | | | |
| | | AUXILIAR | Isabel Patricia Izquierdo | 26/05/2009 | 08:00 a.m. | | | |
| | | Psicologia | Milena | N/A | N/A | N/A | N/A | |
| | | Practicante Sena | Angela Becerra | N/A | N/A | N/A | N/A | |
| | | AuxBodega | Carlos A. Echeverry | N/A | N/A | N/A | N/A | |

Figura 10 Relación de Visitas para Actualizar Office 2007

- ✓ Se realizan visitas para recolección de información y programando la instalación del Service Pack 3. Ver Figura 12


| service pack 1 | service pack 2 | service pack 3 | Programa para la Ejecución de Actualizaciones en Service Pack Windows XP | | | | |  |
|----------------|----------------|----------------|--|------------------------------|---------------|------------|-------------------|---|
| | | | Area | Nombre | Fecha (d/m/a) | Hora | Firma Funcionario | |
| | | | Administradorcalidad | Karol Eliana | 22/04/2009 | 08:00 a.m. | | Alejandro |
| | | | Sistemas | Alba lucia Bedoya Benjumea | 23/04/2009 | 09:00 a.m. | | Mauricio |
| | | | Aux-sistemas | Aux-sistemas | 23/04/2009 | 09:30 a.m. | | Mauricio |
| | | | Practicante Sistemas | Hernan Mauricio Atuesta | 24/04/2009 | 10:30 a.m. | | Mauricio |
| | | | coordinadoraRH | Alexandra Arcila | 23/04/2009 | 10:00 a.m. | | Mauricio |
| | | | administrativa | Rosa Cardona | 22/04/2009 | 10:00 a.m. | | Mauricio |
| | | | repcion | Ana Delia Acevedo Rios | 22/04/2009 | 07:00 a.m. | | Alejandro |
| | | | Psicologia | Milena | N/A | N/A | | N/A |
| | | | Practicante Sena | Angela Becerra | N/A | N/A | | N/A |
| | | | comercial | Andrea Cardona | 22/04/2009 | 07:00 a.m. | | Mauricio |
| | | | asiscomercial | Viviana Builes | 22/04/2009 | 12:30 p.m. | | Alejandro |
| | | | Aux_comercial | Yudi Catherine | 22/04/2009 | 09:00 a.m. | | Mauricio |
| | | | auxcomercia1 | Luisa Fernanda | 22/04/2009 | 07:30 a.m. | | Mauricio |
| | | | aux-facturacion | Natalia Giraldo | 22/04/2009 | 09:00 a.m. | | Alejandro |
| | | | JefeBodega | Carlos A. Echeverry | 22/04/2009 | 08:00 a.m. | | Mauricio |
| | | | AuxBodega | Carlos A. Echeverry | N/A | N/A | | N/A |
| | | | tesoreria | Claudia Patricia Alvarez | 22/04/2009 | 10:30 a.m. | | Mauricio |
| | | | secretgerencia | Claudia Lopez | 22/04/2009 | 08:30 a.m. | | Alejandro |
| | | | gerentegral | Miguel Angel Rendon Moncada | 25/04/2009 | 09:00 a.m. | | Mauricio |
| | | | coordinadoraT | Isabel Cristina Muñoz Molina | 22/04/2009 | 09:30 a.m. | | Mauricio |
| | | | comunicación | Julian Andres Zapata | 22/04/2009 | 11:00 a.m. | | Mauricio |
| | | | comunicacio1 | Practicante Comunicación | 22/04/2009 | 11:30 p.m. | | Mauricio |
| | | | comunicacion2 | Practicante Comunicación | 22/04/2009 | 12:00 p.m. | | Mauricio |
| | | | AUX_CONTABILIDAD | Olga Lucia Navarro | 22/04/2009 | 02:00 p.m. | | Mauricio |
| | | | Pastora_C | Pastora Cañaveral | 23/04/2009 | 01:00 p.m. | | Mauricio |
| | | | AUXILIAR | Isabel Patricia Izquierdo | 22/04/2009 | 02:00 p.m. | | Mauricio |

Figura 11 Relación de Visitas Actualización Service Pack

6.2.2 Acciones Tomadas kaspersky

- ✓ Se instala el agente de administración en algunos de los equipos
- ✓ Se incluyen los equipos que faltaban a la base de datos de la consola de administración
- ✓ Se programa una tarea de escaneo automático en modo grupal cada miércoles después de la jornada laboral.

