UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD DE INGENIERÍA EN SISTEMAS ELECTRÓNICA E INDUSTRIAL

DIRECCIÓN DE POSGRADO

MAESTRÍA EN REDES Y TELECOMUNICACIONES

TEMA:

"GESTIÓN DE AUDITORÍA DE ACCESO A INFORMACIÓN COMPARTIDA EN RED Y SU INCIDENCIA EN LA VULNERABILIDAD DE LA INFORMACIÓN EN LA COOPERATIVA DE AHORRO Y CREDITO COCA LTDA."

Trabajo de Titulación

Previo a la obtención del Grado Académico de Magíster en Redes y Telecomunicaciones

Autor: Ingeniero Henry Rodrigo Vivanco Herrera
Director: Ingeniero Franklin Mayorga Mayorga, Magíster.

Ambato - Ecuador

2015

Al Consejo de Posgrado de la Universidad Técnica de Ambato.

El Tribunal de Defensa del trabajo de titulación presidido por Ingeniero José Vicente Morales Lozada Magíster., Presidente del Tribunal e integrado por los señores Ingeniero Oswaldo Eduardo Paredes Ochoa Magíster, Ingeniero Marco Antonio Jurado Lozada Magíster, Ingeniero Juan Pablo Pallo Noroña Magíster., designados por el Consejo Académico de Posgrado de la Facultad de Ingeniería en Sistemas Electrónica e Industrial de la Universidad Técnica de Ambato, para receptar la defensa oral del trabajo de titulación para graduación con el tema: **"GESTIÓN DE AUDITORÍA DE ACCESO A INFORMACIÓN COMPARTIDA EN RED Y SU INCIDENCIA EN LA VULNERABILIDAD DE LA INFORMACIÓN EN LA COOPERATIVA DE AHORRO Y CREDITO COCA LTDA."**, elaborado y presentado por el señor Ingeniero Henry Rodrigo Vivanco Herrera, para optar por el Grado Académico de Magister en Redes y Telecomunicaciones. Una vez escuchada la defensa oral el Tribunal aprueba y remite el trabajo de titulación para uso y custodia en las bibliotecas de la UTA.

Ingeniero José Vicente Morales Lozada, Magíster
Presidente del Tribunal de Defensa

Ingeniero Oswaldo Eduardo Paredes Ochoa, Magíster
Miembro del Tribunal

Ingeniero Marco Antonio Jurado Lozada, Magíster
Miembro del Tribunal

Ingeniero Juan Pablo Pallo Noroña, Magíster
Miembro del Tribunal

AUTORÍA DE LA INVESTIGACIÓN

La responsabilidad de las opiniones, comentarios y críticas emitidas en el trabajo de titulación con el tema: **"GESTIÓN DE AUDITORÍA DE ACCESO A INFORMACIÓN COMPARTIDA EN RED Y SU INCIDENCIA EN LA VULNERABILIDAD DE LA INFORMACIÓN EN LA COOPERATIVA DE AHORRO Y CREDITO COCA LTDA."**, le corresponde exclusivamente a: Ingeniero Henry Rodrigo Vivanco Herrera, Autor bajo la dirección de: Ingeniero Franklin Mayorga Mayorga, Magíster. Director del trabajo de titulación; y el patrimonio intelectual del mismo a la Universidad Técnica de Ambato.

Ingeniero Henry Rodrigo Vivanco Herrera	Ingeniero Franklin Mayorga Mayorga, Magíster
Autor	Director

DERECHOS DE AUTOR

Autorizo a la Universidad Técnica de Ambato, para que haga de este trabajo de titulación como un documento disponible para su lectura, consulta y procesos de investigación.

Cedo los Derechos de mi trabajo de titulación, con fines de difusión pública, además autoriza su reproducción dentro de las regulaciones de la Universidad.

Ingeniero Henry Rodrigo Vivanco Herrera

CC: (1712715463)

DEDICATORIA

A mi esposa; Ing. Tannia Mayorga Mg., por su constante apoyo y motivación para la conclusión de mi Maestría.

A mi hijo; José Daniel, como muestra de que toda meta se puede alcanzar sin importar el tiempo que tome.

A mis padres; Rosita Herrera y Vicente Vivanco, y mi suegro; Lcdo. José Mayorga, por su tiempo, apoyo e incentivo para la terminación de la Maestría.

A mis hermanos; Edgar, Danilo y Vinicio (+), como incentivo para su constante formación académica.

Ing. Henry Rodrigo Vivanco Herrera

AGRADECIMIENTO

A Dios por darme la dicha de vivir el tiempo suficiente para concluir mi tesis.

A mi Director; Ing. Franklin Mayorga Mg., por la paciencia y el permitir hacer uso de la tecnología para comunicarnos remotamente.

A Ing. Victor Hugo Abril Mg, por los conocimientos impartidos para la estructuración del plan de tesis.

A Econ. Aldrin Cuvi; Gerente General de Cooperativa Coca Ltda. por su apertura a la realización de esta investigación en pro de mejorar el aseguramiento de la información de su representada.

Al personal operativo y administrativo de Cooperativa Coca Ltda. por su colaboración durante la elaboración de ésta investigación.

A mis revisores; Ing. Oswaldo Paredes, Ing. Marco Jurado e Ing. Juan P. Pallo, por sus observaciones y correcciones que permitieron mejorar el informe de investigación.

Ing. Henry Rodrigo Vivanco Herrera

ÍNDICE

AUTORÍA iii

DERECHOS DE AUTOR iv

Dedicatoria v

Agradecimiento vi

Resumen ejecutivo xv

CAPÍTULO I EL PROBLEMA 1

1.1 Tema de Investigación 1

1.2 Planteamiento del problema 1

1.2.1 Contextualización 1

1.2.2 Análisis crítico 3

1.2.2.1 Árbol de problemas 3

1.2.2.2 Relación causa-efecto 4

1.2.3 Formulación del problema 5

1.2.4 Preguntas directrices 5

1.2.5 Delimitación 6

1.3 Justificación 6

1.4 Objetivos 7

1.4.1 General 7

1.4.2 Específicos 7

CAPÍTULO II MARCO TEÓRICO 8

2.1 Antecendentes Investigativos 8

2.2 Fundamentación filosófica 8

2.3 Fundamentación legal 9

2.4 Categorías Fundamentales 10

2.4.1 Visión dialéctica de conceptualizaciones que sustentan las variables del problema 10

2.4.1.1 Marco conceptual variable independiente 10
2.4.1.2 Marco conceptual variable dependientea 12
2.4.2 Gráficos de inclusión interrelacionados 15
2.5 Hipótesis 17
2.6 Señalamiento variables de la hipotesis 17

CAPÍTULO III METODOLOGÍA 18
3.1 Enfoque 18
3.2 Modalidad básica de la investigación 18
3.2.1 Investigación de campo 18
3.2.2 Investigación bibliográfica documental 19
3.2.3 Experimental 19
3.3 Nivel o tipo de investigación 19
3.3.1 Investigación exploratoria 19
3.3.2 Investigación descriptiva 20
3.3.3 Investigación asociación de variables (correlacional) 20
3.3.4 Investigación explicativa 21
3.4 Población y muestra 21
3.4.1 Población 21
3.4.2 Muestra 22
3.5 Operacionalización de variables 22
3.5.1 Operacionalización de la variable independiente 24
3.5.2 Operacionalización de la variable dependiente 25
3.6 Recolección de la información 26
3.6.1 Plan para la recolección de información 26
3.7 Procesamiento y análisis 28
3.7.1 Plan de procesamiento de información 28
3.7.2 Plan de análisis e interpretación de resultados 29

CAPÍTULO IV ANÁLISIS E INTERPRETACIÓN DE RESULTADOS 31
4.1 Análisis de los resultados 31
4.2 Interpretación de los resultados 31
4.2.1 Encuesta realizada al personal operativo y administrativo . . . 32
4.2.2 Entrevista realizada al Gerente General 48
4.3 Verificación de hipótesis 50
4.3.1 Formulación de la Hipótesis Nula (Ho) y la Hipótesis de Investigación (Hi) 51
4.3.1.1 Modelo Lógico 51

4.3.1.2 Modelo Estadístico 51
4.3.1.3 Determinación del nivel de significancia o riesgo . . . 51
4.3.1.4 Frecuencia Observada 53
4.3.1.5 Grados de libertad 53
4.3.1.6 Frecuencia Esperada 53
4.3.1.7 Tabla de cálculo Ji-cuadrado 54
4.3.1.8 Zona de aceptación/rechazo 54
4.3.1.9 Decisión 54

CAPÍTULO V CONCLUSIONES Y RECOMENDACIONES 55

5.1 Conclusiones 55
5.2 Recomendaciones 55

CAPÍTULO VI PROPUESTA 57

6.1 DATOS INFORMATIVOS 57
6.1.1 Tema 57
6.1.2 Datos informativos 57
6.2 ANTECEDENTES 58
6.3 JUSTIFICACIÓN 59
6.4 OBJETIVOS 60
6.4.1 General 60
6.4.2 Específicos 60
6.5 ANÁLISIS DE FACTIBILIDAD 61
6.6 FUNDAMENTACIÓN 61
6.7 METODOLOGÍA 64
6.8 MODELO OPERATIVO 66
6.8.1 Diagnóstico de situación actual 66
6.8.1.1 Esquema de red actual 66
6.8.2 Análisis de riesgos de la información compartida en red 66
6.8.3 Rediseño esquema de red de datos de la Oficina Matriz de la Cooperativa de Ahorro y Crédito Coca Ltda. 71
6.8.4 Definición de políticas de control de acceso a la información compartida en red 71
6.8.4.1 Instructivo para etiquetado y manejo de información y documentos 72
6.8.4.2 Políticas para asegurar el acceso a la red de datos . . 75
6.8.4.3 Formulario para la solicitud de creación de usuario . 79

6.8.4.4 Formulario para la solicitud de acceso al servidor de archivos 80
6.8.4.5 Políticas para el correcto uso del servidor de archivos 82
6.8.4.6 Pregunta 16: ¿Considera que compartir información en la red de datos de la Coooperativa es seguro? . . . 83
6.8.4.7 Formulario para el registro de incidencias en el servidor de archivos 84
6.8.4.8 Directivas de auditoría 85
6.9 ADMINISTRACIÓN 87
6.10 PLAN DE ACCIÓN 88
6.11 PREVISIÓN DE LA EVALUACIÓN 88
6.11.1 Tabulación de resultados 90
6.11.1.1 Primera fase: sin control de acceso a la información compartida en red 90
6.11.1.2 Segunda fase: implementación de políticas de control de acceso a la información compartida en red 90
6.11.1.3 Equipo encargado de la evaluación 91
6.11.2 EVALUACIÓN 91
6.11.2.1 Entrevista aplicada a los miembros del equipo de evaluación 91
6.11.2.2 Evaluación por parte del investigador 93
6.12 CONCLUSIONES Y RECOMENDACIONES 94
6.12.1 Conclusiones 94
6.12.2 Recomendaciones 94

BIBLIOGRAFIA **95**

ANEXOS **100**

ÍNDICE DE TABLAS

2 Nómina oficial de empleados de la oficina matriz de Cooperativa de Ahorro y Crédito Coca Ltda. 22
3 Operacionalización DE LA VARIABLE INDEPENDIENTE 24
4 Operacionalización DE LA VARIABLE DEPENDIENTE 25
5 Título con la idea principal de la pregunta 28
6 Relación de objetivos específicos, conclusiones y recomendaciones . . 30
7 Empleado tiene asignado un computador 32
8 Digita o seleCCIÓNa un usuario para poder utilizar el computador . 33
9 Computador protegido con contraseña 34
10 Contraseña relacionada con información personal (Iniciales, identificación, fecha de cumpleaños,etc) 35
11 Sabe como compartir información 36
12 Tiene información compartida en red 37
13 ¿Cómo comparte la información con otros usuarios a través de la red? 38
14 Conoce que puede establecer permisos de acceso a la información compartida 39
15 información compartida en red ha sido modificada sin permiso 40
16 información compartida en red ha sido eliminada 41
17 Tiene respaldo de la información relacionada con el trabajo 42
18 información compartida está segura 43
19 Restringir el acceso a la información compartida solo a usuarios seleccionados 44
20 Establecer permisos de acceso a la información compartida 45
21 Determinar quien modificó o eliminó la información compartida . . . 46
22 Compartir información a través de la red de la Cooperativa es seguro 47
23 Facilita el trabajo el acceder a información compartida en red 48
25 Frecuencia Observada 53
26 Frecuencia Esperada 53
27 Tabla de Cálculo Ji-cuadrado 54

28 Amenazas físicas de la información compartida en red 67
29 Amenazas lógicas de la información compartida en red 68
30 Vulnerabilidades físicas 69
31 Vulnerabilidades lógicas 70
37 Compartir información a través de la red de la Cooperativa es seguro 83
39 Administración 87
40 Evaluación de acceso a la información del departamento de contabilidad compartida en red 90
41 Evaluación de acceso a la información del departamento de contabilidad compartida en red luego de aplicar políticas de acceso a la información 90
42 Equipo encargado de la evaluación 91

ÍNDICE DE FIGURAS

1 Árbol de problemas 3

2 Superordinación conceptual 15
3 Subordinación conceptual. 16

4 Ejemplo de figura a ser utilizada 29

5 Empleado tiene asignado un computador 32
6 Digita o seleCCIÓNa un usuario para poder utilizar el computador . 33
7 Computador protegido con contraseña 34
8 Contraseña relacionada con información personal (Iniciales, identificación, fecha de cumpleaños,etc) 35
9 Sabe como compartir información a través de la red 36
10 Tiene información compartida en red 37
11 ¿Cómo comparte información con otros usuarios en red? 38
12 Establecer permisos de acceso a la información compartida 39
13 información compartida en red ha sido modificada sin permiso 40
14 información compartida en red ha sido eliminada 41
15 Tiene respaldo de la información relacionada con el trabajo 42
16 información compartida en red está segura 43
17 Restringir el acceso a la información compartida solo a usuarios seleccionados 44
18 Establecer permisos de acceso a la información compartida 45
19 Determinar quien modificó o eliminó la información compartida . . . 46
20 Compartir información a través de la red de la Cooperativa es seguro 47
21 Facilita el trabajo el acceder a información compartida en red 48

22 Sistema de gestión de auditoría de acceso a recursos compartidos en red 65
23 Esquema de red de la Cooperativa de Ahorro y Crédito Coca Ltda. . 66
24 Esquema propuesto de red de la Cooperativa de Ahorro y Crédito Coca Ltda. 71

25 Compartir información a través de la red de la Cooperativa es seguro 83
26 Cronograma de implementación de ambiente de pruebas 89
27 Evaluación de la propuesta 91
28 Evaluación de la propuesta 92
29 Evaluación de la propuesta 92
30 Acceso a información compartida en red si restricción 93
31 Acceso a información compartida en red si restricción 93

RESUMEN EJECUTIVO

Texto del resumen ejecutivo

CAPÍTULO I

EL PROBLEMA

1.1. TEMA DE INVESTIGACIÓN

"Gestión de auditoría de acceso a información compartida en red y su incidencia en la vulnerabilidad de la información en la Cooperativa de Ahorro y Crédito Coca Ltda."

1.2. PLANTEAMIENTO DEL PROBLEMA

1.2.1. Contextualización

Hoy en día son mayores los riesgos asociados a los sistemas de información, equipos y comunicaciones con que cuentan las empresas más aún si éstas no poseen adecuados controles de seguridad, acceso, autorización y autenticación. La continua masificación del uso y acceso a las tecnologías de información y comunicaciones (TIC's) ha traído consigo un incremento de las amenazas a las que se exponen las organizaciones; sean éstas grandes, medianas o pequeñas y que dependiendo del ámbito, importancia y posicionamiento que tienen; en el sector que se desenvuelven, pueden ser víctimas del espionaje industrial, robo de información, interrupción de sus servicios y fallas críticas en la infraestructura y sistemas centrales de información. En mayo del 2013 la Corporación de Radio y Televisión Española a través de su sitio web RTVE.es publicó la noticia de que el Departamento de Defensa de los Estados Unidos de Norteamérica (Pentágono); en un informe anual, acusaba directamente a China de estar utilizando espionaje para acceder a tecnologías que ayuden a su acelerado programa de modernización militar. Esto significaría que China ha usado cyber-espionaje y ha vulnerado todas las seguridades establecidas por el Pentágono para evitar este tipo de intrusiones. Lo que más preocupa al Pentágono; según el

mismo informe, es que "... las habilidades necesarias para este tipo de intrusiones son muy similares a las necesarias para llevar a cabo ataques informáticos".

En el trabajo de Salazar and Campos (sf) hace referencia a la noticia de que en el mes de mayo del año 2008 se publicó en internet información personal (números de identidad, direcciones, teléfonos comerciales y particulares, correos electrónicos e información académica y social) de alrededor de seis millones de chilenos misma que fue obtenida; de manera fraudulenta, de los sitios web de instituciones como la Dirección General de Movilización Nacional, el Servicio Electoral, el Ministerio de Educación, el sitio de la Prueba de Selección Universitaria (PSU) y registros telefónicos.

El Ecuador no es ajeno a este tipo de problemas y amenazas. El 12 abril del año 2013 se difundió a través de los medios de comunicación; entre ellos Ecuadorinmediato (2013), que el Alcalde de la Ciudad de Riobamba realizó una denuncia en la cual hacía mención a un hackeo de las cuentas en el Banco Central del Ecuador producto de lo cual se realizaron transferencias por un valor de poco más de 13 millones de dólares de la cuenta del cabildo riobambeño. En la semana siguiente a la denuncia se pudo conocer que la misma no se encontraba fundamentada. Luego que se realizaron las primeras investigaciones se obtuvo como resultado que no existió ningún tipo de hackeo sino que se trató del mal uso de claves de acceso del Alcalde, Director Financiero y Tesorera del Municipio de Riobamba. Adicionalmente el propio alcalde manifestó que su contraseña era conocida por al menos otra persona.

En el año 2009 las instituciones públicas del Ecuador; entre ellas la Presidencia de la República, fueron el objetivo de ataques conocidos como *"defacement"* (en el área de la informática se refiere a la modificación o alteración de manera intensionada de un sitio web), mismos que se atribuyó el grupo "Anonymous Ecuador" en su operación denominada Cóndor Libre como parte de las protestas en contra de la Ley de Comunicación.

Como se puede apreciar, la información digital se ha convertido en el activo más valioso de toda empresa y al ser compartida dentro de una red de computadores se encuentra expuesta a amenazas (vulnerabilidad) y posibles ataques informáticos; tanto internos como externos, más aún si no se establecen adecuadas políticas de control de acceso y protección de la misma.

En el caso de una institución financiera los datos con que cuentan son aún más sensibles y críticos, ya que posee información sumamente delicada de sus clientes y socios (ingresos, egresos, patrimonio, direcciones, teléfonos de contacto, familiares)

que de ser divulgadas; con o sin el conocimiento de las autoridades de la entidad, podrían acarrearle problemas incluso de índole legal. La Cooperativa de Ahorro y Crédito Coca Ltda., ha tenido un continuo crecimiento en los últimos años, razón por la cual ha sido necesario que su planta de recurso humano se incremente. Esto conlleva un aumento en lo que a equipos de computación se refiere lo que a su vez implica que exista una mayor cantidad de información compartida y disponible a través de la red de datos sin ningún tipo de restricción o bitácora de registro de acceso a la misma por lo que se ha vuelto imperativo el contar con un método de autenticación de acceso a la red, autorización de acceso a la información compartida y un registro de auditoría de que empleado accedió y que tareas realizó con la misma, precautelando de esta manera la posible pérdida de información o modificación no autorizada de los datos.

1.2.2. Análisis crítico

1.2.2.1. Árbol de problemas

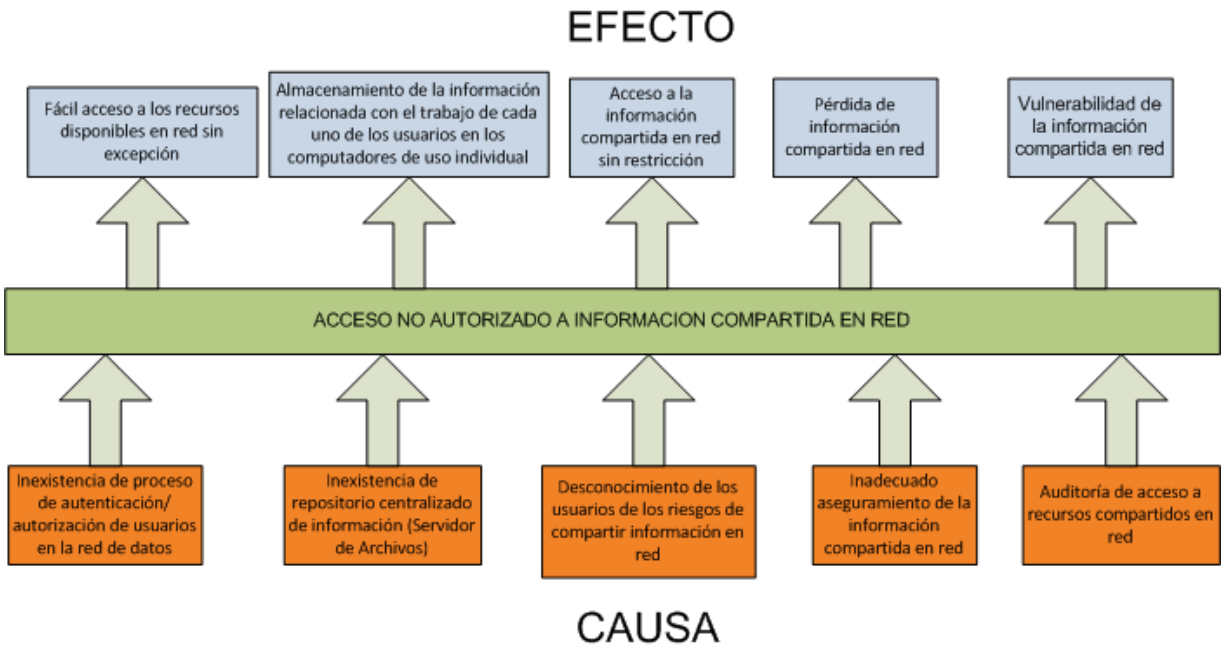


Figura 1: Árbol de problemas
Fuente: Matriz MAS
Elaborado por: Henry Vivanco (2014)

1.2.2.2. Relación causa-efecto

El incremento del uso de las TIC's ha hecho que la mayor cantidad de información de toda institución se encuentre almacenada en medios digitales; sean estos: discos compactos, disco duro, correo electrónico, entre otros. Esto a su vez conlleva un alto riesgo de que sea eliminada o alterada o de que personas no autorizadas tengan acceso a ella. Es así que de no establecer mecanismos adecuados que la protejan harán que ella se encuentre sumamente vulnerable.

Lo anteriormente descrito puede observarse de forma clara y precisa en la Matriz de Análisis de Situación (Anexo 1)

La Cooperativa de Ahorro y Crédito Coca Ltda. no cuenta con ningún método o proceso de autenticación y autorización de usuarios para el acceso a su red de datos lo cual se convierte en un grave riesgo puesto que cualquier persona que acceda a la red; de manera inalámbrica o con cable, tendrá acceso a todos los recursos que se encuentren disponibles a través de ésta y en especial a la información compartida la cual; en la mayoría de casos, es sumamente sensible como por ejemplo la financiera.

Un Servidor de Archivos es un lugar físico centralizado en el cual los empleados de una institución deben guardar la información con la que realizan sus actividades diarias. Entre varias de las ventajas que este tipo de servicio ofrece el principal es que se puede gestionar de una manera fácil y adecuada los respaldos de la misma al punto de poder recuperar el estado de un archivo a una fecha y hora específica. Al no contar la Cooperativa de Ahorro y Crédito Coca Ltda. con este servicio sus empleados se ven obligados a almacenar la información de trabajo en el computador que le ha sido asignado así como también por propia cuenta mantener un respaldo de la información que a su criterio es la más importante, muchas de las veces en dispositivos no adecuados como una memoria USB con el consecuente riesgo de que la misma se pierda o dañe provocando la perdida de información.

Los empleados de la Cooperativa; por otra parte, desconocen los riesgos a que exponen su información al compartirla en red tanto es así que muchos de los equipos tienen compartido su disco duro completo y además con permisos de lectura/escritura lo cual facilitaría; además de copiar la información, que ésta sea alterada o eliminada sin poder determinar quien lo hizo.

Considerando la importancia que representa para toda institución su información se hace necesario el poder contar con mecanismos que ayuden a la protección de la misma así como también aquellos que ayuden a prevenir posibles accesos no

autorizados a la información. En el caso de la Cooperativa de Ahorro y Crédito Coca Ltda. el contar con auditoría de acceso a recursos compartidos red se vuelve una herramienta que permitirá reducir la vulnerabilidad de la información.

Considerando todo lo anterior; en caso de no realizar ésta investigación, la Cooperativa de Ahorro y Crédito Coca Ltda. seguirá expuesta a pérdida o alteración de información compartida en red ocasionando graves inconvenientes a quienes pertenece la misma y sin medios que permitan determinar quién originó estos inconvenientes.

1.2.3. Formulación del problema

¿Es la inaplicación de la gestión de auditoría de acceso a información compartida en red la principal causa de acceso no autorizado y vulnerabilidad de información compartida en red en la oficina matriz de la Cooperativa de Ahorro y Crédito Coca Ltda. durante el periodo comprendido entre junio y noviembre del año 2014?

1.2.4. Preguntas directrices

- ¿Qué herramientas informáticas existen que permitan proteger la información compartida en red de accesos no autorizados?
- ¿Qué políticas; acordes a la realidad de la Cooperativa de Ahorro y Crédito Coca Ltda., se deben definir para compartir información en la red de datos?
- ¿Centralizar la información de todos los usuarios; relacionada con las tareas que desempeñan, en un servidor de archivos permitirá reducir la pérdida o alteración de información?
- ¿Qué aspectos deben ser tomados en cuenta para definir las políticas de autenticación y autorización de acceso a la red de datos?
- ¿Cómo ayuda una adecuada gestión de auditoría de acceso a información compartida en red a la disminución de la vulnerabilidad de la información?
- ¿Conocen los usuarios el riesgo que representa el compartir la información en red sin ningún tipo de restricción?
- ¿Qué nivel de confianza tienen los empleados de la Cooperativa de Ahorro y Crédito Coca Ltda. respecto de compartir la información en red?

- ¿Tienen los usuarios respaldo de su información sensible de tal manera de poder recuperarla en caso de que se presente algún incidente en el cual su computador sufra algún desperfecto físico o lógico?

1.2.5. Delimitación

- **Campo:** Maestría en Redes y Telecomunicaciones (primera versión)
- **Área:** Administración y Seguridad de Redes, Internet working NT y 2000 Advanced Server
- **Aspecto:** Acceso autorizado a información compartida en red
- **Temporal:** La investigación se realizó desde el mes de junio hasta el mes de noviembre del año 2014
- **Espacial:** El proyecto de investigación se llevó a cabo en las instalaciones de la oficina matriz de la Cooperativa de Ahorro y Crédito Coca Ltda., ubicada en la Av. Quito y Bolívar en la ciudad de Francisco de Orellana provincia Orellana. (Anexo 2: Registro Unico de Contribuyentes)

1.3. JUSTIFICACIÓN

En la actualidad uno de los temas que más preocupa a cualquier institución es poder asegurar su información. Sin embargo, muchas veces no le dan la importancia que realmente merece y es recién cuando sucede algún incidente en el cual su información se ve comprometida que deciden tomar acciones para evitar que vuelvan a suceder. En el caso puntual de la Cooperativa de Ahorro y Crédito Coca Ltda. sucedió que una información que la Jefe de Crédito tenía compartida en red fue eliminada y; considerando el hecho de que era una recopilación de datos de cerca de un año, el impacto para la Cooperativa fue sumamente grave.

La importancia de esta investigación radica en establecer adecuadas políticas de acceso a la información compartida en red, que a su vez permitan realizar una adecuada gestión del registro de las actividades realizadas con la misma (modificación, creación, eliminación).

El presente proyecto de investigación es factible en la Institución ya que se cuenta con el apoyo del Gerente General y la colaboración de los jefes de cada departamento así como también del personal operativo. En lo que se refiere a documentación existe

suficiente material bibliográfico que ayudará al adecuado desarrollo de la misma.

Los beneficiarios directos de la investigación será todo el personal que labora en la oficina Matriz de la Cooperativa Coca Ltda. y en general la institución por sí misma. Así se dará cumplimiento a parte de la Ley de Economía Popular y Solidaria y su reglamento que establece que las cooperativas deben hallar los mecanismos adecuados para disminuir la vulnerabilidad y asegurar la información con que cuentan.

1.4. OBJETIVOS

1.4.1. General

- Diseñar una adecuada gestión de auditoría de acceso a información compartida en red que disminuya el riesgo de vulnerabilidad de la información en la Cooperativa de Ahorro y Crédito Coca Ltda..

1.4.2. Específicos

- Establecer políticas para la compartición de información en red para reducir el nivel de vulnerabilidad de la misma
- Definir adecuadas políticas de auditoría de acceso a información compartida en red para evidenciar accesos no autorizados a la misma
- Proponer el diseño de un sistema de gestión de auditoría de acceso a información compartida en red que permita obtener evidencia de intentos de acceso no autorizado y posibles alteraciones a la misma

CAPÍTULO II

MARCO TEÓRICO

2.1. ANTECENDENTES INVESTIGATIVOS

Una de las principales preocupaciones para cualquier institución ha sido el asegurar su información, independientemente de cómo o donde se encuentre ella almacenada. En la tesis de Enríquez Miranda (2010) establece que:

Debemos comprender que para que la información se considere segura debe contar con las siguientes características:

> **Integridad:** La información sólo puede ser modificada por quien está autorizado y de manera controlada.
>
> **Confidencialidad:** La información sólo debe ser legible para los autorizados.
>
> **Disponibilidad:** Debe estar disponible cuando se necesita.
>
> **Irrefutabilidad:** El uso y/o modificación de la información por parte de un usuario debe ser irrefutable, es decir, que el usuario no puede negar dicha acción

2.2. FUNDAMENTACIÓN FILOSÓFICA

Un paradigma de investigación; para Ortiz (1998), es "...el conjunto de normas y creencias básicas que sirven de guía a la investigación".

La presente investigación se fundamenta en el paradigma positivista cuyas características principales; según Álvarez-Gayou (2005), son las siguientes:

> - El punto de partida del científico es la realidad, que mediante la investigación le permite llegar a la ciencia. El científico observa, descubre, explica y predice aquello que lo lleva a un conocimiento sistemático de

la realidad [Tamayo 1994].

- Los fenómenos, los hechos y los sujetos son rigurosamente examinados o medidos en términos de cantidad, intensidad o frecuencia.
- La realidad se considera estática.
- Se pretende objetividad del investigador.
- Las situaciones "extrañas" que afecten la observación y la objetividad del investigador se controlan y evitan.
- Se considera que hay una realidad allá afuera que debe ser estudiada, capturada y entendida [Taylor y Bogdan 1996].

El enfoque predominante de investigación es el cuantitativo sobre el cual Grajales (2000) dice lo siguiente:

> Enfoques positivistas promueven la investigación empírica con un alto grado de objetividad suponiendo que si alguna cosa existe, existe en alguna cantidad y si existe en alguna cantidad se puede medir. Esto da lugar al desarrollo de investigaciones conocidas como cuantitativas, las cuales se apoyan en las pruebas estadísticas tradicionales.

2.3. FUNDAMENTACIÓN LEGAL

El Código Orgánico Integral Penal(COIP) (2014), publicado en el Registro Oficial Suplemento No. 180 del 10 de febrero de 2014 en su Capítulo Tercero: Delitos Contra los Derechos del Buen Vivir, Sección Tercera: Delitos contra la seguridad de los activos de los sistemas de información y comunicación, dice:

> **Art. 229.-** Revelación ilegal de base de datos.- La persona que, en provecho propio o de un tercero, revele información registrada, contenida en ficheros, archivos, bases de datos o medios semejantes, a través o dirigidas a un sistema electrónico, informático, telemático o de Telecomunicaciones; materializando voluntaria e intencionalmente la violación del secreto, la intimidad y la privacidad de las personas, será sancionada con pena privativa de libertad de uno a tres años. Si esta conducta se comete por una o un servidor público, empleadas o empleados bancarios internos o de instituciones de la economía popular y solidaria que realicen intermediación financiera o contratistas, será sancionada con pena privativa de libertad de tres a cinco años.
>
> **Art. 230.-** Interceptación ilegal de datos.- Será sancionada con pena

privativa de libertad de tres a cinco años: 1. La persona que sin orden judicial previa, en provecho propio o de un tercero, intercepte, escuche, desvíe, grabe u observe, en cualquier forma un dato informático en su origen, destino o en el interior de un sistema informático, una señal o una transmisión de datos o señales con la finalidad de obtener información registrada o disponible. (. . .)

Art. 232.- Ataque a la integridad de sistemas informáticos.- La persona que destruya, dañe, borre, deteriore, altere, suspenda, trabe, cause mal funcionamiento, comportamiento no deseado o suprima datos informáticos, mensajes de correo electrónico, de sistemas de tratamiento de información, telemático o de Telecomunicaciones a todo o partes de sus componentes lógicos que lo rigen, será sancionada con pena privativa de libertad de tres a cinco años.(. . .)

Art. 234.- Acceso no consentido a un sistema informático, telemático o de Telecomunicaciones.- La persona que sin autorización acceda en todo o en parte a un sistema informático o sistema telemático o de Telecomunicaciones o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho, para explotar ilegítimamente el acceso logrado, modificar un portal web, desviar o redireCCIÓNar de tráfico de datos o voz u ofrecer servicios que estos sistemas proveen a terceros, sin pagarlos a los proveedores de servicios legítimos, será sancionada con la pena privativa de la libertad de tres a cinco años.

2.4. CATEGORÍAS FUNDAMENTALES

2.4.1. Visión dialéctica de conceptualizaciones que sustentan las variables del problema

2.4.1.1. Marco conceptual variable independiente

Seguridad Informática.- Según (Mayorga Jácome, 2013); basado en (Matilla, A. 2013, pág.1), respecto de la seguridad informática dice lo siguiente:

> ...es el área de la informática que se enfoca en la protección de la infraestructura computacional y todo lo relacionado con ésta (incluyendo la información contenida) y puede ser aplicada en cualquier ámbito como es la educación, en donde juega un papel fundamental la aplicación de estándares, protocolos, métodos, reglas, herramientas y leyes concebidas

> para minimizar los posibles riesgos en el área tecnológica, ya sea de laboratorios de computación, de equipos que maneja el personal administrativo y docente, la infraestructura de red, información y sistemas con sus respectivas bases de datos que se utilicen para facilitar la gestión de matrículas, calificaciones, entre otros; es decir constituye todo lo que la organización valore como activo y signifique un riesgo si esta llega a manos de otras personas.

Sistema de Gestión de Seguridad de la información (SGSI).- (Ortin, 2013)en su página web dice que:

> El concepto clave de un SGSI es el diseño, implantación y mantenimiento de un conjunto de procesos para gestionar eficientemente la accesibilidad de la información, buscando asegurar la confidencialidad, integridad y disponibilidad de los activos de información minimizando a la vez los riesgos de seguridad de la información.

Auditoría Informática.- Para comprender de mejor manera este concepto, es conveniente primero definir lo que es auditoría. Para Buades (2002), auditoría es la "Actividad para determinar, por medio de la investigación, la adecuación de los procedimientos establecidos, instrucciones, especificaciones, codificaciones y estándares u otros requisitos, la adhesión a los mismos y la eficiencia de su implantación." . El mismo autor define la auditoría informática como:

> Es el conjunto de técnicas, actividades y procedimientos, destinados a analizar, evaluar, verificar y recomendar en asuntos relativos a la planificación, control eficacia, seguridad y adecuación del servicio informático en la empresa, por lo que comprende un examen metódico, puntual y discontinuo del servicio informático, con vistas a mejorar en: rentabilidad, seguridad, eficacia

Para el autor Rivas (1989) la auditoría informática es considerada un "examen metódico del servicio informático, o de un sistema informático en particular, realizado de una forma puntual o de modo discontinuo, a instancias de la dirección con la intención de ayudar o mejorar conceptos de la seguridad, eficacia, rentabilidad del servicio o del sistema que resultan auditados" Por lo que se puede decir que la auditoría informática es realizada con la finalidad de precautelar los activos informáticos, velar por la integridad de los mismos, usar eficientemente los recursos, cumplimiento de leyes y regulaciones establecidas, se enfoca en los fines que la organización o empresa persigue, los encargados de hacerlo recopilan, agrupan y

evalúan evidencias; deben ser profesionales especializados en auditoría informática o certificados en alguna metodología, estándar como por ejemplo COBIT (modelo para auditar la gestión y control de los Sistemas de información y Tecnología cuyas siglas en Ingles son "Control Objective for Information Systems and related technology" y fue desarrollado por ISCA (Information Systems Audit and Control Asociation), ITIL (pertenece a la OGC (Oficina de Comercio de Gobierno Británico) y es de libre utilización), Normas ISO 27000 (conjunto de normas internacionales emitida por la organización internacional ISO la última revisión fue la ISO IEC 27001 2013). La auditoría informática puede realizarse internamente con personal que trabaja en una organización lo que es conocida como Auditoría interna o puede realizarse contratando profesionales externos que realicen este proceso y emitan criterios con soluciones lo cual se conoce como auditoría externa.

Auditoría de redes.- Una de las áreas más importantes de una empresa; en lo que respecta a la informática, es su red de datos. Su correcto funcionamiento es hoy uno de los aspectos críticos para la continuidad del negocio de cualquier institución razón por la cual protegerla es una necesidad y una manera de asegurar su correcto funcionamiento es precisamente el realizar una auditoría enfocada exclusivamente a la red de datos. Para Ochoa Correa (2010) la auditoría de redes "son una serie de mecanismos mediante los cuales se prueba una Red Informática, evaluando su desempeño y seguridad, logrando una utilización mas eficiente y Segura de la información.".

2.4.1.2. Marco conceptual variable dependientea

Ataque informático: De acuerdo a Mieres (2009), existen 5 fases que conforman un ataque informático, éstas son: reconocimiento (reconnaissance), exploración (scanning), obtención de acceso (gaining access), mantener el acceso (maintaining Access), cubrir huellas (covering tracks).

A continuación una breve explicación de cada fase:

- **Reconocimiento:** Obtener información relevante de una potencial víctima de ataque, que puede ser una persona o una empresa.
- **Exploración:** Con la información obtenida en la fase anterior, se intenta obtener datos más específicos como por ejemplo direcciones de red (IP), nombres de equipo (hosts), datos de autenticación (usuarios y claves), en general cualquier información que permita establecer un primer acceso a la

red de la víctima.

- **Obtención de acceso:** Esta fase es donde se comienza a materializar el ataque. Para el efecto se intenta determinar las vulnerabilidades y fallas de seguridad de los sistemas para poder explotarlas y obtener acceso.
- **Mantener el acceso:** Una vez que el atacante ha logrado tener acceso intentará mantenerlo todo el tiempo que le sea posible para lo cual utilizará programas (Software) malicioso que facilite su objetivo.
- **Cubriendo huellas:** Si hay algo de lo que se preocupan los atacantes es eliminar cualquier rastro que ayude al personal encargado de la seguridad informática o administradores de red detectar su acceso o cuales fueron las vulnerabilidades que aprovechó para obtener el mismo.

Seguridad de la información.- En general la seguridad de la información establece 3 aspectos principales que debe cumplir: confidencialidad, integridad y disponibilidad. Enríquez, José (2011: Internet) añade un aspecto adicional que lo denomina irrefutabilidad. A continuación se hace una breve explicación de cada uno de ellos:

- **Confidencialidad:** La información no puede o debe ser divulgada por ningún medio y que además debe ser conocida únicamente por quien le pertenece. Un claro ejemplo son los datos de autenticación y autorización (usuarios y contraseñas)
- **Integridad:** Este aspecto se refiere a que la información a la que se accede o que es transmitida no sea alterada hasta llegar a su destino. Es decir que quien la va a leer puede estar seguro que la información confiable y no ha tenido modificaciones.
- **Disponibilidad:** Se relaciona con el hecho de que un recurso (por ejemplo: información, red, impresora, internet) sea accesible en el momento que se requiera hacer uso de la misma.
- **Irrefutabilidad:** Este concepto se refiere a que quien hizo uso o modificó información no pueda negar haber realizado dicha acción.

Gestión de Riesgos de la información.- ISACA (2013) considera la gestión de riesgos de la información como:

> ...el proceso de identificar vulnerabilidades y amenazas a los recursos de información utilizados por una organización para alcanzar sus

> objetivos, y decidir cuales controles, si alguno, deben aplicar para reducir el riesgo a un nivel aceptable, basado en el valor del recurso de información para la organización

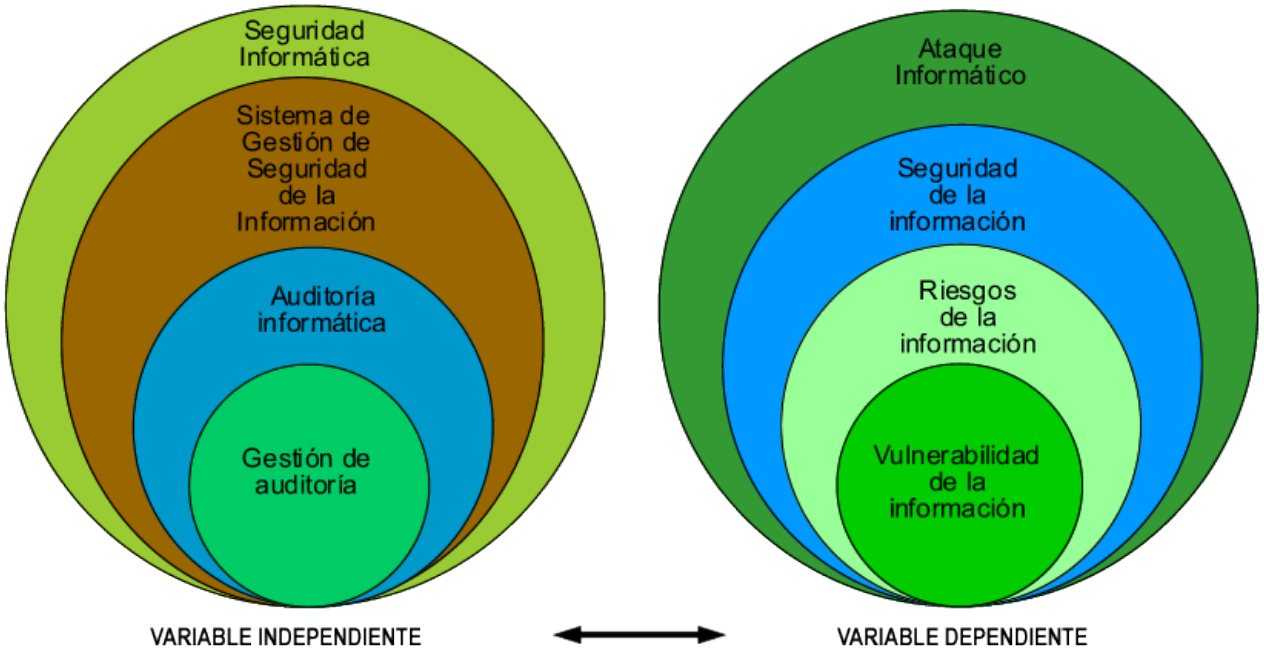
Vulnerabilidad de la información.- La vulnerabilidad de la información es comprometer la confidencialidad, integridad y/o disponibilidad de la información. La norma ISO 27005 define la vulnerabilidad como una debilidad de un activo o grupo de activos que puede ser explotado por una o más amenazas, se puede identificar vulnerabilidades en forma cualitativa de acuerdo a la experiencia del experto en seguridades, usando un escenario de pruebas o utilizando software de intrusión, de tal forma que al identificar las mismas sea posible tomar los correctivos del caso.