- ✓ Se instaure como rutina un seguimiento diario a la consola de administración, en busca de inconvenientes presentados.
- ✓ Se configuran las actualizaciones con el fin que se activen cada vez que el equipo sea encendido
- ✓ Se cambia la ruta de los archivos temporales debido al poco espacio en disco y se redujo su tiempo de almacenamiento.
- ✓ Se extraen estadísticas acerca de los virus más frecuentes y su ruta de almacenamiento, teniendo en cuenta los equipos donde se presentaban.
- ✓ Se realiza un seguimiento a los mensajes de error presentados por el antivirus y se les dio solución, según el caso presentado.
- ✓ Se depura la base de datos en relación a mensajes obsoletos y equipos fuera de uso
- ✓ Se le hace un seguimiento a los archivos en cuarentena

6.2.3 Acciones Tomadas Wireshark

- ✓ Se instala el analizador Wireshark en el servidor de la cooperativa con fines administrativos, sacando provecho que es una herramienta bajo licenciamiento GPL.
- ✓ Se ejecuta el programa en busca de novedades en el tráfico de la red.
- ✓ Se le da solución a los problemas encontrados.

- ✓ Actualmente se le hace seguimiento a la operación de la red a través de la herramienta.

6.2.4 Acciones Tomadas en las Políticas de Seguridad

- ✓ Se crea el documento de políticas de seguridad informática, cuyo objetivo es establecer un estándar para la creación, el uso, gestión y control de contraseñas robustas, la protección y la frecuencia de cambio de las mismas dentro de los sistemas y equipos de la Cooperativa a fin de evitar o reducir los incidentes de seguridad.
- ✓ Se diseña un formato donde se consigna el ingreso a la cooperativa de nuevos funcionarios con el objetivo de brindar información pertinente al administrador de sistemas y este pueda aplicar las políticas de seguridad establecidas. Ver figura 13

| | | | |
|--|----------------------------------|------------------------------|--|
| COODESURIS | AVISO DE INGRESO DE FUNCIONARIOS | | COD: FOXX VERSIÓN 1 |
| | DESCRIPCION DEL FUNCIONARIO | | |
| NOMBRE | | CARGO | TIEMPO CONTRATO |
| | | | Menor a 1 Mes Menor a 6 Meses Indefinido |
| SOLO DILIGENCIE HASTA ACA Y ENTREGUE AL AREA DE SISTEMAS | | | |
| Equipo a utilizar: | | | |
| Asignar nuevo _____ Compartir con _____ | | | |
| Programas a manejar: | | | |
| ALFA _____ NOVASOFT _____ OFFICE _____ OUTLOOK _____ | | | |
| Carpetas a crear: | | | |
| Unidad Z _____ Unidad S _____ Copia de seguridad _____ | | | |
| Privilegios otorgados: | | | |
| | | | |
| | | | |
| | | | |
| Tipo de usuario: | | | |
| Administrador _____ Usuario avanzado _____ Usuario Restringido _____ | | | |
| FECHA IMPLEMENTACION: | | RESPONSABLE AREA DE SISTEMAS | |
| FIRMA DE ACEPTACIÓN DEL USUARIO: | | | |

Figura 12 Formato Ingreso Funcionarios

- ✓ Se diseña un formato donde se consigna el retiro de los funcionarios de la cooperativa con el objetivo de brindar información pertinente al administrador de sistemas y este pueda aplicar las políticas de seguridad establecidas. Ver figura 14

| | | | | |
|--|---------------------------------|------------------------------|-----------|------------------------|
| COODESURIS | AVISO DE RETIRO DE FUNCIONARIOS | | COD: FOXX | |
| | | | VERSIÓN 1 | |
| | | | | |
| DESCRIPCION DEL DOCUMENTO | | | | |
| NOMBRE | | CARGO | | TIPO DE RETIRO |
| | | | | Temporal Definitivo |
| | | | | |
| DESCRIPCION DEL RETIRO TEMPORAL | | | | |
| Causa: | | | | |
| VACACIONES ____ INCAPACIDAD ____ SUSPENSIÓN ____ RETIRO DEFINITIVO ____ | | | | |
| Tiempo: | | | | |
| 8 días a 15 días ____ 15 días a 30 días ____ Mas de 30 días ____ | | | | |
| INACTIVACIÓN DEFINITIVA? SI ____ NO ____ | | | | |
| FECHA IMPLEMENTACION: | | RESPONSABLE AREA DE SISTEMAS | | |

Figura 13 Formato Salida Usuarios

6.2.5 Acciones Tomadas en el Firewall

- ✓ Se abren puertos para dar permisos a algunos usuarios y se deja registro de los cambios realizados.
- ✓ Se ingresan direcciones Mac de los usuarios que se encuentran habilitados para realizar descargas.
- ✓ Se registran eventos de ataques hechos a la red.

- ✓ Se restringe el acceso a páginas y así mismo se permite el acceso a otras.

6.3 MEJORAS TÉCNICAS Y TECNOLÓGICAS EN LA OPERACIÓN

6.3.1 Acciones Tomadas en la Mejora técnica servidor

En un principio se pensó en actualizar los componentes del servidor, pero después de realizar la respectiva valoración y consultar con los proveedores de tecnología, se tomó la decisión que convenía más adquirir un servidor nuevo que invertir dinero en el que ya se tenía.

- ✓ Se valoraron tecnologías y sus beneficios, estudiando cada opción disponible y aplicable encontrada en el mercado.
- ✓ Se observó la necesidad que tenía la cooperativa en cuanto a servidor y se evaluaron los requerimientos mínimos que se debían cumplir para la compra.
- ✓ Se solicitaron cotizaciones a diferentes proveedores que cumplieran con las características establecidas.
- ✓ Se tomaron en cuenta las recomendaciones de adquisición que ofrecían los proveedores

6.3.2 Acciones Tomadas en la conexión remota

Después de analizar cada una de las propuestas de conexión se optó por la opción de Logme in y se proseguí con las siguientes actividades.

- ✓ Se crea una cuenta global de administrador en el sitio web de logme in

- ✓ Se configura como prueba piloto el logme in Free en todas las farmacias.
- ✓ Se crean contraseñas para cada una de las cuentas

6.3.3 Acciones Tomadas en la actualización de la página web

- ✓ Se reasignaron espacios en las cuentas de correo con el fin de buscar mayor espacio libre y realizar otro tipo de actividades.
- ✓ Se procedió a adquirir cotizaciones acerca de un Hosting con mayor espacio conservando el dominio de Coodesuris.com
- ✓ Se evaluó en conjunto con la administración de sistemas el hecho de implementar sobre la página web unas cuentas de FTP con el fin de compartir archivos con las farmacias.

CONCLUSIONES

La práctica profesional de ingeniería de sistemas y telecomunicaciones de la Universidad Católica es una oportunidad donde el estudiante puede aplicar muchos de los conceptos adquiridos durante su formación, donde se está preparado para iniciar una nueva ganancia de conocimientos y experiencias que sólo se logran con unas bases bien fundadas.