Markus (2009) en su blog menciona; respecto de la vulnerabilidad de la información, la siguiente definición:

> La Vulnerabilidad es la capacidad, las condiciones y características del sistema mismo (incluyendo la entidad que lo maneja), que lo hace susceptible a amenazas, con el resultado de sufrir algún daño. En otras palabras, es la capacitad y posibilidad de un sistema de responder o reaccionar a una amenaza o de recuperarse de un daño
>
> También menciona que las vulnerabilidades; dependiendo de su origen se pueden clasificar en las siguientes:
>
> - Ambiental/Física: Desastres naturales, ubicación, capacidad técnica, materiales, etc.
> - Económica: Escasez y mal manejo de recursos
> - Socio-Educativa: Relaciones, comportamientos, métodos, conductas, etc.
> - Institucional/Política: Procesos, organización, burocracia, corrupción, autonomía.

2.4.2. Gráficos de inclusión interrelacionados

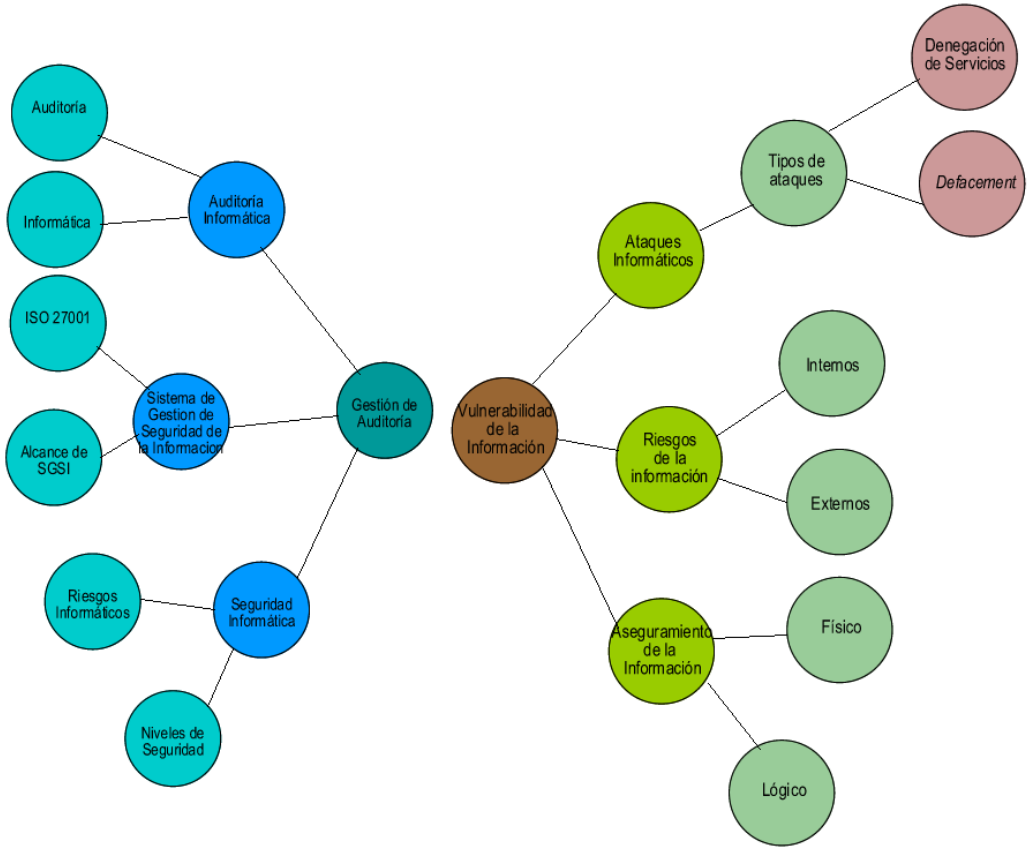
- Superordinación conceptual



Elaborado por: Henry Vivanco (2014)

Figura 2: Superordinación conceptual

- Subordinación conceptual



Elaborado por: Henry Vivanco (2014)

Figura 3: Subordinación conceptual.

2.5. HIPÓTESIS

La no aplicación de gestión de auditoría de acceso a información compartida en red es la principal causa de vulnerabilidad de información en la Cooperativa de Ahorro y Crédito Coca Ltda.

2.6. SEÑALAMIENTO VARIABLES DE LA HIPOTESIS

- **Variable independiente**: Gestión de auditoría
- **Variable dependiente**: Vulnerabilidad de la información
- **Unidad de observación**: Cooperativa de Ahorro y Crédito Coca Ltda.

CAPÍTULO III

METODOLOGÍA

3.1. ENFOQUE

Al comparar la metodología cuantitativa respecto de la cualitativa, Pita Fernández S. (2002) manifiesta lo siguiente: "La diferencia fundamental entre ambas metodologías es que la cuantitativa estudia la asociación o relación entre variables cuantificadas y la cualitativa lo hace en contextos estructurales y situacionales", más adelante manifiesta que "La investigación cuantitativa trata de determinar la fuerza de asociación o correlación entre variables, la generalización y objetivación de los resultados a través de una muestra para hacer inferencia a una población de la cual toda muestra procede".

Basado en lo anterior, el enfoque que predomina en la presente investigación es el cuantitativo que; entre otras herramientas que ofrece se encuentran la encuesta y la entrevista, mismas que fueron utilizadas para recabar información.

3.2. MODALIDAD BÁSICA DE LA INVESTIGACIÓN

3.2.1. Investigación de campo

Franco (2011)menciona que la investigación de campo es:

> el análisis sistemático de problemas en la realidad, con el propósito bien sea de describirlos, interpretarlos, entender su naturaleza y factores constituyentes, explicar sus causas y efectos, o predecir su ocurrencia, haciendo uso de métodos característicos de cualquiera de los paradigmas o enfoques de investigación conocidos o en desarrollo.

Además, la principal característica de la investigación de campo es que la información

se la obtiene de primera mano, directamente de las personas; en este caso particular, que están involucradas en el problema que la presente investigación solventó.

3.2.2. Investigación bibliográfica documental

Grajales (2000)en su documento explica que; "según Zorrilla (1993:43) La investigación documental es aquella que se realiza a través de la consulta de documentos (libros, revistas, periódicos, memorias, anuarios, registros, códices, constituciones, etc.)..."

Para la presente investigación fue necesario el realizar consultas en todas las fuentes documentales (físicas y electrónicas) que se pudo conseguir ya que siempre es necesario el conocer posibles investigaciones que se hayan realizado en torno a la presente.

3.2.3. Experimental

La investigación experimental consiste en la manipulación de una variable experimental no comprobada, en condiciones rigurosamente controladas, con el fin de describir de qué modo o por qué causa se produce una situación o acontecimiento en particular.

Se trata de un experimento porque precisamente el investigador provoca una situación para introducir determinadas variables de estudio manipuladas por él, para controlar el aumento o disminución de esa variable, y su efecto en las conductas observadas. El investigador maneja deliberadamente la variable experimental y luego observa lo que sucede en situaciones controladas.

3.3. NIVEL O TIPO DE INVESTIGACIÓN

3.3.1. Investigación exploratoria

Grajales (2000)respecto de la investigación exploratoria dice lo siguiente:

> Los estudios exploratorios nos permiten aproximarnos a fenómenos desconocidos, con el fin de aumentar el grado de familiaridad y contribuyen con ideas respecto a la forma correcta de abordar una investigación en particular. Con el propósito de que estos estudios

> no se constituyan en pérdida de tiempo y recursos, es indispensable aproximarnos a ellos, con una adecuada revisión de la literatura. En pocas ocasiones constituyen un fin en sí mismos, establecen el tono para investigaciones posteriores y se caracterizan por ser màs flexibles en su metodología, son más amplios y dispersos, implican un mayor riesgo y requieren de paciencia, serenidad y receptividad por parte del investigador. El estudio exploratorio se centra en descubrir.

Lo anterior respalda el hecho de que el nivel que más se utilizó en la presente investigación es justamente la exploración, ya que se hizo una minuciosa observación de las distintas particularidades que se pudieron determinar en torno al problema de investigación y que permitió a su vez encontrar una solución que disminuyó las consecuencias provocadas por éste.

3.3.2. Investigación descriptiva

Acerca de qué es investigación descriptiva Namakforoosh (2000) dice que "...es una forma de estudio para saber quién, dónde, cuándo, cómo y por qué del sujeto de estudio". Siendo así, este nivel de investigación ayudó a determinar el porcentaje de usuarios afectados por el problema objeto de estudio de la presente investigación.

3.3.3. Investigación asociación de variables (correlacional)

Referente a este tipo de investigación Grajales (2000) dice qué:

> Los estudios correlacionales pretender medir el grado de relación y la manera como interactúan dos o mas variables entre sí. Estas Relaciones se establecen dentro de una mismo contexto, y a partir de los mismos sujetos en la mayoría de los casos. En caso de existir una correlación entre variables, se tiene que, cuando una de ellas varía, la otra también experimenta alguna forma de cambio a partir de una regularidad que permite anticipar la manera cómo se comportará una por medio de los cambios que sufra la otra.

En esta investigación, este nivel permitió determinar el grado de relación existente entre la variable independiente y dependiente que fueron descritas en el capítulo anterior.

3.3.4. Investigación explicativa

Gross (2010) en su blog, respecto de la investigación explicativa dice que:

> Se encarga de buscar el porqué de los hechos mediante el establecimiento de Relaciones causa-efecto. En este sentido, los estudios explicativos pueden ocuparse tanto de la determinación de las causas (investigación postfacto), como de los efectos (investigación experimental), mediante la prueba de hipótesis. Sus resultados y conclusiones constituyen el nivel más profundo de conocimientos.

Este nivel permitió detallar claramente cada uno de los aspectos que fueron cubiertos en el transcurso de la investigación, especialmente aquellos que son la base de la misma. De igual manera, facilitó las herramientas necesarias para poder explicar los efectos que fueron reducidos y que tenían como origen el problema objeto de la investigación.

3.4. POBLACIÓN Y MUESTRA

3.4.1. Población

Para la presente investigación, se tomó como población a todo el personal administrativo y operativo que labora en la oficina matriz de la Cooperativa de Ahorro y Crédito Coca Ltda. A continuación se detallan los nombres y el cargo que desempeña cada uno de los empleados.

Tabla 2: Nómina oficial de empleados de la oficina matriz de Cooperativa de Ahorro y Crédito Coca Ltda.

No.	Nombres	Cargo
1	Aldrin Cuvi	Gerente General
2	Alba Calero	Asistente Gerencia
3	Mayra Cedeño	Contadora General
4	Kathetine Vera	Auxiliar Contabilidad
5	Paola Cabezas	Auxiliar Contabilidad
6	Mayra Tenorio	Auditoría interna
7	Katiuska Valladares	Jefe Crédito
8	Christian Vargas	Oficial Crédito
9	Rita Llori	Oficial Crédito
10	Jenny Rogel	Oficial Crédito
11	Isabel Casa	Oficial Crédito
14	Viviana Olaya	Talento Humano
12	Mónica Mayalica	Atención Cliente
13	Juan Román	Jefe Cajas
15	Gina González	Cajera
16	Emma Valarezo	Cajera

Fuente: Departamento Talento Humano
Elaborado por: Henry Vivanco (2014)

3.4.2. Muestra

Dado que el número de elementos que comprenden la población es reducido no es necesario obtener una muestra por lo que en la presente investigación se trabajó con toda la población.

3.5. OPERACIONALIZACIÓN DE VARIABLES

Betancur López (2000)en su trabajo dice que:

> Una variable es operacionalizada con el fin de convertir un concepto abstracto en uno empírico, susceptible de ser medido a través de la aplicación de un instrumento. Dicho proceso tiene su importancia en la posibilidad que un investigador poco experimentado pueda tener la seguridad de no perderse o cometer errores que son frecuentes en un proceso investigativo, cuando no existe relación entre la variable y la forma en que se decidió medirla, perdiendo así LA VALIDEZ (grado en que la medición empírica representa la medición conceptual). La

> precisión para definir los términos tiene la ventaja de comunicar con exactitud los resultados.

Para Ferrer (2010) en cambio “Es un proceso que se inicia con la definición de las variables en función de factores estrictamente medibles a los que se les llama indicadores”. Así también menciona qué:

> La Operacionalización de las variables está estrechamente vinculada al tipo de técnica o metodología empleadas para la recolección de datos. Estas deben ser compatibles con los objetivos de la investigación, a la vez que responden al enfoque empleado, al tipo de investigación que se realiza. Estas técnicas, en líneas generales, pueden ser cualitativas o cuantitativas.

Ávila Baray (2006)dice qué:

> Operacionalizar es definir las variables para que sean medibles y manejables, significa definir operativamente el PON. Un investigador necesita traducir los conceptos (variables) a hechos observables para lograr su medición. Las definiciones señalan las operaciones que se tienen que realizar para medir la variable, de forma tal, que sean susceptibles de observación y cuantificación

En la presente investigación la Operacionalización se utilizó para definir los indicadores que permitieron probar cuan relacionadas se encuentran las variables objeto de estudio que se establecieron en el capítulo 2.

3.5.1. Operacionalización de la variable independiente

Tabla 3: Operacionalización DE LA VARIABLE INDEPENDIENTE

VARIABLE INDEPENDIENTE: Gestión de auditoría				
CONCEPTUALIZACIÓN	CATEGORIAS	INDICADORES	ITEMS BÁSICOS	TÉCNICAS E INSTRUMENTOS DE RECOLECCIÓN DE información
La gestión de auditoría de acceso a información compartida en red se puede conceptualizar como: Utilizar los archivos de auditoría de acceso a información compartida; generados por el sistema operativo, y almacenarlos dentro de un repositorio estructurado que permita mostrar dicha información en un formato que sea fácilmente entendible	-Autenticación de Usuarios -Administración de usuarios -Compartir información entre usuarios -Acceso a información compartida -Perdida de información -Respaldo de información	- Número de usuarios de red -Número de equipos en red -Cantidad de carpetas compartidas -Información compartida en red que no necesita estarlo -Porcentaje de información compartida a la que deben tener acceso los usuarios -Pérdida de información	¿Existe un método para la autenticación de usuarios que acceden a la red de datos? ¿Existen políticas para la administración de usuarios (creación y eliminación)? ¿Existen políticas para compartir información? ¿Cuenta con políticas que especifique como proceder cuando un usuario necesita acceder a información compartida? ¿Tienen políticas de respaldo? ¿Cuentan con plan de contingencia y recuperación de desastres?	Encuestas a personal operativo y administrativo Entrevista con cuestionario (Ver Anexo 3) Observación a todos los computadores del personal operativo y administrativo Observación con lista de cotejo (Anexo 4)

Fuente: Marco Teórico
Elaborado por: Henry Vivanco

3.5.2. Operacionalización de la variable dependiente

Tabla 4: Operacionalización DE LA VARIABLE DEPENDIENTE

VARIABLE DEPENDIENTE: Vulnerabilidad de la información				
CONCEPTUALIZACIÓN	CATEGORIAS	INDICADORES	ITEMS BÁSICOS	TÉCNICAS E INSTRUMENTOS DE RECOLECCIÓN DE información
La vulnerabilidad de la información se puede conceptualizar como: El riesgo de que cualquiera de los aspectos relacionados a la seguridad de la información esté expuesto a ataques, sean estos internos o externos.	- información compartida en red - Bloqueo de equipo con contraseñas - Amenazas lógicas - Amenazas físicas	- Número de carpetas compartidas en red por equipo - Número de equpos a los que se puede acceder sin contraseña - Número de equipos con contraseña en blanco - Cantidad de contraseñas fáciles de deducir - Cantidad de equipos que cuentan con regulador/UPS - Cantidad de equipos fáciles de sustraer	¿Existe restricción de acceso a la información compartida (permisos lectura/escritura) ¿Cuántos computadores tienen contraseña? ¿Cuántos equipos tienen contraseña en blanco? ¿Cuántos equipos tienen contraseña relacionada con la información del usuario (identificación, nombre, apellido, nombre de hijo(a))? ¿Cuántos equipos cuentan con regulador de voltaje/UPS? ¿Cuántos servidores se encuentran protegidos por UPS? ¿Cuántos equipos tienen seguridades para evitar robo?	Encuestas a personal operativo y administrativo Entrevista con cuestionario (Ver Anexo 5) Observación a todos los computadores del personal operativo y administrativo Observación con lista de cotejo (Ver Anexo 6)

Fuente: Marco Teórico.
Elaborado: Henry Vivanco (2014)

3.6. RECOLECCIÓN DE LA INFORMACIÓN

Metodológicamente; para **Herrera et al. (2004, pág. 174-178 y 183-185)**, la construcción de la información se opera en dos fases: plan para la recolección de información y plan para el procesamiento de información.

3.6.1. Plan para la recolección de información

Este plan contempla estrategias metodológicas requeridas por los objetivos (ver Pág. 7) e hipótesis de investigación (ver Pág. 17), de acuerdo con el enfoque escogido que para el presente estudio es predominantemente cuantitativo (ver Pág. 18), considerando los siguientes elementos:

- **Definición de los sujetos:** En la presente investigación, los sujetos que participaron en la investigación fueron el personal administrativo y operativo de la oficina matriz de la Cooperativa de Ahorro y Crédito Coca Ltda. así como cada una de las computadoras que les han sido asignadas para realizar sus labores diarias. (ver Pág. 22).
- **Selección de las técnicas a emplear en el proceso de recolección de información:** Para la obtención de la información se utilizó las técnicas de encuesta dirigida al personal operativo, entrevista dirigida al personal administrativo y observación en lo que se refirió a la revisión de los computadores que utiliza cada funcionario que forma parte de la población detallada anteriormente (ver Pág. 24, 25).
- **Instrumentos seleccionados o diseñados de acuerdo con la técnica escogida para la investigación.** En virtud de la información que se deseaba recabar, los instrumentos a que se utilizaron son: cuestionario (para el caso de la entrevista), encuesta y fichas (lista de cotejo) para lo que corresponde a la observación. (ver Pág. 24, 25) y (ver Anexos 4, 5 y 6)
- **Explicitación de procedimientos para la recolección de información.**
  - **Cuestionario:** Sampieri et al. (1998) respecto de este procedimiento de recolección de información manifiesta que "Es el método que utiliza un instrumento o formulario impreso, destinado a obtener respuestas sobre el problema en estudio y que el consultado llena por sí mismo".
  - **Entrevista:** Cruz Jaramillo (2011) respecto del concepto de entrevista

menciona que:

> La define el Prof. García Ferrado como "una investigación realizada sobre una muestra de sujetos representativa de un colectivo mas amplio, utilizando procedimientos estandarizados de interrogación con intención de obtener mediciones cuantitativas de una gran variedad de características objetivas y subjetivas de la población"

- **Encuesta:** en la fuente antes citada, respecto de la encuesta dice que:

  > Segú la definición de Jose A. Avilez M.(Internet: 2003) en su monografía Recolección de Datos "Las entrevistas se utilizan para recabar información en forma verbal, a través de preguntas que propone el analista. Quienes responden pueden ser gerentes o empleados, los cuales son usuarios actuales del sistema existente, usuarios potenciales del sistema propuesto o aquellos que proporcionarán datos o serán afectados por la aplicación propuesta. El analista puede entrevistar al personal en forma individual o en grupos algunos analistas prefieren este método a las otras técnicas que se estudiarán más adelante. Sin embargo, las entrevistas no siempre son la mejor fuente de datos de aplicación"

- **Lista de cotejo:** En el documento Estrategias de resolución de problemas de la FUNDACION DE ESTUDIOS SUPERIORES DR. PLACIDO MARIN (sf) respecto de la lista de cotejo explica que "es un instrumento de observación que permite registrar el grado, de acuerdo con una escala determinada, en el cual un comportamiento, una habilidad o una actitud determinada es desarrollada por la o el estudiante"

- **Observación:** Para Hernández Sampieri et al. (2010)"La observación consiste en el registro sistemático, válido y confiable de comportamientos o conducta manifiesta. Puede utilizarse como instrumento de medición en muy diversas circunstancias."

En la presente investigación la encuesta estuvo dirigida al personal operativo de la Cooperativa de Ahorro y Crédito Coca Ltda. en tanto que la entrevista se la realizó al señor Econ. Aldrin Cuvi, Gerente General de dicha institución financiera.

La observación se la utilizó para establecer las amenazas y vulnerabilidades

a las que se encuentra expuesta la información compartida en los equipos de cada uno de los funcionarios operativos y administrativos de la Cooperativa de Ahorro y Crédito Coca Ltda.

En esta investigación, los cuestionarios sirvieron para realizar las encuestas al personal operativo y administrativo y también para la entrevista que se realizó al Gerente General de la Cooperativa de Ahorro y Crédito Coca Ltda. En lo que respecta a las listas de cotejo, contiene los ítems que ayudaron en la observación que se realizó en cada uno de los equipos de los funcionarios operativos y administrativos.