Implementar mejoras técnicas a una entidad, es un tema bastante delicado donde no se pueden dejar escapar factores de ningún tipo, ya que cualquier mala decisión por pequeña que sea, puede causar grandes problemas en la operación y pérdidas de información.

Según encuestas realizadas por IBM y Cisco la mayoría de las empresas en Latinoamérica no cuentan con una persona dedicada al tema de seguridad informática. La exposición de estas empresas a cualquier ataque es demasiado grande, por tal razón es conveniente empezar a considerar mayor inversión en tiempo y dinero frente a este tema.

Después de realizar mi práctica profesional en Coodesuris y conocer un poco del método de operación de esta empresa y a su vez descubrir la falta de administración de su red, la carencia de planes de contingencias y seguridad, se puede concluir que este es un tema al que muchas entidades le restan importancia, afortunadamente muy pocas veces es tarde para corregir las fallas de este tipo, éstas aún pueden ser intervenidas por medio de procesos de mejoramiento que puedan afianzar las actividades llevadas a cabo por la entidad o institución.

En este presente podemos afirmar que el uso herramientas tecnológicas aumentan en las empresas, lastimosamente en muchas de ellas estas herramientas son subutilizadas y no pueden cumplir con su propósito final por falta de conocimiento de los encargados de su administración.

RECOMENDACIONES

Directorio Activo

- ✓ La persona encargada de la administración del directorio activo debe realizar mantenimientos periódicos a sus bases de datos.
- ✓ Debe existir una permanente comunicación entre la coordinadora de talento humano y la persona encargada del directorio activo, para dar a conocer el personal que ingresa nuevo o el que entrega su puesto.
- ✓ Se deben realizar cambios periódicos a los nombres de inicio de sesión y las contraseñas de los usuarios cumpliendo con las directivas establecidas de seguridad.
- ✓ Cualquier ingreso de un usuario o estación de trabajo a la cooperativa debe de ser analizado de acuerdo a su labor a desempeñar y así asignarle su grupo correspondiente a sus privilegios de usuario.
- ✓ Después de la configuración previa de un equipo se debe considerar si cuenta con las licencias de acceso (CAL) para unirse al dominio, siendo la administración de sistemas el área encargada de solucionar esta parte legal.

Archivos Compartidos

- ✓ El administrador debe velar por que se conserve la estructura de los espacios comunes para compartir archivos.

- ✓ Se debe realizar la depuración periódica pertinente de los espacios para compartir archivos.
- ✓ Crear y mantener la cultura a los funcionarios de que suban sus archivos a compartir de forma temporal.

Mantenimiento Servidor

- ✓ El administrador regularmente debe realizar mantenimiento a los discos del servidor.
 - Realizar el proceso de desfragmentación
 - Escanear los discos
 - Depurar la información.
 - Borrar temporales
 - Borrar entradas de registro antiguas
- ✓ Para evitar tener archivos obsoletos o inútiles dentro del equipo es importante realizar un cleanup del disco al menos una vez por semana.
- ✓ Determinar problemáticas asociadas a intrusiones, ataques Dos, etc.

Plan de Copias de Seguridad

- ✓ Vigilar regularmente si las copias de seguridad se hicieron, si se presenta el caso contrario investigar cual fue el motivo, o pasar a revisar los informes del porque el fallo de su realización.
- ✓ Mantener el control y permisos a las copias de seguridad globales y de usuarios

- ✓ Tratar en lo posible de no compartir la carpeta de copias de seguridad
- ✓ Implementar alguna solución física para las copias de seguridad en tiempo Real.

Estaciones de Trabajo

- ✓ Periódicamente a los equipos de la cooperativa se les debe revisar que tengan las últimas actualizaciones de software.
- ✓ Es necesario que el administrador de sistemas siempre esté al tanto de que los equipos que llegan nuevos se les instalen las últimas actualizaciones.
- ✓ El administrador debe estar atento a cualquier actualización de interés para la cooperativa que salga al mercado, para su respectiva adquisición y así reducir el grado de vulnerabilidad.
- ✓ Incluir en el mantenimiento preventivo el control y vigilancia de las acciones anteriormente tomadas.
- ✓ Vigilar que los equipos nuevos que se instalen en la cooperativa se encuentren configurados como debe ser.
- ✓ Velar por que las configuraciones cambiadas no sean alteradas por ninguna otra persona ajena al área de sistemas

Antivirus Kaspersky

Son funciones del administrador y se recomienda crear un cronograma de actividades.

- Examinar los informes de los resultados de funcionamiento de las aplicaciones en los equipos cliente.
- Leer en el buzón de correo del administrador las alertas enviadas desde los equipos cliente y el servidor de administración.
- Actualización puntual de la base antivirus en los equipos cliente y módulos de software de aplicaciones instaladas en los equipos cliente.
- Vigilar el espacio disponible en el servidor para almacenar los envíos desde los clientes, así como la memoria libre disponible en el servidor para procesar los datos enviados.
- Agregar a la red lógica los nuevos equipos detectados en la red local, e instale en ellos las aplicaciones antivirus necesarios, de forma regular.
- Hacer copias de seguridad periódicas de los datos del sistema de administración.

Administración Wireshark

- ✓ La persona encargada de la administración de la red debe hacer uso de la herramienta como mínimo 2 veces por semana evitando al máximo que se pase por inadvertido cualquier infiltración que pueda conducir a serias consecuencias.
- ✓ Cualquier novedad encontrada se debe corregir en el menor tiempo posible y se le debe hacer su respectivo seguimiento.

Firewall

- ✓ Cualquier acción tomada debe quedar registrada en un historial de administración.
- ✓ La persona que se encuentre al frente de la administración del firewall debe estar en capacidad de instalar este software y configurarlo en el momento en que sea necesario.
- ✓ Se deben programar cambios de claves y acceso a la configuración del firewall
- ✓ Ninguna persona ajena a la administración de sistemas, puede entrar a hacer modificaciones a la configuración del Firewall
- ✓ Se les debe hacer seguimiento a los equipos que se encuentran habilitados para realizar descargas.
- ✓ No habilitar el acceso de descargas a cualquier usuario.
- ✓ Se debe mantener las listas negras y blancas actualizadas con sus respectivas direcciones

Políticas de Seguridad Informática

- ✓ Periódicamente se debe actualizar el manual de políticas de seguridad de la empresa, mejorando su contenido según las novedades presentadas desde su última versión.
- ✓ Se debe realizar un seguimiento a las políticas establecidas vigilando su correcto funcionamiento.
- ✓ El encargado de las políticas de seguridad debe asegurar que el funcionario cumpla con sus responsabilidades asignadas.
- ✓ El administrador debe ser la única persona que asigne privilegios de usuarios de acuerdo al grupo que el usuario ha sido asignado.

Mejora Técnica Servidor

- ✓ Adquirir un servidor que cubra mejoras y planes de contingencia en cuanto a:
 - Discos Duros
 - Fuente de poder
 - Memoria RAM
- ✓ Trabajar con tecnologías actuales tanto en hardware como en software.
- ✓ Cualquier adquisición tecnológica que se realice debe contar con un proceso cuidadoso de implementación.

- ✓ Se debe realizar una configuración de seguridad y rendimiento que se acople a la cooperativa sacando el mayor provecho de la adquisición realizada.
- ✓ Es vital rescatar que el propósito de la adquisición del servidor es crear planes de contingencia a fallos técnicos, con el fin de que la cooperativa no detenga sus actividades y sean perdidas las producidas.

Conexión y Acceso remoto

- ✓ Realizar un seguimiento a esta implementación teniendo en cuenta las ventajas y desventajas con el fin de garantizar el buen servicio.
- ✓ No revelar, ni escribir las claves de acceso en ningún documento.
- ✓ Cambiar periódicamente las claves de acceso a los equipos de cada farmacia o el acceso a la cuenta global ya que es la única herramienta de seguridad que se tiene a la mano y con la que se cuenta en este tipo de implementaciones.