3.7. PROCESAMIENTO Y ANÁLISIS

3.7.1. Plan de procesamiento de información

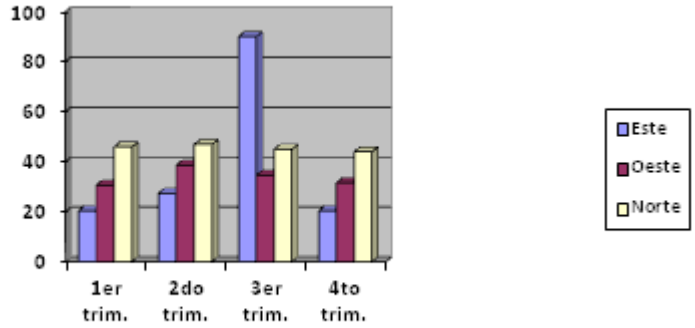
- **Revisión crítica de la información recogida:** Es decir limpieza de información defectuosa: contradictoria, incompleta, no pertinente, etc.
- **Repetición de la recolección:** En ciertos casos individuales, para corregir fallas de contestación.
- **Tabulación o cuadros según variables de cada hipótesis, manejo de información, estudio estadístico de datos para presentación de resultados:** Ejemplo de tabla a ser utilizada para la cuantificación de los resultados obtenidos con los instrumentos de recolección de información primaria (de campo).

Tabla 5: Título con la idea principal de la pregunta

opciones	CANTIDAD	FRECUENCIA, %
SI		
NO		
TOTAL		

Fuente: Entrevista, encuesta, observación
Elaborado por: Henry Vivanco (2014)

Figura 4: Ejemplo de figura a ser utilizada



Fuente: Investigación de campo, encuestas
Elaborado por: Henry Vivanco (2014)

- **Representaciones gráficas:** Ejemplo de figura a ser utilizada para la presentación visual porcentual de los resultados cuantificados en la tabla anterior.

3.7.2. Plan de análisis e interpretación de resultados

- **Análisis de los resultados estadísticos.** Destacando tendencias o Relaciones fundamentales de acuerdo con los objetivos e hipótesis (lectura de datos).
- **Interpretación de los resultados.** Con apoyo del marco teórico, en el aspecto pertinente.
- **Comprobación de hipótesis.** Explicar el posible método estadístico de comprobación de hipótesis (H1) a ser utilizado en el desarrollo de la investigación, con sus respectivos pasos, incluyendo la cita de texto y su utilidad, teniendo en cuenta el enfoque (cuantitativo o cualitativo) de la hipótesis de trabajo; así como, del tamaño de la población (finita o infinita, N $\leq 100 \geq$ N) y/o muestra.
- **Establecimiento de conclusiones y recomendaciones.** Explicación del procedimiento de obtención de las conclusiones y recomendaciones. Las conclusiones se derivan de la ejecución y cumplimiento de los objetivos específicos de la investigación. Las recomendaciones se derivan de las conclusiones establecidas. A más de las conclusiones y recomendaciones derivadas de los objetivos específicos, si pueden establecerse más conclusiones y recomendaciones propias de la investigación.

Tabla 6: Relación de objetivos específicos, conclusiones y recomendaciones

OBJETIVOS ESPECÍFICOS	**CONCLUSIONES**	**recomendaciones**
Establecer políticas para la compartición de información en red para reducir el nivel de vulnerabilidad de la misma		
Definir adecuadas políticas de auditoría de acceso a información compartida en red para evidenciar accesos no autorizados a la misma		
Proponer el diseño de un sistema de gestión de auditoría de acceso a información compartida en red que permita obtener evidencia de intentos de acceso no autorizado y posibles alteraciones a la misma		

Fuente: Investigación de campo
Elaborado por: Henry Vivanco (2014)

CAPÍTULO IV

ANÁLISIS E INTERPRETACIÓN DE RESULTADOS

Los datos obtenidos a través de la encuesta sobre "Gestión de auditoría de acceso a información compartida en red y su incidencia en la vulnerabilidad de la información en la Cooperativa de Ahorro y Crédito Coca Ltda." fueron sometidos al respectivo análisis para lo que se aplicó conocimientos de estadística descriptiva siguiendo los siguientes pasos:

1. Tabulación de datos pregunta por pregunta
2. Elaboración de las respectivas tablas y cuadros estadísticos
3. Cálculo de la media aritmética para la respectiva interpretación de los datos
4. Elaboración de graficas estadísticas de los resultados obtenidos.

4.1. ANÁLISIS DE LOS RESULTADOS

Los datos obtenidos con la aplicación de la encuesta a los empleados de la Cooperativa de Ahorro y Crédito Coca Ltda. fueron tabulados permitiendo así realizar el respectivo análisis e interpretación de cada pregunta lo cual dejó en evidencia el alto nivel de vulnerabilidad que tiene la información que actualmente cada uno de los empleados tiene compartida en la red. Los datos tabulados han sido representados en gráficos estadísticos de barras con la ayuda del programa Microsoft Excel 2007.

4.2. INTERPRETACIÓN DE LOS RESULTADOS

A continuación se detalla el análisis e interpretación de los resultados que se obtuvieron de la tabulación de la encuesta realizada a cada uno de los empleados.

4.2.1. Encuesta realizada al personal operativo y administrativo

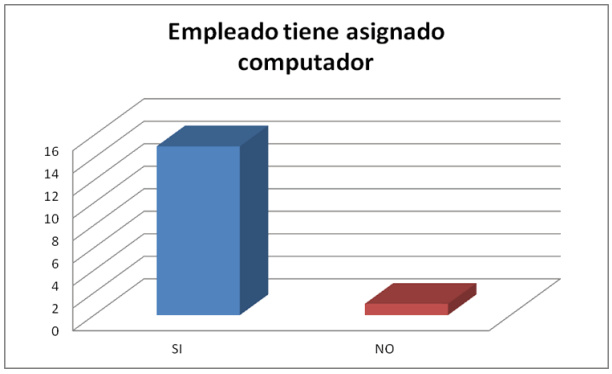
Pregunta 1: ¿Tiene asignado un computador para realizar sus actividades?

Tabla 7: Empleado tiene asignado un computador

opciones	CANTIDAD	FRECUENCIA, %
SI	15	93.75 %
NO	1	6.25 %
TOTAL	16	100 %

Fuente: Encuesta
Elaborado por: Henry Vivanco (2014)

Figura 5: Empleado tiene asignado un computador



Fuente: Encuesta
Elaborado por: Henry Vivanco (2014)

Análisis e interpretación:

El 93.75 % (15) de los empleados tiene asignado un computador para realizar sus actividades diarias referentes al trabajo mientras que el 6.25 % (1) aún no le han asignado un computador.

Lo anterior evidencia que en general cada empleado tiene su propio computador para poder realizar sus tareas diarias. El usuario que no cuenta con computador es porque recién empezaba a trabajar.

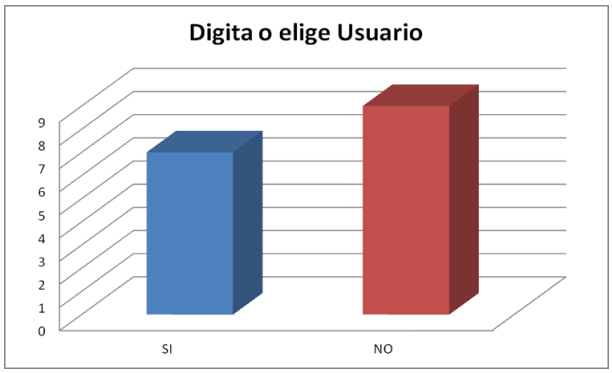
Pregunta 2: ¿Es necesario digitar o seleccionar un usuario para poder utilizar su computador?

Tabla 8: Digita o seleCCIÓNa un usuario para poder utilizar el computador

opciones	CANTIDAD	FRECUENCIA, %
SI	7	43.75 %
NO	9	56.25 %
TOTAL	16	100 %

Fuente: Encuesta
Elaborado por: Henry Vivanco (2014)

Figura 6: Digita o seleCCIÓNa un usuario para poder utilizar el computador



Fuente: Encuesta
Elaborado por: Henry Vivanco (2014)

Análisis e interpretación:

El 43.75 % (7) de los empleados debe digitar o elegir un usuario antes de poder empezar a utilizar su computador en tanto que el restante 56.25 % no necesita hacerlo.

Lo anterior da a notar que cualquier persona; sea o no empleado de la Cooperativa, puede utilizar la mayoría de los computadores sin una previa autorización.

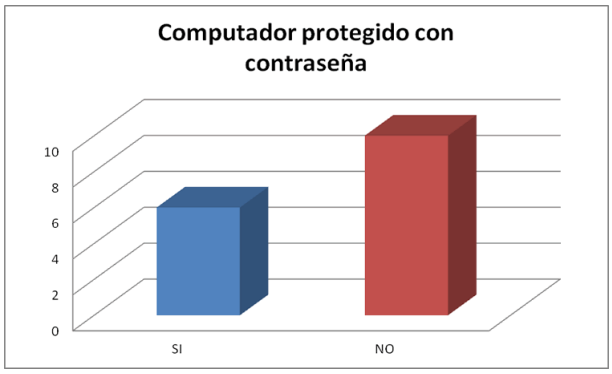
Pregunta 3: ¿Está protegido su computador con contraseña?

Tabla 9: Computador protegido con contraseña

opciones	CANTIDAD	FRECUENCIA, %
SI	6	37.50 %
NO	10	62.50 %
TOTAL	16	100 %

Fuente: Encuesta
Elaborado por: Henry Vivanco (2014)

Figura 7: Computador protegido con contraseña



Fuente: Encuesta
Elaborado por: Henry Vivanco (2014)

Análisis e interpretación:

El 37.50 % (6) de los computadores se encuentran protegidos con contraseña mientras que el 62.50 % restante no.

Lo anterior deja al descubierto que cualquier persona; sea o no empleado de la Cooperativa, con solo hacer un clic puede desbloquear la mayoría de los equipos y tener acceso total a la información que en éstos se encuentra almacenada.

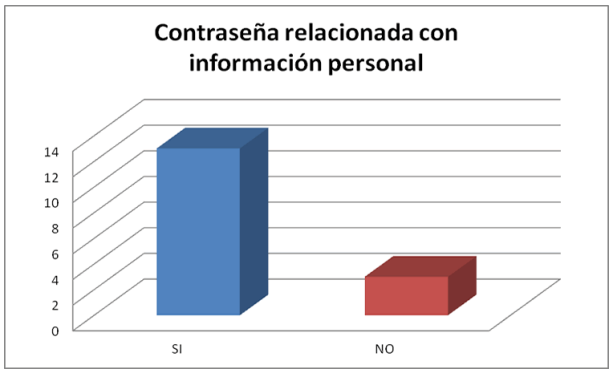
Pregunta 4: ¿La contraseña que utiliza es fácil de descifrar o adivinar?

Tabla 10: Contraseña relacionada con información personal (Iniciales, identificación, fecha de cumpleaños,etc)

opciones	CANTIDAD	FRECUENCIA, %
SI	13	81.25 %
NO	3	18.75 %
TOTAL	16	100 %

Fuente: Encuesta
Elaborado por: Henry Vivanco (2014)

Figura 8: Contraseña relacionada con información personal (Iniciales, identificación, fecha de cumpleaños,etc)



Fuente: Encuesta
Elaborado por: Henry Vivanco (2014)

Análisis e interpretación:

Las contraseñas del 81.25 % (13) de los empleados está relacionada con su información personal, como por ejemplo: iniciales, identificación, fecha de cumpleaños que el restante 18.75 % (3) de las contraseñas no.

Queda en evidencia el alto nivel de vulnerabilidad de los equipos que utilizan los empleados ya que sus contraseñas son fáciles de descifrar.

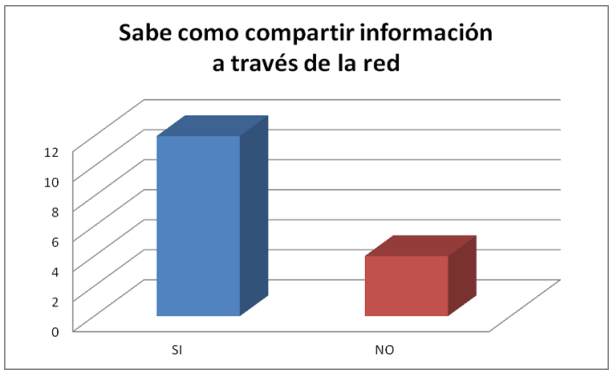
Pregunta 5: ¿Sabe Usted como compartir información con otros usuarios a través de la red?

Tabla 11: Sabe como compartir información

opciones	CANTIDAD	FRECUENCIA, %
SI	12	75.00 %
NO	4	25.00 %
TOTAL	16	100 %

Fuente: Encuesta
Elaborado por: Henry Vivanco (2014)

Figura 9: Sabe como compartir información a través de la red



Fuente: Encuesta
Elaborado por: Henry Vivanco (2014)

Análisis e interpretación:

El 75.00 % de los empleados sabe como compartir información a través de la red. El 25 % restante no sabe como hacerlo.

En esta tabla se puede apreciar que un gran porcentaje de los empleados sabe como compartir información a través de la red de datos.

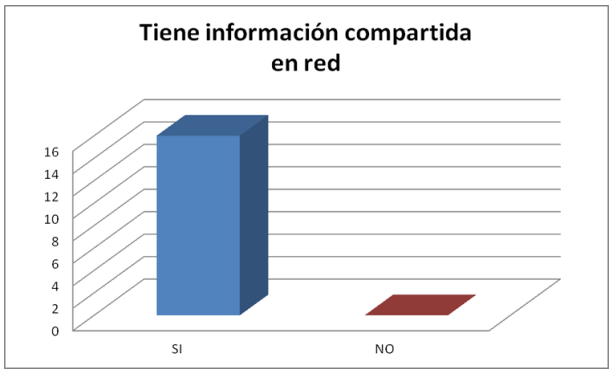
Pregunta 6: ¿Tiene información compartida con otros usuarios a través de la red?

Tabla 12: Tiene información compartida en red

opciones	CANTIDAD	FRECUENCIA, %
SI	16	100.00 %
NO	0	0.00 %
TOTAL	16	100 %

Fuente: Encuesta
Elaborado por: Henry Vivanco (2014)

Figura 10: Tiene información compartida en red



Fuente: Encuesta
Elaborado por: Henry Vivanco (2014)

Análisis e interpretación:

El 100 % de los empleados tiene información compartida en red.

Se puede apreciar que absolutamente todos los empleados de la Cooperativa tienen información disponible para el acceso a través de la red.

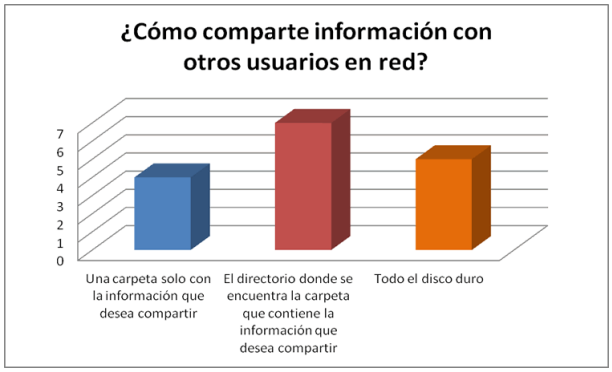
Pregunta 7: ¿Cómo comparte información con otros usuarios a través de la red?

Tabla 13: ¿Cómo comparte la información con otros usuarios a través de la red?

opciones	CANTIDAD	FRECUENCIA, %
Una carpeta solo con la información que desea compartir	4	25.00 %
El directorio donde se encuentra la carpeta que contiene la información que desea compartir	7	43.75 %
Todo el disco duro	5	31.25 %
TOTAL	16	100 %

Fuente: Encuesta
Elaborado por: Henry Vivanco (2014)

Figura 11: ¿Cómo comparte información con otros usuarios en red?



Fuente: Encuesta
Elaborado por: Henry Vivanco (2014)

Análisis e interpretación:

El 25 % de los empleados comparte solo la información que desea poner en red, el 43.75 % comparte toda la carpeta donde se encuentra la información y el 31.25 % comparte toda la información del disco duro.

La mayoría de los empleados de la Cooperativa da acceso a través de la red a más información de la que desea que sus compañeros tengan acceso. Esto eleva notablemente la vulnerabilidad de la información.

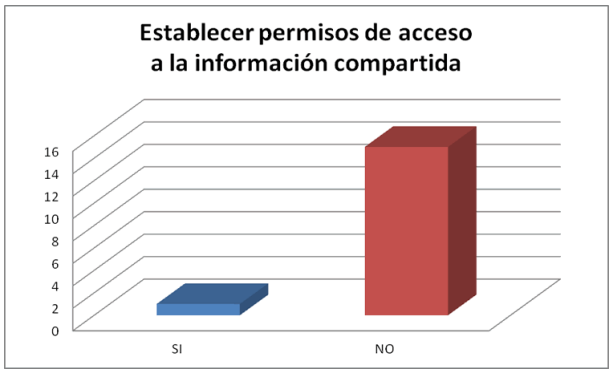
Pregunta 8: ¿Conoce que se puede establecer permisos de acceso a la información que comparte en red?

Tabla 14: Conoce que puede establecer permisos de acceso a la información compartida

opciones	CANTIDAD	FRECUENCIA, %
SI	1	6.25 %
NO	15	93.75 %
TOTAL	16	100 %

Fuente: Encuesta
Elaborado por: Henry Vivanco (2014)

Figura 12: Establecer permisos de acceso a la información compartida



Fuente: Encuesta
Elaborado por: Henry Vivanco (2014)

Análisis e interpretación:

El 93.75 % desconoce que se puede establecer permisos de acceso a la información compartida en red. El 6.25 % conoce que puede definir permisos de acceso a la información compartida en red.

Casi la totalidad de los empleados de la Cooperativa desconoce que puede establecer permisos de tal manera de restringir quienes podrían tener acceso a la información compartida en red.

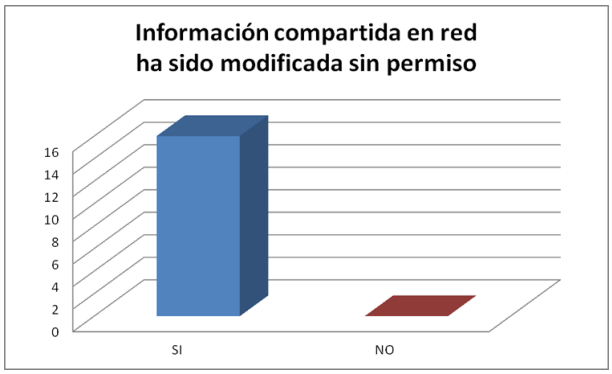
Pregunta 9: ¿En alguna ocasión la información que compartió en red ha sido modificada sin su consentimiento?

Tabla 15: información compartida en red ha sido modificada sin permiso

opciones	CANTIDAD	FRECUENCIA, %
SI	16	100.00 %
NO	0	0.00 %
TOTAL	16	100 %

Fuente: Encuesta
Elaborado por: Henry Vivanco (2014)

Figura 13: información compartida en red ha sido modificada sin permiso



Fuente: Encuesta
Elaborado por: Henry Vivanco (2014)

Análisis e interpretación:

El 100 % de los empleados afirma que en algún momento la información que han compartido en red ha sido modificada sin su consentimiento.

Todos los empleados afirman que en algún momento la información que han compartido en red ha sido modificada sin su consentimiento.

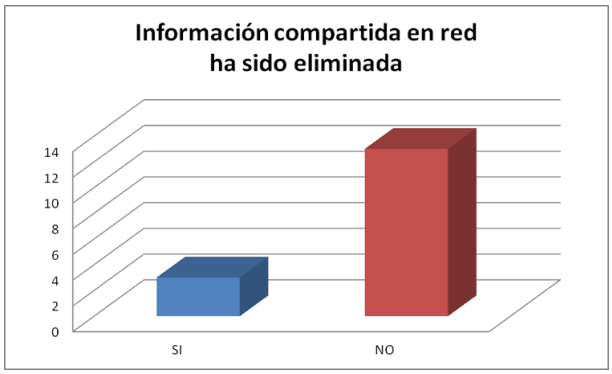
Pregunta 10: ¿Alguna vez han borrado su información compartida sin su consentimiento?

Tabla 16: información compartida en red ha sido eliminada

opciones	CANTIDAD	FRECUENCIA, %
SI	3	18.75 %
NO	13	81.25 %
TOTAL	16	100 %

Fuente: Encuesta
Elaborado por: Henry Vivanco (2014)

Figura 14: información compartida en red ha sido eliminada



Fuente: Encuesta
Elaborado por: Henry Vivanco (2014)

Análisis e interpretación:

El 18.75 % de los empleados afirma que en algún momento la información que han compartido en red ha sido eliminada sin su consentimiento en tanto que el restante 81.25 % manifiesta no haber tenido este inconveniente.

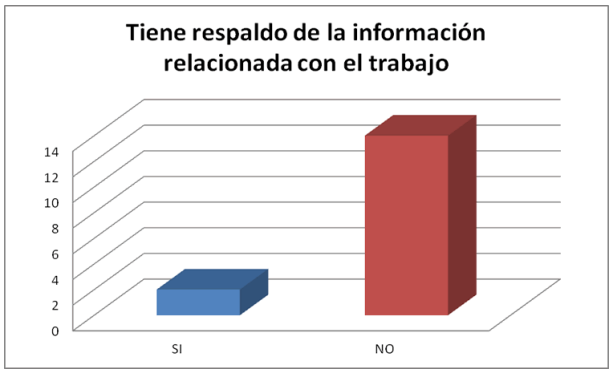
Pregunta 11: ¿Tiene un respaldo de su información relacionada a las tareas que a diario realiza como parte de su trabajo?

Tabla 17: Tiene respaldo de la información relacionada con el trabajo

opciones	CANTIDAD	FRECUENCIA, %
SI	2	12.50 %
NO	14	87.50 %
TOTAL	16	100 %

Fuente: Encuesta
Elaborado por: Henry Vivanco (2014)

Figura 15: Tiene respaldo de la información relacionada con el trabajo



Fuente: Encuesta
Elaborado por: Henry Vivanco (2014)

Análisis e interpretación:

El 12.5 % de los encuestados afirma tener respaldo de su información el restante 87.50 % no tiene respaldos de su información.