Actualización Página Web

- ✓ Adquirir un plan de Hosting de 5 GB de espacio
- ✓ Crear y Administrar las cuentas de correo por medio de la aplicación Google Apps, que brinda 7 GB por cada cuenta, además de brindar estabilidad y seguridad.
- ✓ Configurar el Servicio de FTP para transferencia de archivo de la sede principal de la cooperativa a cada una de las farmacias o viceversa.

COMPLEMENTARIOS

Políticas de Seguridad Informática

Responsabilidades del usuario

- a. Si algún usuario requiere una contraseña, se debe referir a este documento y ponerse en contacto con la Administración de sistemas de la Cooperativa.
- b. No revelar a terceros su nombre de usuario y combinación de contraseña, o de acceso.
- c. No utilizar las funciones de recordar las contraseñas que poseen algunas aplicaciones (por ejemplo, OutLook, Netscape, Messenger, etc.)
- d. No escribir las contraseñas en ningún documento que se encuentre en su lugar de trabajo.
- e. No almacenar las contraseñas en ninguna computadora (incluyendo agendas personales o dispositivos similares) sin cifrar la información.
- f. No enviar la contraseña vía mail.
- g. No intentar acceder a los ordenadores o servicios de computación en los cuales no se le está permitido.
- h. No utilizar la misma contraseña para los usos personales ni para los formularios electrónicos.
- i. No revelar una contraseña dentro de cuestionarios o formas de seguridad, ni en ningún documento similar.

- j. No utilizar la misma contraseña para más de un sistema.
- k. En caso de olvido de la contraseña, deberá gestionar el cambio de la misma con su responsable de área.
- l. No hacer alusión al formato de una contraseña.
- m. No hablar de las contraseñas frente de otras personas.
- n. No revelar las contraseñas a los jefes.

Responsabilidades del Administrador

- a. El Administrador deberá crear una contraseña con una longitud mínima de 8 caracteres combinando números, letras y símbolos de puntuación.
- b. No usar contraseñas por defecto o iguales al nombre de usuario o del perfil del usuario, nombres de familiares, amigos, mascotas, patentes, número de teléfono, números de documentos, etc. que sean fáciles de detectar.
- c. Cada contraseña de usuario será única para un sistema dado.
- d. Las claves de administradores de las estaciones de trabajo serán administradas entre el personal autorizado para dichas tareas.
- e. Cada clave será única para cada estación de trabajo.
- f. Las contraseñas de usuarios Administradores deberán ser compartidas entre el personal técnico asignado y el responsable de seguridad de cada sistema en particular.

- g. Todos los sistemas dispondrán de un máximo de 3 intentos erróneos de ingreso de contraseña luego del cual inhabilitarán el usuario y/o estación de trabajo.
- h. El administrador será el responsable de rehabilitar al usuario correspondiente bajo la autorización del superior del usuario inhabilitado.
- i. Todos los sistemas dispondrán un mecanismo que fuerce la caducidad de la contraseña la que será de un máximo de 120 días.
- j. Implementar procedimientos de verificación de contraseñas débiles. Estos se ejecutarán periódicamente y se informará al responsable de seguridad de cada sistema respecto al usuario cuya contraseña ha sido detectada.
- k. Todos los sistemas dispondrán de mecanismos de autenticación de usuarios con ocultamiento de ingreso de la contraseña.
- l. Inmediatamente al establecerse la baja de un perfil de usuario, y hasta tanto se efectúe la baja real correspondiente, el administrador de seguridad del sistema cambiará las contraseña del perfil.
- m. En caso de olvido de la contraseña de un usuario, el responsable de área deberá gestionar el cambio de la misma dirigiéndose al administrador de seguridad.
- n. En caso de detectarse que una contraseña ha sido comprometida deberá cambiarse inmediatamente en todos los sistemas donde el usuario use la misma contraseña.
- o. En caso de un incidente de seguridad, deberán cambiarse inmediatamente todas las contraseñas del sistema afectado.