Un gran porcentaje de empleados no posee un respaldo de la información que a diario utiliza para realizar sus actividades de trabajo. Estos constituye una gran vulnerabilidad a la información.

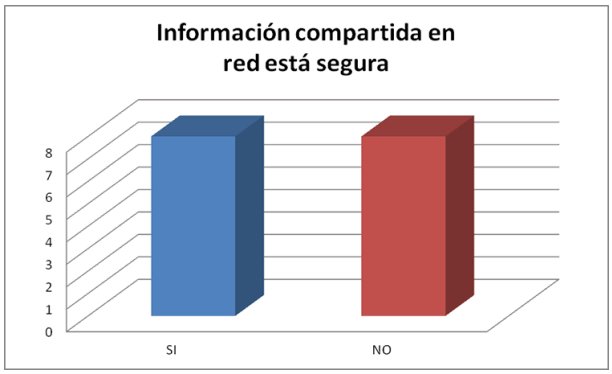
Pregunta 12: ¿Considera que es seguro compartir su información a través de la red?

Tabla 18: información compartida está segura

opciones	CANTIDAD	FRECUENCIA, %
SI	8	50.00 %
NO	8	50.00 %
TOTAL	16	100 %

Fuente: Encuesta
Elaborado por: Henry Vivanco (2014)

Figura 16: información compartida en red está segura



Fuente: Encuesta
Elaborado por: Henry Vivanco (2014)

Análisis e interpretación:

El 50 % de los encuestados afirma es seguro compartir su información en red mientras que el otro 50 % afirma que no es seguro.

La mitad de los encuestados desconoce o minimiza el riesgo y las vulnerabilidades a las que se encuentra expuesta la información que comparte a través de la red.

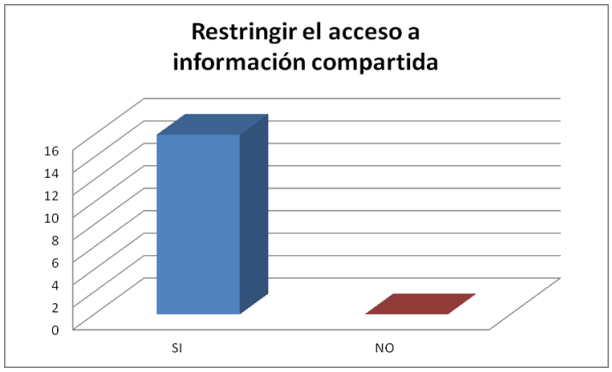
Pregunta 13: ¿Le gustaría restringir el acceso a la información compartida solo a aquellos compañeros a quienes elija?

Tabla 19: Restringir el acceso a la información compartida solo a usuarios seleccionados

opciones	CANTIDAD	FRECUENCIA, %
SI	16	100 %
NO	0	0.00 %
TOTAL	16	100 %

Fuente: Encuesta
Elaborado por: Henry Vivanco (2014)

Figura 17: Restringir el acceso a la información compartida solo a usuarios seleccionados



Fuente: Encuesta
Elaborado por: Henry Vivanco (2014)

Análisis e interpretación:

El 100 % de los encuestados quisiera poder restringir el acceso a la información compartida solo a aquellos que realmente necesitan acceso.

Todos los empleados quisieran poder restringir el acceso a la información que comparten en red solo con aquellos compañeros que necesitan tener acceso.

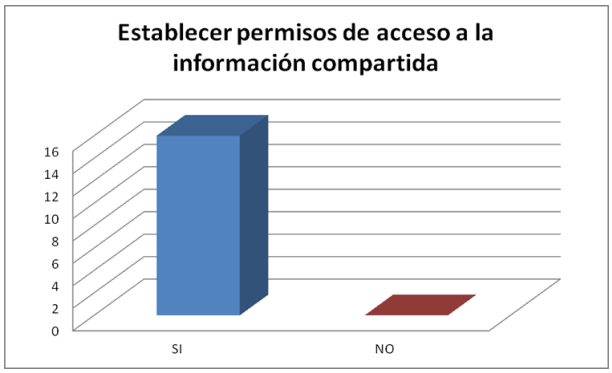
Pregunta 14: ¿Quisiera establecer las acciones que los usuarios pueden realizar en la información que comparte a través de la red?

Tabla 20: Establecer permisos de acceso a la información compartida

opciones	CANTIDAD	FRECUENCIA, %
SI	16	100 %
NO	0	0.00 %
TOTAL	16	100 %

Fuente: Encuesta
Elaborado por: Henry Vivanco (2014)

Figura 18: Establecer permisos de acceso a la información compartida



Fuente: Encuesta
Elaborado por: Henry Vivanco (2014)

Análisis e interpretación:

El 100 % de los encuestados manifiesta que le gustaría establecer permisos de acceso a las acciones que puedan realizar con la información compartida en red.

Todos los empleados quisieran poder establecer los permisos de acceso para determinar que usuario pueden realizar que acciones con la información que comparten en red

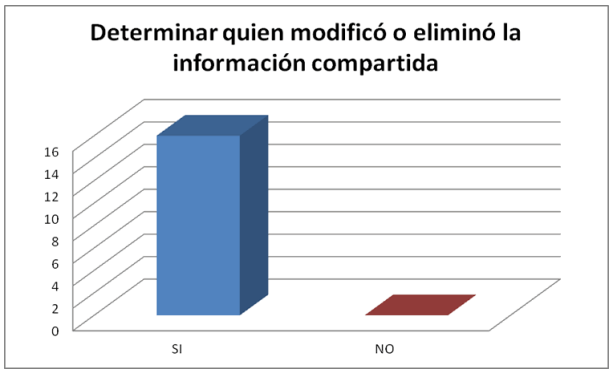
Pregunta 15: ¿Le gustaría conocer que usuario modificó o eliminó la información que ha compartido?

Tabla 21: Determinar quien modificó o eliminó la información compartida

opciones	CANTIDAD	FRECUENCIA, %
SI	16	100 %
NO	0	0.00 %
TOTAL	16	100 %

Fuente: Encuesta
Elaborado por: Henry Vivanco (2014)

Figura 19: Determinar quien modificó o eliminó la información compartida



Fuente: Encuesta
Elaborado por: Henry Vivanco (2014)

Análisis e interpretación:

El 100 % de los encuestados quisiera poder conocer quien eliminó o modificó la información compartida en red.

Todos los empleados quisieran saber en algún momento quien modificó o eliminó la información que tienen compartida en red

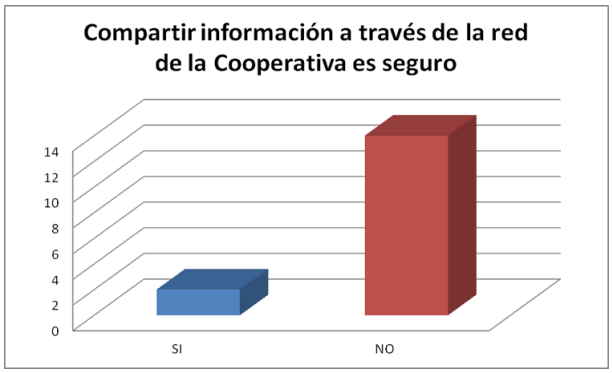
Pregunta 16: ¿Considera que compartir información en la red de datos de la Coooperativa es seguro?

Tabla 22: Compartir información a través de la red de la Cooperativa es seguro

opciones	CANTIDAD	FRECUENCIA, %
SI	3	18.75 %
NO	13	81.25 %
TOTAL	16	100 %

Fuente: Encuesta
Elaborado por: Henry Vivanco (2014)

Figura 20: Compartir información a través de la red de la Cooperativa es seguro



Fuente: Encuesta
Elaborado por: Henry Vivanco (2014)

Análisis e interpretación:

El 18.75 % de los encuestados considera que es seguro compartir su información en la red el 81.25 % considera que no es seguro.

La mayoría de los empleados coincide en que el compartir información en la red de datos actual representa un gran riesgo para su información.

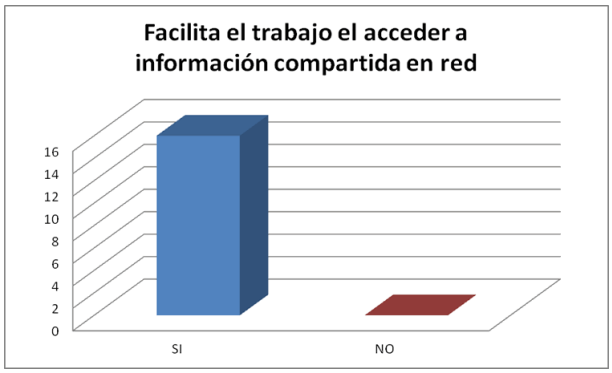
Pregunta 17: ¿Considera que es útil para realizar su trabajo el que pueda acceder a la información que comparten sus compañeros?

Tabla 23: Facilita el trabajo el acceder a información compartida en red

opciones	CANTIDAD	FRECUENCIA, %
SI	16	100 %
NO	0	0.00 %
TOTAL	16	100 %

Fuente: Encuesta
Elaborado por: Henry Vivanco (2014)

Figura 21: Facilita el trabajo el acceder a información compartida en red



Fuente: Encuesta
Elaborado por: Henry Vivanco (2014)

Análisis e interpretación:

El 100 % de los encuestados afirma que es útil; para realizar su trabajo, el poder acceder a información compartida en red.

La totalidad de los encuestados considera que el contar con información de sus compañeros disponible en red es útil para realizar su trabajo diario

4.2.2. Entrevista realizada al Gerente General

A continuación se resume las respuestas dadas por el señor Econ. Aldrin Cuvi, Gerente General de la Cooperativa de Ahorro y Crédito Coca Ltda.

Preguntas de la encuesta	**Respuestas obtenidas**
1. ¿Cuenta con un método de autenticación para el acceso a la red de datos?	No se tiene ningún método
2. ¿Ha definido políticas para la administración de usuarios (creación, asignación de permisos, baja de usuarios?	Políticas no, únicamente se crea usuarios para el uso del sistema transaccional
3. ¿Cuentan con procedimientos para compartir información en la red de datos?	No. Cada empleado comparte la información que considere en la red
4. Si la respuesta a la pregunta anterior es afirmativa, detalle de manera general ¿Cuál es el procedimiento establecido?	No responde
5. ¿Existe un solo repositorio para toda la información de usuarios? (Servidor de Archivos)	No. Cada empleado guarda su información en el computador que le ha sido asignado
6. ¿Cuenta con un método para determinar el acceso de usuarios y las acciones que realizan con la información que se encuentra compartida en red?	No. No existe manera de saber si un empleado accedió a la información de sus compañeros
7. ¿Cuentan con políticas para el respaldo de información sensible de los usuarios y la institución?	No. Unicamente se les ha asignado un disco externo a los jefes departamentales para que ahí guarden la información que consideren importante
8. ¿Cuenta con un espacio físico destinado exclusivamente para servidores y equipos de comunicación (Centro de Datos)?	Si, se adecuó un pequeño espacio en la planta baja para este fin.
9. ¿El acceso al Centro de Datos está restringido solo a personal autorizado?	Si. Aunque no como esperaría. En especial fuera del horario de trabajo.

Preguntas de la encuesta	Respuestas obtenidas
10. ¿Cuenta con un programa (software) antivirus?	Se ha instalado un antivirus gratuito en todos los equipos (AVG antivirus)
11. Para el uso de internet ¿Ha definido políticas de control de acceso a contenido?	En parte. Los jefes departamentales y jefes de agencia tienen acceso sin restricción.
12. ¿Cada funcionario de la Cooperativa tiene cuenta de correo institucional?	No. Únicamente los jefes departamentales y jefes de agencia.
13. ¿Se han definido políticas para el filtrado de archivos adjuntos que se envían o reciben a través de correo electrónico?	No. No existe este tipo de control.
14. ¿Le gustaría implementar las políticas y controles de acceso que durante la presente entrevista se han determinado que son deficientes?	Si, me gustaría que se implemente mayores controles y seguridades para evitar la pérdida de información.
15. De ser afirmativa la respuesta a la pregunta anterior ¿Luego de qué tiempo lo haría? (3 meses, 6 meses, 1 año, posterior a un año)	En el mediano plazo, mucho depende del monto de inversión que se requiera si acaso sobrepasa el valor destinado a él área de tecnología.

4.3. VERIFICACIÓN DE HIPÓTESIS

Consiste en evaluar la hipótesis entre sus dos variables categóricas, mediante la utilización del método estadístico denominado Ji-cuadrado.

Las variables que interviene en la hipótesis son:

- **Variable Independiente:** Gestión de auditoría de acceso a información compartida en red
- **Variable Dependiente:** Vulnerabilidad de la información

4.3.1. Formulación de la Hipótesis Nula (Ho) y la Hipótesis de Investigación (Hi)

4.3.1.1. Modelo Lógico

Ho:

La gestión de auditoría de acceso a información compartida en red no incide en la vulnerabilidad de la información de la Cooperativa de Ahorro y Crédito Coca Ltda.

Hi:

La gestión de auditoría de acceso a información compartida en red si incide en la vulnerabilidad de la información de la Cooperativa de Ahorro y Crédito Coca Ltda.

4.3.1.2. Modelo Estadístico

Considerando el hecho de que la población sobre la que se realizó la investigación es menor a 30, para la comprobación de la hipótesis se utilizó la prueba Ji-Cuadrado, cuya fórmula es la siguiente:

$$X^2 = \sum \left(\frac{(O - E)^2}{E} \right)$$

Donde:

X^2= Ji-cuadrado

$\sum$= Sumatoria

O = Frecuencia observada

E^2= Frecuencia esperada

4.3.1.3. Determinación del nivel de significancia o riesgo

La presente investigación tiene un nivel de confianza del 95 %, por lo tanto el nivel de significancia es del 5 %; es decir, $\alpha = 0.05$.

1. **Planteamiento de las hipótesis**

   Hi: $\mu_{inv} > \mu_t$

   Ho: $\mu_{inv} \leq \mu_t$

Donde:

μ_{inv}: Significa el valor numérico de Chi-cuadrado calculado o investigado

μ_t: Significa el valor numérico de Chi-cuadrado tabulado

2. **Elección de la prueba estadística**

   En lo referente a la elaboración de la matriz de tabulación se tomó en cuenta cinco preguntas del cuestionario de encuesta aplicado a los empleados de la Cooperativa de Ahorro y Crédito Coca Ltda., que son las que evidencian la vulnerabilidad de la información y el deseo por reducirla.

   Pregunta 6: ¿Tiene información compartida con otros usuarios en la red?

   Pregunta 8: ¿Conoce Usted que tiene la posibilidad de establecer permisos de acceso a la información que ha compartido?

   Pregunta 10: ¿La información que ha compartido en alguna ocasión ha sido eliminada sin que Usted lo sepa?

   Pregunta 12: ¿Considera que la información compartida con otros usuarios a través de la red está segura?

   Pregunta 15: ¿Le gustaría saber que usuario modificó o eliminó la información que ha compartido?

4.3.1.4. Frecuencia Observada

Tabla 25: Frecuencia Observada

	SI	NO	TOTAL
PREGUNTA 6	16	0	16
PREGUNTA 8	1	15	16
PREGUNTA 10	16	0	16
PREGUNTA 12	8	8	16
PREGUNTA 15	16	0	16
TOTAL	57	23	80

Fuente: Encuesta
Elaborado por: Henry Vivanco (2014)

4.3.1.5. Grados de libertad

Grados de libertad (gl) = (filas -1) * (columnas - 1)

gl = (5 - 1) * (2 - 1)

gl = (4) * (1)

gl = 4

El valor en la tabla de la distribución Chi-Cuadrado para 4 grados de libertad con un valor de significancia de 0.05 es de 9.49

4.3.1.6. Frecuencia Esperada

Tabla 26: Frecuencia Esperada

	SI	NO	TOTAL
PREGUNTA 6	11.4	4.46	16
PREGUNTA 8	11.4	4.46	16
PREGUNTA 10	11.4	4.46	16
PREGUNTA 12	11.4	4.46	16
PREGUNTA 15	11.4	4.46	16
TOTAL	57	23	80

Fuente: Encuesta
Elaborado por: Henry Vivanco (2014)

4.3.1.7. Tabla de cálculo Ji-cuadrado

Tabla 27: Tabla de Cálculo Ji-cuadrado

	SI	NO	TOTAL
PREGUNTA 6	1.856140351	4.6	6.456140351
PREGUNTA 8	9.487719290	23.51304348	33.00076278
PREGUNTA 10	1.856140351	4.46	6.456140351
PREGUNTA 12	1.014035088	2.513043478	3.527078566
PREGUNTA 15	1.856140351	4.46	6.456140351
TOTAL	16.07	39.83	55.9

Elaborado por: Henry Vivanco (2014)

4.3.1.8. Zona de aceptación/rechazo

El valor de Ji-cuadrado con 4 grados de libertad y con un nivel de significancia de 0.05 es de 9.49

4.3.1.9. Decisión

Contrastando el valor de Ji-cuadrado calculado (55.9) con el valor de Ji-cuadrado tabulado que se considera en la presente investigación (9.49), se determina que el valor calculado es mayor al valor tabulado por lo cual se acepta la Hipótesis de investigación y se descarta la hipótesis Nula. Con esto se confirma que "La gestión de auditoría de acceso a información compartida en red si incide en la vulnerabilidad de la información en la Cooperativa de Ahorro y Crédito Coca Ltda."

CAPÍTULO V

CONCLUSIONES Y RECOMENDACIONES

5.1. CONCLUSIONES

1. Como producto de la encuesta realizada se pudo evidenciar un alto nivel de vulnerabilidad de la información que se encuentra compartida en red puesto que todos los empleados disponen de información compartida en red sin ningún tipo de restricción o control sobre quienes pueden acceder y modificar la misma.
2. Con la comprobación de la hipótesis queda demostrado que es necesario la implementación de la infraestructura necesaria que permita gestionar de manera adecuada la auditoría de acceso a información compartida en red
3. Se hace imperativo establecer políticas y procedimientos que permitan disminuir los accesos y el uso no autorizado de la información que se encuentra compartida en red

5.2. RECOMENDACIONES

1. Utilizar herramientas informáticas que permitan establecer métodos adecuados para la creación, autenticación y autorización de usuarios para los empleados de la Cooperativa de Ahorro y Crédito Coca Ltda.
2. Establecer políticas adecuadas para la creación y mantenimiento (actualización de permisos, inhabilitación, eliminación) de usuarios para los empleados de la Institución
3. Establecer un repositorio único para la información que cada uno de los usuarios utiliza en sus labores diarias y que en este momento se encuentra dispersa y expuesta en cada uno de los computadores que utilizan, lo que disminuirá notablemente la vulnerabilidad de la misma

4. Establecer políticas adecuadas para compartir información en red, tanto en el repositorio central como en los computadores que cada empleado utiliza
5. Diseñar un sistema que permita una adecuada gestión de la auditoría de acceso a la información compartida en red en el repositorio centralizado

CAPÍTULO VI

PROPUESTA

6.1. DATOS INFORMATIVOS

6.1.1. Tema

"Sistema de gestión de auditoría de acceso a información compartida en red para la Cooperativa de Ahorro y Crédito Coca Ltda."

6.1.2. Datos informativos

La Cooperativa de Ahorro y Crédito Coca Ltda. es una institución de intermediación financiera regida por la Ley de Economía Popular y Solidaria. Fue un 19 de Enero de 1998 en la que un grupo de 15 personas lideradas por el Señor Diego Cabrera (+), quien fuera también el primer Gerente de la Institución. Se encuentra domiciliada en la ciudad de Francisco de Orellana (El Coca) en la Provincia de Orellana, en la intersección de las avenidas Quito y Bolívar.

La entidad ha tenido un crecimiento importante durante los 16 años de vida Institucional que han transurrido convirtiéndose en una de las más importantes y sólidas de Francisco de Orellana. Actualmente cuenta con dos agencias ubicadas una en el Cantón Loreto y otra en el Cantón Joya de los Sachas. Adicionalmente cuenta con ventanillas de servicio en los sectores de: Shushufindi, San Carlos, Dayuma y San Sebastián contribuyendo al desarrollo económico y social del norte de la amazonía ecuatoriana, a través de un equipo humano comprometido e innovador que brinda servicios financieros de calidad a sus socios y la comunidad en general.

- Su visión es

  Ser una institución financiera solvente y reconocida por la prestación de servicios financieros que satisfagan las necesidades de sus socios para mejorar su calidad de vida y contribuir al desarrollo de la comunidad.

- Sus valores son:
  - Solidaridad
  - Honestidad
  - Lealtad
  - Responsabilidad
  - Respeto
  - Confianza
  - Transparencia
- Los objetivos estratégicos que se han trazado actualmente son:
  - Incrementar la participacin en el mercado financiero de la amazonia ecuatoriana
  - Fortalecer la estructura de obligaciones con el público
  - Contribuir al desarrollo económico y social de la amazonía ecuatoriana
  - Incrementar el nivel de socios activos
  - Fortalecer la calidad de atención a los socios

6.2. ANTECEDENTES

Gracias a la confianza de sus socios, la Cooperativa ha permanecido en constante crecimiento lo que a su vez se ve reflejado en el incremento del personal y los servicios que debe brindar tanto a sus socios y en general a toda la comunidad.

Con el aumento de personal y la diversificación de servicios ha venido de la mano el incremento de equipos de cómputo así como también de hardware apropiado que de soporte a las aplicaciones que a diario se utilizan en la Cooperativa. No obstante ésto también acarrea la necesidad de contar con una mejor administración de seguridades que disminuyan el riesgo de pérdida, hurto o modificación de la información que

mantiene la Institución.