Responsabilidades de Talento Humano

En caso de presentarse el retiro de un funcionario, el responsable de la coordinación de talento humano deberá diligenciar el formato No xxxx llamado (Formato retiro de funcionarios), luego de diligenciar el formato deberá entregarlo en la administración de sistemas con el fin de que el encargado en esta área evalúe si se debe o no realizar un cambio de contraseñas cumpliendo con los criterios de políticas de contraseñas establecidos en este documento.

En caso de presentarse el ingreso de un funcionario el coordinador de talento humano deberá diligenciar el formato No xxx llamado (Formato Ingreso Funcionarios), luego de diligenciar el formato deberá entregarlo en la administración de sistemas con el fin de que el encargado en esta área asigne una contraseña cumpliendo con las políticas de contraseñas y grupos establecidos en este documento.

Políticas de Grupos

Grupo Administradores

Siendo este grupo de usuarios los que controlan por completo todo el dominio. Se encontró que a él pertenecían funcionarios de la cooperativa que no podían estar allí por cuestiones de seguridad y manejo, ya que no tienen el conocimiento de los sistemas de información para controlar este tipo de herramientas. Es recomendable agregar con cautela los usuarios, puesto que este grupo controla por completo el dominio. A continuación se describen unas cuantas funciones a lo que tiene acceso este grupo.

- ✓ Tener acceso al equipo servidor desde la red
- ✓ Ajustar las cuotas de memoria de un proceso
- ✓ Hacer copia de seguridad de archivos y directorios
- ✓ Saltarse la comprobación de recorrido
- ✓ Cambiar la hora del sistema
- ✓ Crear un archivo de paginación
- ✓ Depurar programas
- ✓ Habilitar la confianza para la delegación de las cuentas de usuario y de equipo
- ✓ Forzar el apagado desde un sistema remoto

- ✓ Aumentar la prioridad de programación
- ✓ Cargar y descargar controladores de dispositivo
- ✓ Permitir el inicio de sesión local
- ✓ Administrar el registro de auditoría y seguridad
- ✓ Modificar valores de entorno del firmware
- ✓ Hacer perfil de un solo proceso
- ✓ Hacer perfil del rendimiento del sistema
- ✓ Quitar un equipo de una estación de acoplamiento
- ✓ Restaurar archivos y directorios
- ✓ Apagar el sistema
- ✓ Tomar posesión de archivos y otros objetos.

Los Miembros que se deben alojar en este grupo son aquellos que pertenezcan al área de sistemas, que cumplan con los conocimientos de manejo del directorio activo, aquellos miembros que tengan presente que cualquier permiso mal asignado puede ser una posible puerta abierta para usuarios maliciosos de la red externa. Se recomienda que antes de realizar cualquier cambio se le haga un repaso general a toda la base de datos del directorio.

Grupo Administradores del dominio

Es importante no mezclar miembros de tipo usuarios con miembros de tipo equipos, aunque estos mantiene una relación incondicional este grupo controla el dominio por completo y sus integrantes deben ser cuentas de usuarios. De forma predeterminada, este grupo pasa a ser miembro del grupo Administradores en todos los controladores, estaciones de trabajo y servidores miembros del dominio en el momento en que se une a éste..

El único miembro para el caso de Coodesuris es el administrador general, el esquema se ha diseñado de tal manera teniendo en cuenta que la cantidad de equipos en la institución es mínima y no se requiere tener numerosos miembros en este grupo.