Actualmente la Cooperativa cuenta con un centro de datos relativamente pequeño pero a la vez sumamente importante. En este espacio físico se encuentran dos servidores de aplicaciones, un servidor de base de datos, central telefónica, equipos de última milla (2 routers), servidor de aplicación para cajero automático, servidor de mensajería interna y un servidor proxy/firewall, equipos de networking. Todos estos equipos cuentan con al menos seguridades mínimas que disminuyen el riesgo de accesos no autorizados a los mismos; sin embargo al no contar con un método de autenticación y autorización de usuarios la información que está almacenada en cada uno de los servidores es visible para cualquiere equipo de la red y lo que a su vez la hace vulnerable.

En la actualidad cada uno de los empleados mantiene la información con que realiza sus actividades diarias en cada uno de sus equipos y al tener la necesidad de que a la misma tengan acceso sus compañeros la comparten a través de la red de datos. No obstante prima la confianza entre compañeros, está latente el riesgo de posibles accesos o modificaciones a la información que no estén autorizados y que al momento tampoco dejaría evidencia de este tipo de ataque a la información. Tanto así que ha habido eliminación de archivos sin que se pueda determinar quien lo hizo y si fue deliveradamente.

Considerando que la importancia de la información la ha llevado a convertirse en el principal activo de toda institución; sea esta pública o privada, es así que la Cooperativa no es ajena a esta realidad por lo cual se ha propuesto en el corto plazo implementar métodos y políticas que disminuyan la vulnerabilidad de la información y a la vez permitan asegurarla de posibles pérdidas, daños, alteraciones o cualquier otro tipo de ataque que ponga en riesgo la integridad de la misma.

La propuesta que en esta investigación se expone hace énfasis en proteger la información de posibles vulnerabilidades que existen en la red de datos y más aún poder contar con una herramienta que permita evidenciar intentos de acceso no autorizados a la misma así como también de quien modificó o eliminó archivos.

6.3. JUSTIFICACIÓN

El haber dejado al descubierto la facilidad con la cual se puede acceder a la información compartida en red; cuando no existen mínimos controles de acceso a la misma, hace que ésta se encuentre vulnerable y expuesta a cualquier tipo de

amenaza a la información.

Considerando la importancia de la información para cualquier entidad; y más aún si ésta se encuentra en el ámbito financiero como es el caso de la Cooperativa de Ahorro y Crédito Coca Ltda, la pérdida o alteración de la misma puede acarrear graves inconvenientes a la institución.

Por este motivo es importante el poder contar con herramientas que permitan evidenciar intentos de accesos no autorizados así como también poder identificar quien hizo cambios en la información. Esto sin duda disminuirá en gran medida la vulnerabilidad de la información.

6.4. OBJETIVOS

6.4.1. General

Diseñar un sistema de gestión de auditoría que permita mejorar el aseguramiento de la información compartida en red

6.4.2. Específicos

1. Realizar un análisis de la situación actual de la red de datos de la Cooperativa de Ahorro y Crédito Coca Ltda. e identificar las principales amenazas y vulnerabilidades que deben ser atendidas de manera inmediata.
2. Definir un conjunto de políticas que permitan asegurar el acceso a la red de datos de la Cooperativa únicamente a usuarios autorizados
3. Especificar un conjunto mínimo de directivas de auditoría de acceso a información compartida en red que deben ser habilitadas en el servidor de archivos y que aseguren el contar con información suficiente para identificar intentos de acceso no autorizados a los datos así como también de las acciones (modificar, agregar, eliminar) que hayan realizado con ésta
4. Implementar un plan piloto de las políticas y directivas de auditoría de acceso a la información compartida en red
5. Evaluar los resultados obtenidos en la implementación del plan piloto en la reducción de las amanezas y vulnerabilidades identificadas

6.5. ANÁLISIS DE FACTIBILIDAD

La Cooperativa de Ahorro y Crédito Coca Ltda.; a través de su representante legal, se ha comprometido a invertir en el hardware, software y adecuaciones físicas necesarias que permitan disminuir el nivel de vulnerabilidad de la información compartida en red más aún si se considera el beneficio que ésto tendrá para la institución. Adicionalmente se cuenta con el apoyo del personal operativo así como también de los principales directivos de la Institución. Cabe mencionar que las adecuaciones físicas que sea necesario realizar es posible puesto que el edificio en el cual la Cooperativa realiza sus actividades es de propiedad de la Institución.

6.6. FUNDAMENTACIÓN

La presente investigación toma como punto de partida las facilidades que ofrece el sistema operativo Microsoft Windows 2008 Server para la implementación de un servidor de directorio activo al igual que un servidor de archivos y la personalización de auditoría a la información que se expone en red a través de este servicio.

Martinez Alegre (2011) en su página web dice lo siguiente acerca de lo que es el servidor de directorio activo:

> El directorio activo es la herramienta que nos brinda Microsoft para la organización y gestión de los recursos de una red de ordenadores y todo lo que ello implica: usuarios, servicios, puestos, impresoras, permisos, servidores, ... Será por tanto el directorio en el que almacenamos toda la información de los objetos que componen nuestra red. Esto es muy importante porque permite centralizar en un único punto la gestión de red, por ejemplo, los administradores de la red aquí definimos los usuarios, grupos para manejar a los usuarios más fácilmente por secciones, departamentos, o funciones, donde establecemos diversas propiedades de los equipos que pertenecen a esta red, etc. Para los usuarios es bueno ya que conseguimos que no tengan que decir a todos los recursos quienes son, es un buen almacén, por ejemplo, de las contraseñas, haciendo que la contraseña de cada usuario este almacenada en único punto

Leydiani (2011) en su artículo “Directorio Activo” manifiesta que la estructura de servicios que lo integran es la siguiente:

· DHCP (Dynamic Host Configuration Protocol). Protocolo de configuración dinámica de ordenadores, que permite la administración desatendida de direcciones de red.

· DNS (Domain Name System). Servicio de nombres de dominio que permite la administración de los nombres de ordenadores. Este servicio constituye el mecanismo de asignación y resolución de nombres (traducción de nombres simbólicos a direcciones IP) en Internet.

· SNTP (Simple Network Time Protocol). Protocolo simple de tiempo de red, que permite disponer de un servicio de tiempo distribuido.

· LDAP (Lightweight Directory Access Protocol). Protocolo ligero (o compacto) de acceso a directorio. Este es el protocolo mediante el cual las aplicaciones acceden y modifican la información existente en el directorio.

· Kerberos V5. Protocolo utilizado para la autenticación de usuarios y máquinas.

· Certificados X.509. Estándar que permite distribuir información a través de la red de una forma segura.

El servicio de Directorio Activo fue lanzado por Microsoft en sus sistemas operativos para servidor a partir de la versión Windows 2000 Server. Hasta antes de esto, el funcionamiento de un servidor primario de dominio con Windows NT (PDC por su nombre en inglés) se podía emular de manera sencilla con un servidor que estuviese ejecutando Samba sobre un sistema operativo GNU/Linux.

Emular el funcionamiento del Directorio Activo en un entorno GNU/Linux es más complicado ya que deben configurarse los servicios de Samba, Bind (DNS) y Kerberos para que trabajen en conjunto. Rivero (2013)en su página web explica lo siguiente:

> ...por el 2000 Microsoft cambió las reglas del juego, con el Windows XP y Windows 2000 Server se hizo una integración llamada Directorio Activo, donde ya no solo era un servidor controlador de dominio, sino un sistema formado por el PDC, Listas en directorios (Protocolo Ligero de Acceso a Directorios) Aka LDAP y para rematar un DNS Server. Son más cosas pero esas 3 básicas forman en si el Directorio Activo y en los primeros días era horrible homologar un GNU/Linux a un Servidor Windows 2000, 2003 y 2008 para entrar al mundo del Active Directory. No porque no se pueda, si no por que intentarlo es abrumador llevar a cabo todas las configuraciones necesarias.
>
> Afortunadamente la versión 4.0.0 de Samba hace que esto sea un poco mas sencillo...

Es por la razón antes descrita que para esta investigación se optó partir de la implementación de un Servidor de Directorio Activo de Microsoft. Adicionalmente se configurará un servidor de archivos bajo la misma plataforma (Windows 2008 Server) la cual ofrece varias prestaciones. A continuación se detalla cual es el concepto de servidor de archivo Microsoft (2005):

> Un servidor de archivos proporciona una ubicación central en la red, en la que puede almacenar y compartir los archivos con usuarios de la red. Cuando los usuarios necesiten un archivo importante, como un plan de proyecto, podrán tener acceso al archivo del servidor de archivos en lugar de tener que pasarlo entre distintos equipos. Si los usuarios de la red necesitan tener acceso a los mismos archivos y aplicaciones accesibles a través de la red, configure este equipo como un servidor de archivos.

Otra de las funcionalidades que ofrece el sistema operativo Windows 2008 Server; y que para esta investigación es necesaria, son las directivas de auditoría de seguridad avanzada, que Microsoft (2008)las define de la siguiente manera:

> Las mejoras de auditoría de seguridad en Windows Server 2008 R2 y Windows 7 permiten que una organización pueda auditar el cumplimiento de reglas empresariales y de seguridad importantes mediante un seguimiento de actividades definidas con precisión, como por ejemplo:
>
> - Un administrador de grupos modificó la configuración o los datos en los servidores que contienen información financiera.
> - Un empleado de un grupo definido obtuvo acceso a un archivo importante.
> - La lista de control de acceso del sistema (SACL) correcta se aplica a cada archivo y carpeta o clave del Registro en un recurso compartido de archivo o equipo como una medida de seguridad comprobable frente a accesos no detectados...
>
> ...En Windows 7 y Windows Server 2008 R2, el número de opciones de configuración de auditoría para las que se puede realizar un seguimiento de aciertos y errores ha aumentado a 53. Anteriormente, había nueve opciones de configuración de auditoría básicas en Configuración del equipo\Directivas\Configuración de Windows\Configuración de seguridad\Directivas locales\Directiva de auditoría. Estas 53 opciones nuevas permiten al usuario seleccionar solamente los

> comportamientos que desee controlar y excluir los resultados de auditoría de los comportamientos que no son importantes o que crean un excesivo número de entradas en el registro. Además, debido a que la directiva de auditoría de seguridad de Windows 7 y Windows Server 2008 R2 puede aplicarse mediante la directiva de grupo de dominio, las opciones de configuración de directiva de auditoría se pueden modificar, probar e implementar en usuarios y grupos seleccionados con relativa sencillez.

Todos los servicios anteriores funcionando en conjunto en una misma infraestructura ofrecen un ambiente seguro para la información que esté almacenada en el servidor de archivos así como también de la información que se encuentre compartida en red, en el servidor antes mencionado y mejor aún; con los servicios de directivas de auditoría, el sistema operativo se encargará de generar archivos con información de la auditoría.

Si bien es cierto que los archivos de auditoría están disponibles para ser leídos y revisados utilizando la herramienta "Visor de Sucesos" del propio sistema operativo, los datos que se muestran solo serán interpretados de manera adecuada por una persona con el suficiente conocimiento. Esta es la razón por la cual con la presente investigación se pretende exponer la información de la auditoría de una forma más amigable y fácil de entender.

No obstante las facilidades ofrecidas por el sistema operativo elegido para la presente investigación, es importante el contar con adecuadas políticas que permitan establecer parámetros y requisitos mínimos que aseguren el acceso a los empleados únicamente a la información que necesitan y más aún con las acciones que puedan realizar sobre estas.

6.7. METODOLOGÍA

La metodología propuesta para el sistema de gestión de auditoría de acceso a información compartida en red se resume en los siguientes cuatro pasos:

1. **Análisis de riesgos de la información compartida en red:** Establecer las vulnerabilidades (riesgos y amenazas) a las que se encuentra expuesta la información compartida en red.
2. **Definir políticas de control de acceso a la información compartida en**

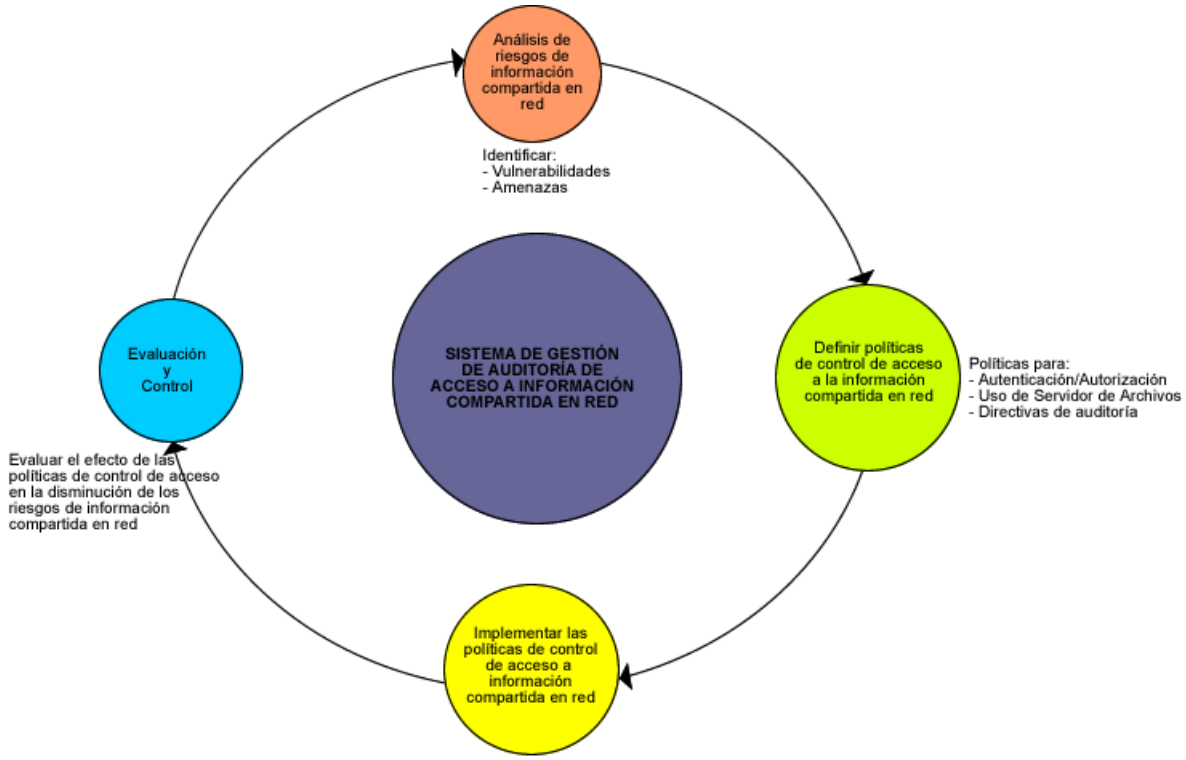
red: Establecer políticas que aseguren métodos de autenticación y autorización de usuarios para el acceso a la red, además de políticas que definan el correcto uso de los recursos de un servidor de archivos y por último establecer directivas de auditoría mínimos que permitan obtener datos respecto de quien accedió a la información compartida en red y que acciones realizó con ésta (modificar, eliminar, agregar)

3. **Implementación de las políticas de control de acceso:** Una vez definidas las políticas éstas fueron implementadas para su posterior evaluación y control. de la incidencia en el aseguramiento de la información compartida en red.

4. **Evaluación y control:** En esta fase se procedió a realizar una evaluación respecto de la incidencia en el aseguramiento de la información compartida en red.

En el gráfico siguiente se puede apreciar como interactúan cada una de las fases entre sí, volviéndose un proceso cíclico que está en constante revisión, actualización y mejoramiento.

Figura 22: Sistema de gestión de auditoría de acceso a recursos compartidos en red



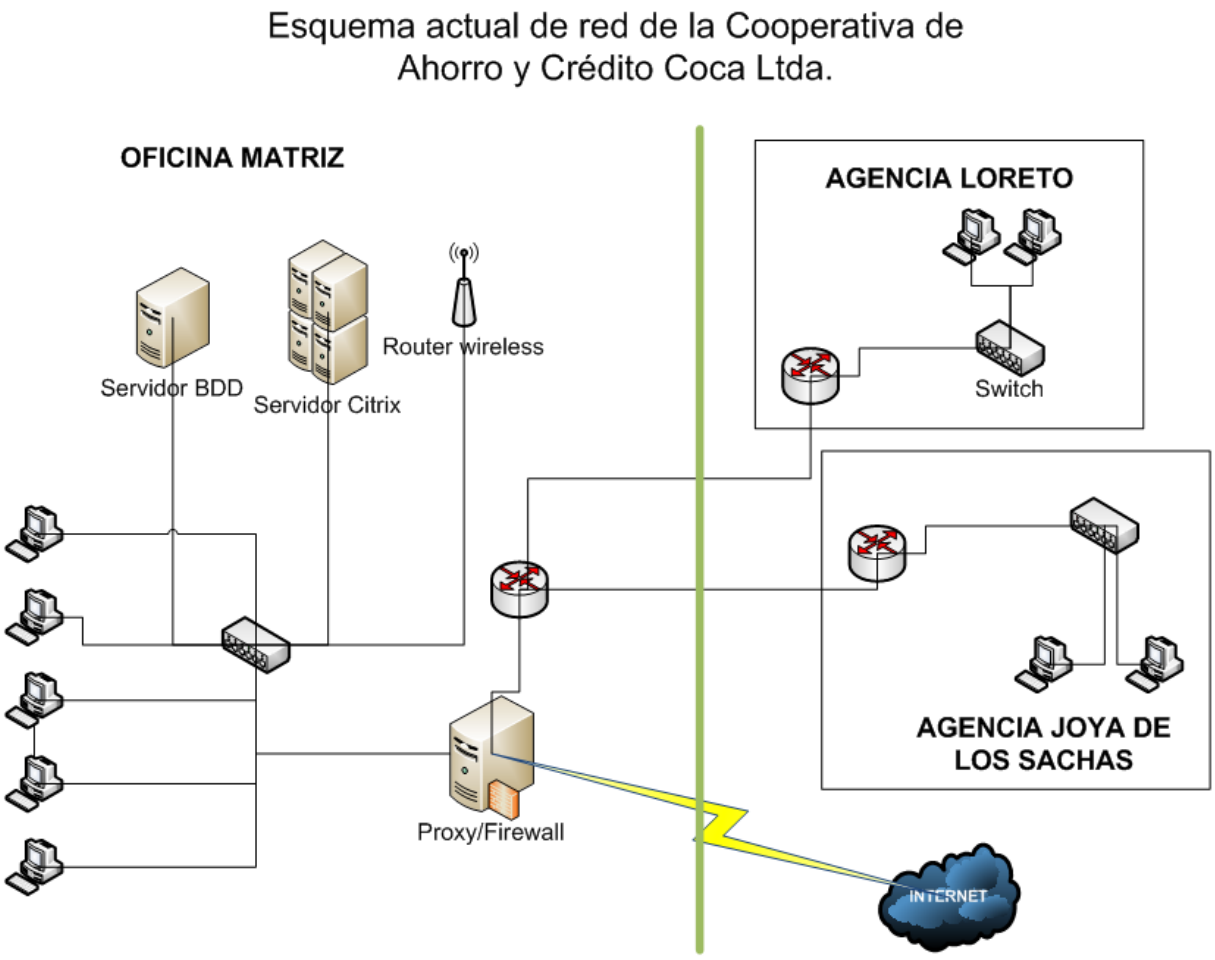
Elaborado por: Henry Vivanco (2014)

6.8. MODELO OPERATIVO

6.8.1. Diagnóstico de situación actual

6.8.1.1. Esquema de red actual

Figura 23: Esquema de red de la Cooperativa de Ahorro y Crédito Coca Ltda.



Fuente: Investigación de campo
Elaborado por: Henry Vivanco (2014)

6.8.2. Análisis de riesgos de la información compartida en red

En esta investigación el análisis de riesgos de la información se dividió en dos fases la primera que se enfoca en la identificación de amenazas y la segunda fase que realiza un análisis de la vulnerabilidad.

Los resultados obtenidos en cada una de las fases se detallan a continuación.

Identificación de amenazas

Para la identificación de amenazas se realizó un análisis de los mecanismos con que contaba la Cooperativa para asegurar el acceso a la información compartida en red. Estas amenazas se clasificaron de acuerdo al ámbito de acción de las mismas en: Físicas y Lógicas, y se detallan a continuación:

Tabla 28: Amenazas físicas de la información compartida en red

TIPO AMENAZA	AMENAZA	DESCRIPCIÓN
FISICO	Conexiones eléctricas	Conexiones eléctricas no reguladas en los sitios de trabajo de cada empleado
	Mecanismos antirobo	Equipos de los empleados no tienen ningún tipo de dispositivo que evite su posible sustracción
	Espacio físico para el Centro de Datos	El espacio físico asignado al Centro de Datos únicamente se encuentra separado por estructura de aluminio y vidrio
	Detectores de Humo	No existen detectores de humo en ninguna de las áreas de trabajo
	Mecanismos Control de acceso al Centro de Datos	Inexistencia de mecanismos de control de acceso hacia el centro de datos
	Dispositivos de almacenamiento externo	Usuarios están habilitados para conectar en sus computadores dispositivos de almacenamiento externo que se pueda conectar a los puertos USB o también copiar en DVD

Fuente: Investigación de campo
Elaborado por: Henry Vivanco (2014)

Tabla 29: Amenazas lógicas de la información compartida en red

TIPO AMENAZA	AMENAZA	DESCRIPCIÓN
LOGICA	Software malicioso	Todo tipo de virus (gusanos, malware, spyware, rootkits, etc)
	Software no licenciado	Programas propietarios de los cuales no se posee licencia (Microsoft Office, Sistema Operativo,)
	Antivirus	Programa antivirus de licencia gratuita
	Software base no estandarizado	Software base para los usuarios de la Cooperativa con diversidad de versiones (Microsoft Office, Sistema Operativo Windows, Antivirus)
	Instalación de software	Libertad a los usuarios para instalar cualquier software
	Acceso a Internet	Acceso a internet sin restricción
	Configuración de red	Todos los equipos se encuentran en el mismo segmento de red

Fuente: Investigación de campo
Elaborado por: Henry Vivanco (2014)

Identificación de vulnerabilidades

De acuerdo a la definición del Diccionario de la Real Academia de la Lengua vulnerabilidad significa "Cualidad de vulnerable". A su vez la definición de vulnerable es "que puede ser dañado herido o dañado física o moralmente". Para la presente investigación vulnerabilidad se considera aquella debilidad que; ante la intervención un agente externo, pudiera poner en riesgo cualquiera de los aspectos de seguridad de información (integridad, disponibilidad, confidencialidad o irrefutabilidad).