Grupo Equipos del dominio

Este grupo contiene todas las estaciones de trabajo y los servidores unidos al dominio. De forma predeterminada, todas las cuentas de equipo creadas pasan a ser miembros de este grupo automáticamente. Tener usuarios como integrantes de este grupo sería tener un mal almacenamiento de la información ya que sólo deben pertenecer los equipos del dominio.

No hay derechos predeterminados en este grupo, quedaría en manos de la administración de sistemas asignarlos.

Grupo Usuarios y Usuarios del dominio

Los miembros de este grupo pueden realizar las tareas más habituales, como ejecutar aplicaciones, utilizar impresoras locales y de red. Por lo tanto, todas las cuentas de usuario que se crean en el dominio son miembros de este grupo.

Grupo Controladores de dominio

Este grupo contiene todos los controladores del dominio. En un principio sus integrantes no cumplían con las características necesarias para pertenecer al grupo por eso se reestructuro de una mejor manera.

Dependiendo del tipo de organización se asignan miembros a otros grupos, en los cuales se desempeñan labores mayores de productividad y seguridad. Para el caso de Coodesuris se asignó como único integrante de estos grupos al usuario Administrador, por ser el usuario global sin restricción alguna y controlado por el área de sistemas de la cooperativa. Algunos de estos grupos son:

- ✓ Grupo Administradores de esquema
- ✓ Grupo Administradores de organización
- ✓ Grupo Operadores de configuración de red
- ✓ Grupo Operadores de cuentas

✓ Grupo Operadores de impresión

REFERENCIAS

Just another WordPress.com weblog. Windows server 2003: Dominios Windows server y directorio activo. (Sitio de internet). Disponible en: <http://admonredes.wordpress.com/dominios-windows-server-y-directorio-activo/>
Consultado: 17 de abril de 2009

Campus Virtual UM. Open Course Ware. Facultad de Ingeniería. Redes. (Sitio de Internet). Disponible en: http://ocw.virtualum.edu.co/ocwum/facultad-de-ingenieria-1/redes-i/redes-i/doc/Que_es_una_Red1.doc. Consultado: 23 de abril de 2009

Allele Mantenimiento de redes y Servidores. Mantenimiento de servidores. Disponible en: <http://www.allele.com.ar/mantenimiento-de-servidores.php>
Consultado: 20 de Abril 2009

Centro de desarrollo de Team Foundation Server. Biblioteca. Herramientas y lenguajes de desarrollo. Visual Studio 2005. Documentación de Visual Studio Team System. Documentación de Team Foundation. Administradores de Team Foundation. Planeamiento de Team Foundation Server. Plan de mantenimiento del servidor. Plan de copia de seguridad y restablecimiento. (Sitio de Internet) Disponible en: [http://msdn.microsoft.com/es-es/library/ms316430\(VS.80\).aspx](http://msdn.microsoft.com/es-es/library/ms316430(VS.80).aspx)
Consultado 17 de abril de 2009

Tanenbaum A. Redes de computadoras. Tanenbaum A. México DF. 4ta edición Prentice Hall, 2003. Cap. 1, 3 y 8

Microsoft. Support TechNet Security. Proceso de Administración de Revisiones. (Sitio de internet). Disponible en: <http://www.microsoft.com/spain/technet/security/guidance/patchmanagement/default.aspx> Consultado 3 de Mayo de 2009.

Kaspersky Lab's Official Sites. Kaspersky Lab documentation. (Sitio de Internet). Disponible en: http://downloads.kaspersky-labs.com/docs/spanish/kasp6.0_ak_deployguidees.pdf Consultado 14 de junio de 2009

Duamu. Portada. Manuales firewalls y seguridad en internet. (Sitio de Internet). Disponible en <http://www.duamu.com/re/manual/1680/id/2652/manuales-firewalls-y-seguridad-en-internet.html> Consultado 26 de Junio de 2009

Williams R, Walla M. La Biblia de Windows Server 2003: Administración de Sistemas. Madrid. 1ra edición Prentice Hall, 2003. Cap. 4 y 6