Partiendo de lo anterior; al igual que las amenazas, dependiendo del área en la cual interviene, se estableció las siguientes vulnerabilidades:

Tabla 30: Vulnerabilidades físicas

TIPO VULNERABILIDAD	VULNERABILIDAD	DESCRIPCIÓN DE LA VULNERABILIDAD
FISICO	Red eléctrica	Al no contar con instalaciones eléctricas reguladas para los equipos, existe la posibilidad de perdida de información por daños eléctricos
	Robo	Los equipos de los usuarios se encuentran a la vista y no cuentan con ningún mecanismo que asegure que estos no puedan ser sustraídos
	Espacio físico asignado al Centro de Datos	El área física asignada al centro de datos está compartida junto a la oficina asignada al área de Talento Humano.
	Incendio	Al no existir detectores de humo ni de calor; de producirse un incendio, las pérdidas tanto de equipos físicos como del personal es alta.
	Acceso al centro de datos	El acceso al centro de datos es a través de una puerta de vidrio común, lo cual en caso de robo permitiría un fácil ingreso a esta área
	Copias no autorizadas de información	Al tener los usuarios la libertad de conectar dispositivos de almacenamiento externo, esto les permite el poder hacer copias de información sin ningún tipo de control o verificación de la misma.

Fuente: Investigación de campo
Elaborado por: Henry Vivanco (2014)

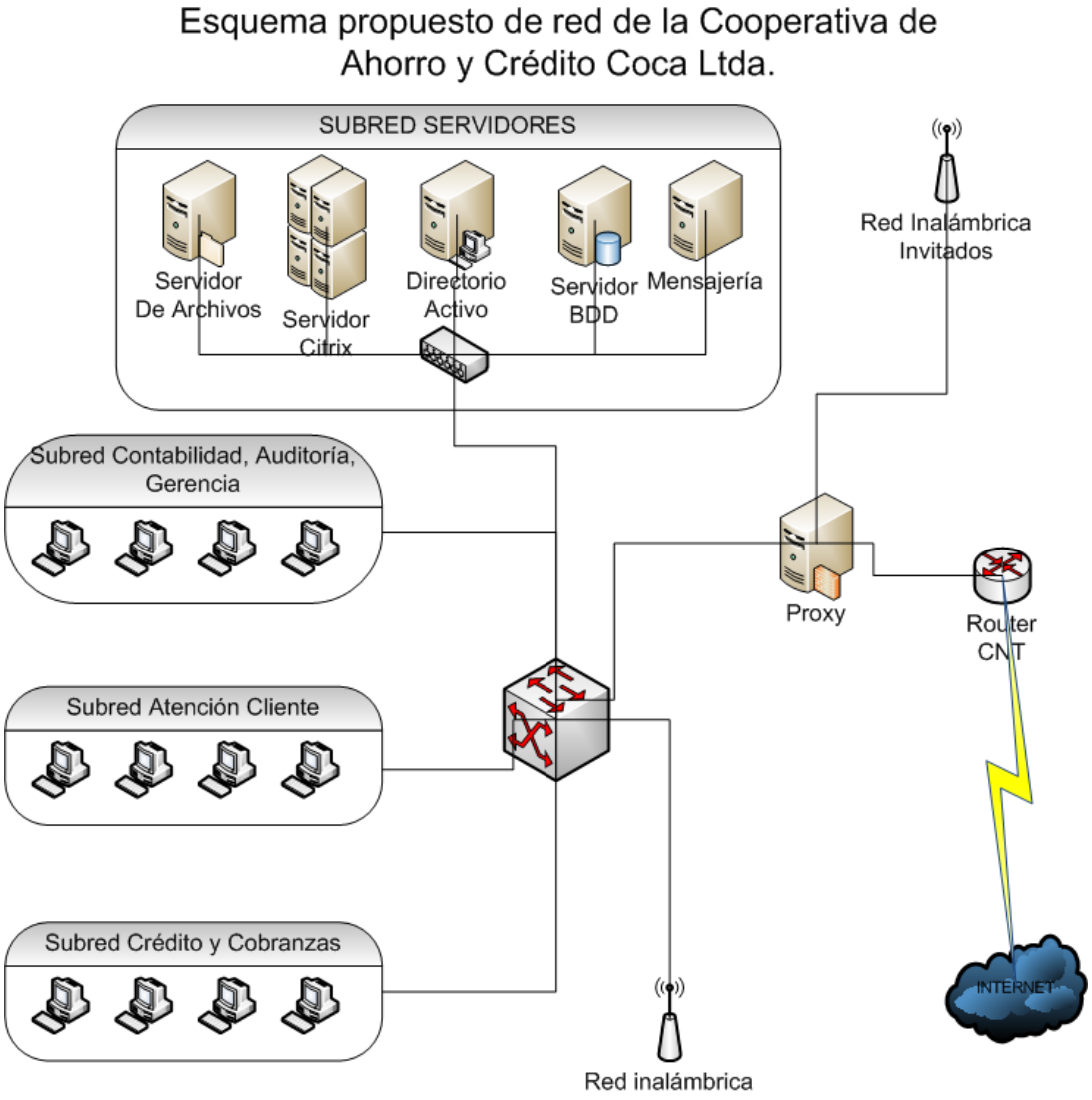
Tabla 31: Vulnerabilidades lógicas

TIPO DE VULNERABILIDAD	VULNERABILIDAD	DESCRIPCIÓN DE LA VULNERABILIDAD
LOGICA	Ataques por virus	Perdida o robo de información por infección de virus
	Software no licenciado	No se puede obtener actualizaciones; especialmente aquellas relacionadas con seguridad, por ejemplo del sistema operativo
	Software base no estandarizado	La diversidad de versiones; principalmente de sistema operativo y ofimática hace que para poder compartir información sea necesario deshabilitar ciertos aspectos de seguridad proporcionados por la aplicación (por ejemplo windows 7)
	Uso de correos personales para envío/recepción de información de la Cooperativa	Perdida de toda la información envíada/recibida cuando un empleado deja de laborar en la Institución
	Acceso a internet	Expone los equipos a posibles infecciones de virus informáticos
	Instalación de programas	Los usuarios están habilitados para instalar cualquier tipo de programa sin control, muchos de ellos descargados desde internet mismos que pueden incluir un virus informático
	Direccionamiento IP	No se han definido segmentos de red para separar los servidores del resto de equipos en la red de datos

Fuente: Investigación de campo
Elaborado por: Henry Vivanco (2014)

6.8.3. Rediseño esquema de red de datos de la Oficina Matriz de la Cooperativa de Ahorro y Crédito Coca Ltda.

Figura 24: Esquema propuesto de red de la Cooperativa de Ahorro y Crédito Coca Ltda.



Elaborado por: Henry Vivanco (2014)

6.8.4. Definición de políticas de control de acceso a la información compartida en red

Antes de proceder a establecer el instructivo de políticas para los procesos; de autenticación y autorización, uso de recurso del servidor de archivos y directivas de seguridad, fue necesario establecer un instructivo que permita etiquetar de manera adecuada los documentos que se fueron generando de tal manera que con solo leer

su identificador se pueda determinar el ámbito de acción de los mismos.

A continuación se describe el conjunto de políticas que deberán ser aplicadas para el aseguramiento de la información compartida en red en la Cooperativa de Ahorro y Crédito Coca Ltda. , mismas que se basan en la propuesta realizada en la Tesis de Maestría de Mayorga Jácome (2013).

6.8.4.1. Instructivo para etiquetado y manejo de información y documentos

Instructivo para etiquetado y manejo de la información			
Fecha emisión:	**Fecha revisión:**	**Fecha Aprobación:**	**Identificador: I-TIC-001-V1.0**
Elaborado por:		**Revisado y Aprobado por:**	

INTRODUCCIÓN

En este documento se explica la metodología que se deberá utilizar para la asignación de códigos para el etiquetado de la información y documentación relacionada con las políticas para el aseguramiento de la información compartida en red en la Cooperativa de Ahorro y Crédito Coca Ltda.

PROCEDIMIENTO PARA EL ETIQUETADO

Todos los documentos que integren el conjunto de políticas para el aseguramiento de la información compartida en red deberán ser identificados con un código de alfanumérico único de 7 caractéres, manteniendo la siguiente estructura:

Instructivo para etiquetado y manejo de la información

- **1er campo de etiquetado**: Tipo de Documento (1 caracter)

Tipos de Documento		
Valor	**Objetivo**	**Descripción**
I	Instructivo	Documento que establece las instrucciones de como realizar una actividad
F	Formulario	Documento utilizado para recolectar información con la cual se realizará una actividad
P	Procedimiento	Documento que describe los pasos a seguirse para realizar una actividad
M	Manual	Documento que contiene información detallada acerca de como realizar los pasos descritos para ejecutar un procedimiento
L	Políticas	Su contenido sirve de guía o lineamiento acerca de los principales puntos a cumplir para asegurar el acceso a la red de datos solo a personal autorizado

Instructivo para etiquetado y manejo de la información

- **2do campo de etiquetado**: Departamento que genera el documento o información (3 caracteres)

Dependencias de la Cooperativa de Ahorro y Crédito Coca Ltda.	
Valor	**Descripción**
TIC	Departamento de Tecnologías de la información y comunicaciones
CRE	Departamento de Crédito y Cobranzas
CAP	Departamento de CaptaCIÓNes y Atención al Cliente
SEC	Asistente de Gerencia
GER	Gerencia

- **3er campo de etiquetado**: Número secuencial del documento o información de 3 dígitos que van desde el 001 al 999.
- **4to campo de etiquetado:** Especifica la versión del documento en cuestión y el formato siempre empezará con la letra V seguida del número de versión del documento mismo que iniciará con el valor 1.0. Cuando el documento tenga algunas modificaciones menores se utilizará un valor adicional que indique cuantas veces ha sido modificado (por ejemplo 1.2). Cuando se hagan modificaciones sustanciales y de fondo al documento el número de versión será el inmediato superior (por ejemplo 2.0).

6.8.4.2. Políticas para asegurar el acceso a la red de datos

Políticas para asegurar el acceso a la red de datos			
Fecha emisión:	**Fecha revisión:**	**Fecha Aprobación:**	**Identificador: L-TIC-001-V1.0**
Elaborado por:		**Revisado y Aprobado por:**	

I. INTRODUCCIÓN

En este documento se especifica las políticas de aseguramiento para el acceso a la red de datos de la Cooperativa de Ahorro y Crédito Coca Ltda.

II. DEPARTAMENTOS RESPONSABLES

Los departamentos que serán los responsables directos de definir, revisar, corregir, mejorar y aprobar las políticas para asegurar el acceso a la red de datos únicamente a personal autorizado son: Jefe del Departamento de TIC's, Gerencia, Jefes Departamentales y Jefes de Agencia.

III. POLÍTICAS DE ACCESO A LA RED DE DATOS DEPARTAMENTO DE TIC's

1. Establecer un documento con un grupo inicial de políticas donde se especifiquen los principales puntos a considerar para restringir, asegurar y conceder el acceso a la red de datos únicamente a usuarios autorizados.
2. Socializar el documento de políticas de acceso a la red de datos con Gerencia para su revisión, corrección y aprobación
3. Realizar la socialización de las políticas de acceso a la red de datos con la Gerencia y Jefes Departamentales para su conocimiento, corrección, mejora y aprobación final del mismo
4. Definir el proceso a seguir cuando un empleado ingresa a trabajar o sale de la Institución
5. Definir un formulario para la solicitud y aprobación de la creación de usuarios para el acceso a la red de datos

Políticas para asegurar el acceso a la red de datos

6. Definir un formato de solicitud de acceso temporal a los recursos de red de la Institución
7. Establecer un documento de acuerdo de confidencialidad del uso de la información de la institución
8. Establecer el proceso adecuado para restringir el acceso a la información compartida en red
9. Definir un formulario de solicitud y aprobación de acceso a información compartida en red
10. Proponer correcciones, mejoras y actualizaciones a las politicas de acceso a la red de datos e información compartida en red
11. Definir los requerimientos de hardware y software necesarios que permitan la correcta instalación, configuración y funcionamiento de un servidor de autenticación y autorización de usuarios para el acceso a la red de datos
12. Definir los requerimientos de hardware y software necesarios que aseguren la correcta instalación, configuración y funcionamiento de un servidor de archivos
13. Establecer políticas para las tareas de administración de usuarios de red, como son: creación y eliminación, asignación a unidades organizacionales, permisos de acceso a información compartida
14. Establecer políticas para el correcto uso de los recursos con que cuenta el servidor de archivos, específicamente en lo que se refiere al tipo de información que se permitirá guardar
15. Establecer un conjunto mínimo de directivas de auditoría en el servidor de archivos que permitan identificar las acciones que los usuarios realizan respecto de la información compartida en red (acceso, modificación, creación y eliminación de información)

Políticas para asegurar el acceso a la red de datos

16. Poner en conocimiento de todo el personal operativo y administrativo los documentos aprobados de las políticas para el aseguramiento del acceso a la red de datos y de la información compartida en red

GERENCIA

1. Aprobar el documento de políticas de administración de usuarios de red
2. Aprobar el documento de políticas para el adecuado uso del servidor de archivos
3. Aprobar el formulario de solicitud de acceso temporal a los recursos de red de la Institución
4. Asegurarse de que el acuerdo de contabilidad esté apegado a las leyes vigentes en el Ecuador
5. Conocer, aprobar y exigir el cumplimiento del contenido del documento de acuerdo de confidencialidad del uso de información de la Cooperativa
6. Socializar con todo el personal operativo y administrativo las políticas de acceso a la red de datos e información compartida en red que se aplicarán en la Institución
7. Apoyar activamente en el cumplimiento de los lineamientos establecidos en las políticas definidas para asegurar eñ acceso a la red de datos e información compartida en red de la Institución
8. Aprobar el formulario de solicitud de creación de usuarios y acceso a la red de datos e información compartida en red
9. Facilitar la adquisición de software y hardware mínimo para la instalación, configuración de un servidor de administración de usuarios de red y de un servidor de archivos

Políticas para asegurar el acceso a la red de datos

10. Establecer sanciones ante el incumplimiento o inobservación de todas las políticas que se establezcan para asegurar el acceso a la red de datos e información compartida en red y de los acuerdos de confidencialidad y solicitud de creación de usuarios

JEFE DE TALENTO HUMANO

1. Asegurarse de que todo el personal que está laborando actualmente haya firmado; y de ser el caso firme, el acuerdo de confidencialidad de la Institución
2. Comunicar con al menos 7 días de antelación de la contratación de nuevo personal, la oficina a la que será designado y las funciones que cumplirá
3. Completar toda la información requerida en el formulario de solicitud de creación de usuario y hacerlo aprobar por Gerencia
4. Asegurarse de que el nuevo personal conozca las políticas definidas en la Institución para el aseguramiento del acceso a la red de datos e información compartida en red
5. Socializar oportunamente; a todo el personal que labora en la Institución, de las políticas definidas en la Institución para el aseguramiento del acceso a la red de datos e información compartida en red
6. Socializar; inmediatamente sean aprobados, los cambios que se realicen a las políticas vigentes en la Institución para el aseguramiento del acceso a la red de datos e información compartida en red
7. Comunicar con al menos quince días de antelación respecto de que un empleado dejará de prestar sus servicios en la Institución; excepto en casos de fuerza mayor

6.8.4.3. Formulario para la solicitud de creación de usuario

Formulario para la solicitud de creación de un nuevo usuario			
Fecha emisión:	**Fecha revisión:**	**Fecha Aprobación:**	**Identificador: F-TIC-001-V1.0**
Elaborado por:		**Revisado y Aprobado por:**	

I. INTRODUCCIÓN

Este documento detalla los campos que deben ser llenados por el Responsable del Area de Talento Humano para solicitar la creación de un nuevo usuario; para acceder a las distintas plataformas que existen en la institución, cuando nuevo personal es contratado

II. PROCEDIMIENTO A SEGUIR

1. Cuando nuevo personal es contratado, el Responsable del área de Talento Humano debe rellenar todos los campos existentes en el formulario para la creación de un usuario, indicando claramente toda la información que se requiera.

2. El formulario debe ser entregado; en primera instancia, a la Gerencia para que a su vez haga las observaciones necesarias previa a la respectiva autorización.

3. El formato al que se hace mención, se detalla a continuación:

COOPERATIVA DE AHORRO Y CREDITO COCA LTDA.

FORMULARIO DE SOLICITUD DE CREACION DE USUARIO

1.- Nombres:_____ Apellidos:_____

2. Oficina: Matriz____ Ag. Sacha____ Ag. Loreto____

3. Area en la que va a trabajar:_____

4. Función que Desempeñará:_____

5. Permisos de Acceso:

Red: _____ Mensajería: _____

Sistema Transaccional: _____ Correo: _____

CITRIX: ____

_____

Solicitado por

6.8.4.4. Formulario para la solicitud de acceso al servidor de archivos

Formulario para la solicitud de acceso al servidor de archivos			
Fecha emisión:	**Fecha revisión:**	**Fecha Aprobación:**	**Identificador: F-TIC-002-V1.0**
Elaborado por:		**Revisado y Aprobado por:**	

I. INTRODUCCIÓN

Este documento describe toda la información que debe ser llenada por un usuario para soliticar el acceso a una carpeta; en el servidor de archivos, en la cual existe información a la que requiere acceder y a la que aún no le han asignado permiso.

II. PROCEDIMIENTO A SEGUIR

1. El formulario deberá ser llenado por el usuario que desea acceder a la información existente en el servidor de archivos. También deberá firmar en el lugar destinado para el solicitante
2. El solicitante debe explicar de forma clara y concisa el motivo por el cual requiere el acceso a la información que está solicitando
3. También debe especificar el tiempo por el cual solicita el acceso a la información; si es temporal, o si el acceso será permanente
4. La solicitud deberá tener la firma de revisado del jefe inmediato superior del solicitante
5. Una vez que ha terminado de llenar la solicitud; en el área solicitante, ésta deberá ser remitida al jefe del departamento responsable de la información a la que el solicitante requiere acceder
6. El jefe del departamento responsable de la información a la que desea acceder el solicitante emitirá un informe en el que debe detallar claramente el o los motivos por los cuales acepta o niega la solicitud

Formulario para la solicitud de acceso al servidor de archivos

7. Tanto la solicitud de acceso a la información como el informe deberán ser remitidos a la Gerencia para que éste a su vez ratifique la aceptación o negación de la petición de acceso a la información

8. En caso de que la solicitud de acceso a información sea autorizada, ésta deberá ser remitida al departamento de TIC's para su ejecución

COOPERATIVA DE AHORRO Y CREDITO
COCA LTDA.

FORMULARIO DE SOLICITUD DE ACCESO
A INFORMACIÓN EN EL SERVIDOR DE ARCHIVOS

Fecha:_____ Hora:_____ Nombre del solicitante:_____

Dpto. Solicitante:_____

Dpto. Responsable Información a la que solicita acceso: _____

Permisos de acceso a la información: Lectura:____ Escritura:_____

Tipo de acceso a la información: Temporal:_____ Permanente:_____

Acceso temporal: Fecha inicio:_____ Hora inicio:_____
Fecha fin:_____ Hora fin:_____

Motivo por el cual requiere acceso a la información:_____
_____
_____
_____
_____

Solicitante Jefe de Solicitante Jefe Dpto. Responsable

Autorizado Gerencia

6.8.4.5. Políticas para el correcto uso del servidor de archivos

Políticas para el correcto uso del servidor de archivos			
Fecha emisión:	**Fecha revisión:**	**Fecha Aprobación:**	**Identificador: L-TIC-002-V1.0**
Elaborado por:		**Revisado y Aprobado por:**	

I. INTRODUCCIÓN

En este documento se describe las políticas que deberán cumplirse para hacer un correcto uso de los recursos existentes en el servidor de archivos.

II. POLITICAS

1. Para cada usuario se debe crear una carpeta en el servidor de archivos; a la cual accederá a través de la red, con permisos de administración total (lectura/escritura) sobre la información que ahí se encuentre almacenada

2. Se debe crear una carpeta por cada departamento de la Cooperativa (por ejemplo: Contabilidad, Cartera, Auditoría). A esta carpeta tendrán acceso de lectura únicamente los usuarios que pertenecen a dicho departamento en tanto que el jefe del departamento tendrá acceso total (lectura/escritura) sobre la información que se encuentre ahí almacenada

3. El servidor de archivos está destinado para que los usuarios guarden información que esté relacionada únicamente con las labores que realiza en la Cooperativa en el desempeño de sus funciones

4. Se hará una revisión diaria de la información almacenada en el servidor y se eliminará aquella que no cumpla lo establecido en el punto anterior, como por ejemplo: archivos de música, videos, fotos personales.

Políticas para el correcto uso del servidor de archivos
5. De evidenciarse que un usuario utilizó el servidor de archivos para guardar información personal; como la menCIÓNada en el punto anterior, deberá ser registrado en el formulario "Registro de incidencias" y notificado tanto al usuario propietario de la información como a la Gerencia.

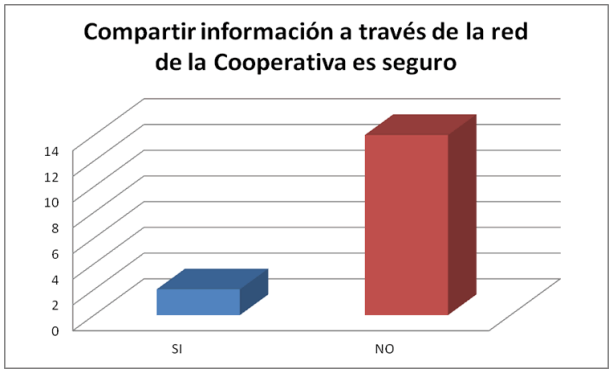
6.8.4.6. Pregunta 16: ¿Considera que compartir información en la red de datos de la Coooperativa es seguro?

Tabla 37: Compartir información a través de la red de la Cooperativa es seguro

opciones	CANTIDAD	FRECUENCIA, %
SI	3	18.75 %
NO	13	81.25 %
TOTAL	16	100 %

Fuente: Encuesta
Elaborado por: Henry Vivanco (2014)

Figura 25: Compartir información a través de la red de la Cooperativa es seguro



Fuente: Encuesta
Elaborado por: Henry Vivanco (2014)

Análisis e interpretación:

El 18.75 % de los encuestados considera que es seguro compartir su información en la red el 81.25 % considera que no es seguro.

La mayoría de los empleados coincide en que el compartir información en la red de datos actual representa un gran riesgo para su información.

6.8.4.7. Formulario para el registro de incidencias en el servidor de archivos

Formulario para el registro de incidencias en el servidor de archivos			
Fecha emisión:	**Fecha revisión:**	**Fecha Aprobación:**	**Identificador: F-TIC-003-V1.0**
Elaborado por:		**Revisado y Aprobado por:**	

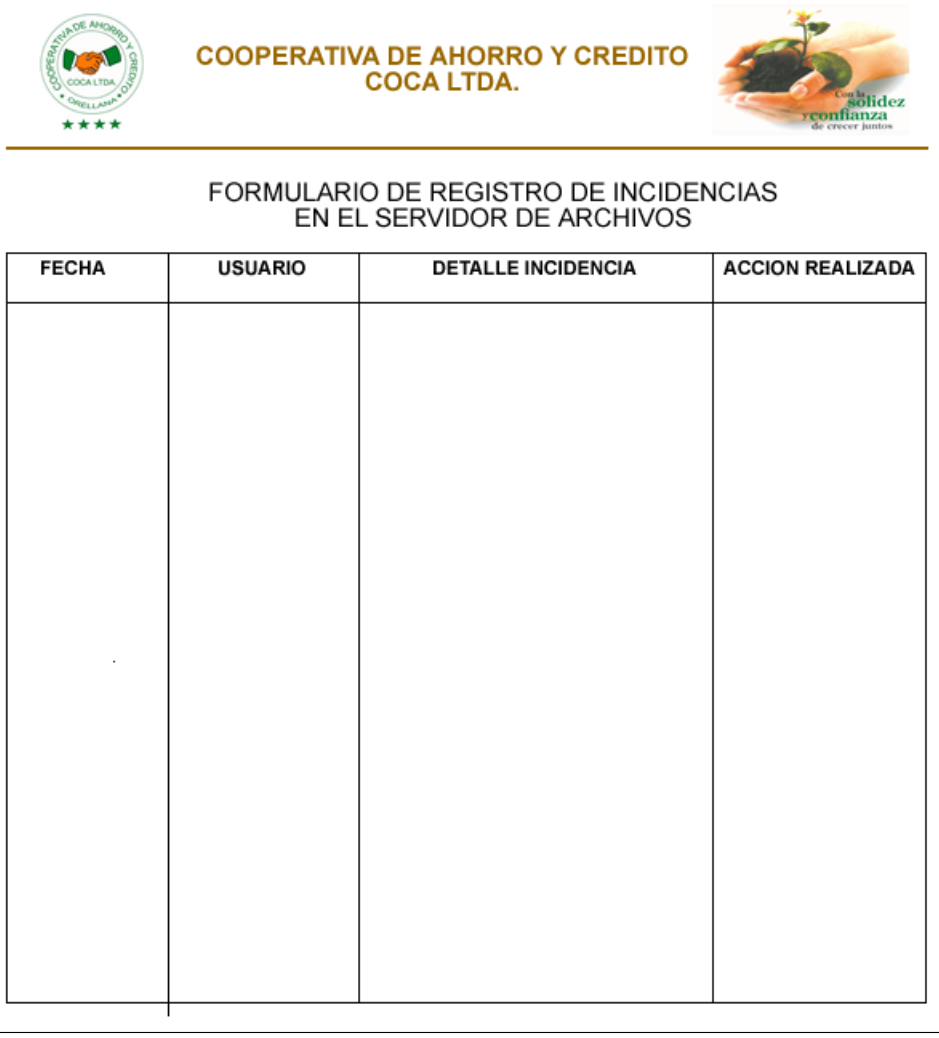
I. INTRODUCCIÓN

En este documento se describe la información con que debe ser llenado el formulario de registro de incidencias en el servidor de archivos por la mala utilización del mismo.

II. DESCRIPCIÓN DE LOS CAMPOS DEL FORMULARIO

1. **Fecha:** En la que se detecta la incidencia en el servidor de archivos
2. **Usuario:** Que tiene los permisos de administración (lectura/escritura) en la carpeta compartida en el servidor de archivos
3. **Detalle:** Descripción pormenorizada de la incidencia detectada respecto del mal uso del servidor de archivos para guardar información no autorizada.
4. **Acción realizada:** Detalle de las acciones que se realizaron para depurar la información que se detectó como no permitida de ser almacenada en el servidor.

Formulario para el registro de incidencias en el servidor de archivos



COOPERATIVA DE AHORRO Y CREDITO
COCA LTDA.

FORMULARIO DE REGISTRO DE INCIDENCIAS
EN EL SERVIDOR DE ARCHIVOS

FECHA	USUARIO	DETALLE INCIDENCIA	ACCION REALIZADA

6.8.4.8. Directivas de auditoría

Las directivas de auditoría son un herramienta incluida en Windows 2008 Server que sirve para generar un registro de los eventos que se van presentando, sean estos correctos o incorrectos. Estos registros ayudan en la identificación del uso no autorizado de recursos dentro de un dominio de red.

Entre los ámbitos que pueden ser auditados se encuentran aquellos relacionados con la seguridad. Para esto solo basta con habilitar las categorías apropiadas.

Windows 2008 Server permite realizar auditoría de los eventos relacionados con:

- **Administración de cuentas:** Alta y baja de usuarios, actualización de información de usuarios (nombres, apellidos, correo)

- **Acceso al servicio del directorio:** El servicio de directorio incluye
  - **Servicios de certificados de Active Directory (AD CS):** Crear, distribuir y administrar certificados de claves públicas personalizados
  - **Servicios de dominio de Active Directory (AD DS):** Almacena datos de directorio y administra la comunicación entre usuarios y dominios, incluso procesos de inicio de sesión de usuarios, autenticación y búsquedas en directorios
  - **Servicios de federación de Active Directory (AD FS):** proporciona tecnologías de inicio de sesión único (SSO) web para autenticar a un usuario en varias aplicaciones web durante una única sesión en línea
  - **Active Directory Lightweight Directory Services (AD LDS):** un Servicio de Directorio del Protocolo Ligero de acceso a directorios (LDAP) ofrece una compatibilidad flexible para aplicaciones habilitadas para el uso de directorios, sin las restricciones de los Servicios de dominio de Active Directory (AD DS).
  - **Active Directory Rights Management Services (AD RMS):** protege la información y trabaja con aplicaciones compatibles con AD RMS para ayudar a proteger la información digital del uso no autorizado.
- **Acceso a objetos:** Recursos (Impresoras, scanner, cámaras, etc.), Servicios (correo electrónico, impresiones, etc.), Usuarios, grupos, unidades organizacionales.
- **Cambio de directivas:** Cualquier modificación que se realice a las directivas de auditoría, ya sea que se active, desactiven o cambie el evento en el cual se genera los registros de auditoría (correcto, incorrecto, no habilitado)
- **Uso de privilegios:** Que actividades ha realizado con el privilegio de usuario asignado. Privilegios como por ejemplo: administrador, usuario avanzados, usuario normal.
- **Procesos:** El comportamiento de los procesos del sistema: cuando se ejecuta, cuando se detiene, que usuario lo ejecutó o detuvo.
- **Eventos del sistema:** Cuando se inicia, reinicia, apaga el servidor o si se produce algún suceso que afecte a la seguridad del sistema.

A las directivas de auditoría se le puede asignar los siguientes valores:

- **Correcto:** Cuando no ocurre ningún problema, por ejemplo: Usuario ingresa su contraseña correctamente
- **Incorrecto:** Cuando se ha producido un error en el evento que está siendo auditado. Por ejemplo: Contraseña incorrecta de usuario
- **Sin Auditar:** El evento no se audita. Esta opción prevalece sobre los valores correcto e incorrecto

En la presente investigación lo que se requería es poder obtener información acerca de las actividades que realizan los usuarios en la información que se encuentra compartida en red de tal manera de identificar accesos no autorizados al igual que las acciones que hayan realizado con ésta, para el efecto se habilitaron las siguientes directivas de seguridad:

- Inicio de Sesión
- Auditoría del sistema de archivos
- Manipulación de identificadores
- Directiva de auditoría de acceso a objetos global del dominio

Los pasos que se siguieron para configurar cada una de las directivas antes listadas se encuentra detalladas en el Anexo 5, Configuración de Directivas de Auditoría.

6.9. ADMINISTRACIÓN

Tabla 39: Administración

Gerente General:	Econ. Aldrin Cuvi
Auditora Interna:	Dra. Maya Tenorio
Responsable Area TIC's	Ing. Henry Vivanco
Contadora General:	Sra. Mayra Cedeño
Asistente de Gerencia:	Srta. Alba Calero
Jefe de Crédito:	Sra. Katiuska Balladares
Jefe de Caja:	Sr. Juan Román

Fuente: Dpto. Talento Humano
Elaborado por: Henry Vivanco (2014)

6.10. PLAN DE ACCIÓN

Con el fin de evidenciar la efectividad de la propuesta respecto de la disminución de los accesos no deseados y pérdida de información compartida en red en la Cooperativa de Ahorro y Crédito Coca Ltda. se solicitó por parte de la Gerencia se implemente previamente un ambiente de pruebas en el que se pudiera manipular la información (acceder, modificar, crear y eliminar archivos) sin que ésto comprometa los datos reales de cada usuario y en sí de la institución mismo.

Con el fin de cumplir lo solicitado se implementó un ambiente de pruebas para el cual se estableció un cronograma de trabajo y evaluación, mismo que se puede apreciar en la figura 25.

6.11. PREVISIÓN DE LA EVALUACIÓN

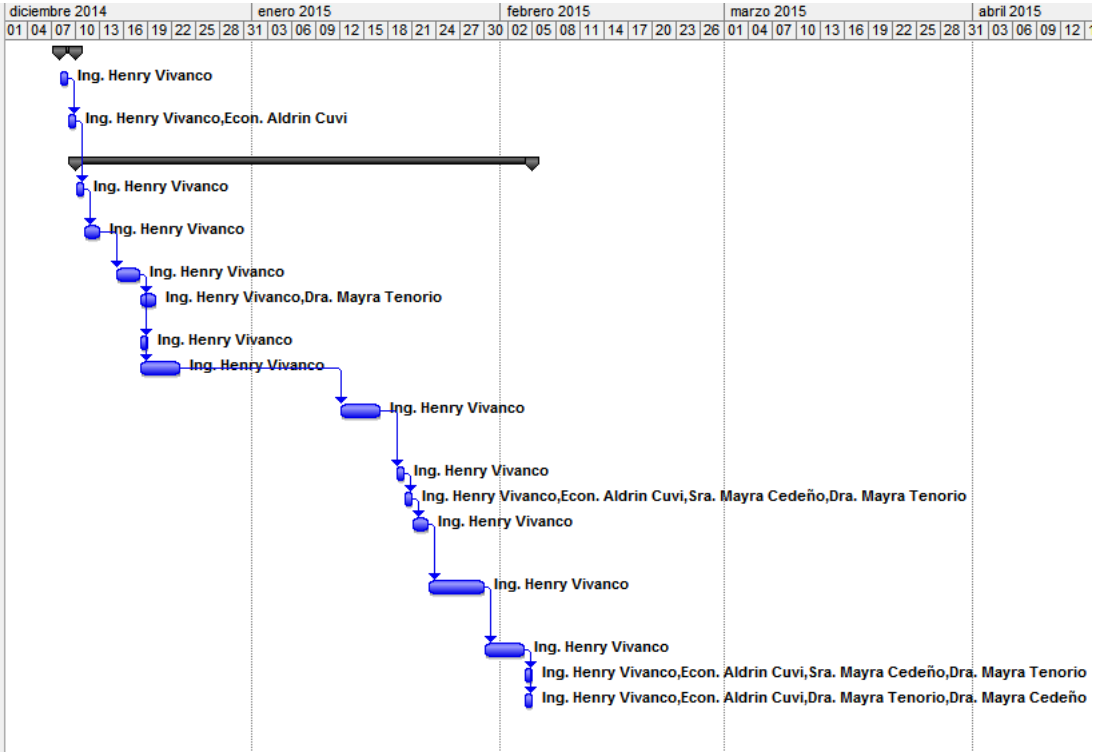
Para el ambiente de pruebas se habilitaron carpetas compartidas para los departamentos de Contabilidad, Crédito y Atención al Cliente en las cuales se puso información irrelevante por lo que su modificación o eliminación no tuvo ninguna incidencia para sus propietarios y en sí para la institución misma.

La evaluación se la realizó en dos fases, la primera cuando el acceso a la información compartida en red no tenía ninguna restricción de acceso y la segunda fase luego de haber aplicado las políticas de control de acceso a la información compartida en red propuestas. Cabe mencionar que antes de iniciar la evaluación fue necesario habilitar las directivas de auditoría de tal manera de poder obtener información respecto de los accesos a la información y las tareas realizadas sobre ésta.

Para una mayor facilidad de la evaluación y la incidencia de las políticas de control de acceso, ésta se realizó en la carpeta asignada al Departamento de Contabilidad.

Figura 26: Cronograma de implementación de ambiente de pruebas

	Nombre de tarea	Duración	Comienzo
1	**Fase 1: Selección de servidor para pruebas**	**2 días**	**lun 12/08/14**
2	Requerimientos mínimos de hardware para instalación de Windows 2008 Server	1 día	lun 12/08/1
3	Seleccionar el servidor a ser utilizado para las pruebas de entre los que no están siendo	1 día	mar 12/09/1
4	**Fase 2: Instalación y configuración de hard**	**41 días**	**mié 12/10/14**
5	Instalación de sistema operativo windows 2008 Server	1 día	mié 12/10/1
6	Configuración de Servidor de Directorio Activo	2 días	jue 12/11/1
7	Configuración de Servidor de Archivos	3 días	lun 12/15/1
8	Pruebas de funcionamiento del Servidor de directorio activo y del servidor de archivos	2 días	jue 12/18/1
9	Activación de directivas de auditoría	1 día	jue 12/18/1
10	Creación de carpetas e información compartida en red para pruebas	3 días	jue 12/18/1
11	Evaluación del acceso a la información del departamento de contabilidad compartida en red sin restricción de acceso	5 días	lun 01/12/1
12	Tabulación de resultados	1 día	lun 01/19/1
13	Presentación de resultados	1 día	mar 01/20/1
14	Aplicación de políticas de seguridad de acceso a información del departamento de contabilidad compartida en red	2 días	mié 01/21/1
15	Evaluación del acceso a la información del departamento de contabilidad compartida en red aplicando políticas de control de acceso	5 días	vie 01/23/1
16	Tabulación de resultados	3 días	vie 01/30/1
17	Presentación de resultados	1 día	mié 02/04/1
18	Comparación de resultados antes y después de la implementación de políticas de acceso a la información compartida en red	1 día	mié 02/04/1



Elaborado por: Henry Vivanco (2014)

6.11.1. Tabulación de resultados

6.11.1.1. Primera fase: sin control de acceso a la información compartida en red

Tabla 40: Evaluación de acceso a la información del departamento de contabilidad compartida en red

		INCIDENCIAS EN ARCHIVOS (cantidad)			
	Accesos de Usuario	Abiertos	Modificados	Eliminados	Añadidos
Usuarios del área de contabilidad	35	15	12	0	6
Usuarios del área de crédito	60	10	10	2	20
Usuarios del área de atención al cliente	20	5	3	1	8
Total	115	30	25	3	34

Fuente: Investigación de campo
Elaborado por: Henry Vivanco (2015)

6.11.1.2. Segunda fase: implementación de políticas de control de acceso a la información compartida en red

Tabla 41: Evaluación de acceso a la información del departamento de contabilidad compartida en red luego de aplicar políticas de acceso a la información

		INCIDENCIAS EN ARCHIVOS (cantidad)			
	Accesos de Usuario	Abiertos	Modificados	Eliminados	Añadidos
Usuarios del área de contabilidad	45	12	8	3	5
Usuarios del área de crédito	8	4	0	0	0
Usuarios del área de atención al cliente	2	2	0	1	0
Total	55	18	8	4	5

Fuente: Investigación de campo
Elaborado por: Henry Vivanco (2015)

6.11.1.3. Equipo encargado de la evaluación

El personal presente en la evaluación de los resultados fue el siguiente:

Tabla 42: Equipo encargado de la evaluación

Gerente General:	Econ. Aldrin Cuvi
Auditora Interna:	Dra. Maya Tenorio
Contadora General:	Sra. Mayra Cedeño
Asistente de Gerencia:	Srta. Alba Calero
Jefe de Crédito:	Sra. Katiuska Balladares
Jefe de Caja:	Sr. Juan Román

Elaborado por: Henry Vivanco (2015)

6.11.2. EVALUACIÓN

6.11.2.1. Entrevista aplicada a los miembros del equipo de evaluación

Una vez presentados los resultados de la aplicación de las políticas de control de acceso a la información compartida en red, se procedió a realizar una encuesta dirigida a los miembros del equipo de evaluación. A continuación los resultados de la misma

Pregunta 1: ¿Qué le pareció la propuesta para el aseguramiento de la información compartida en red?

Figura 27: Evaluación de la propuesta

Fuente: Encuesta
Elaborado por: Henry Vivanco (2015)

Pregunta 2: ¿Considera Usted que con la aplicación de la propuesta, el compartir información en red es seguro?

Figura 28: Evaluación de la propuesta

Fuente: Encuesta
Elaborado por: Henry Vivanco (2015)

Pregunta 3: ¿Estaría dispuesto a implementar en el corto tiempo en ambiente real las políticas para el aseguramiento de información compartida en red?

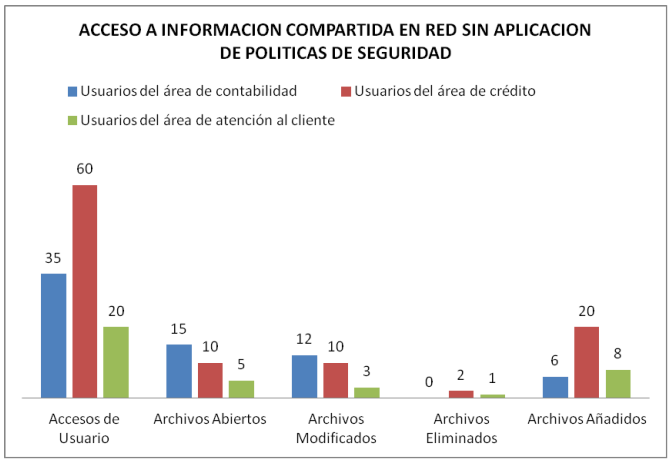
Figura 29: Evaluación de la propuesta

Fuente: Encuesta
Elaborado por: Henry Vivanco (2015)

6.11.2.2. Evaluación por parte del investigador

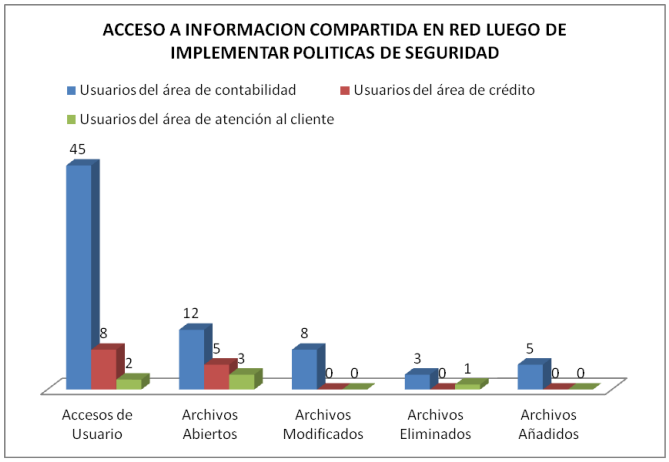
En las dos fases que se dividió la investigación para recabar datos se pudo apreciar una disminución notable del acceso a la información compartida en red y de las actividades que con ellas realizaron los usuarios, en especial aquellos que no estaban autorizados a acceder. Esto último se pudo evidenciar gracias a la información generada por las directivas de auditoría que se activaron para el efecto en conjunto con los otros servicios habilitados (Directorio Activo y Servidor de Archivos). En los gráficos siguientes se puede apreciar la disminución drástica de la interacción de usuarios con la información a la cual no tenían acceso.

Figura 30: Acceso a información compartida en red si restricción



Fuente: Encuesta
Elaborado por: Henry Vivanco (2015)

Figura 31: Acceso a información compartida en red si restricción



Fuente: Encuesta
Elaborado por: Henry Vivanco (2015)

6.12. CONCLUSIONES Y RECOMENDACIONES

6.12.1. Conclusiones

1. Es necesario realizar un rediseño lógico de la red de datos para separar los componentes activos de red (switches, routers, wireless router) y servidores del resto de equipos
2. Las directivas de auditoría para el control y gestión de acceso a información compartida en red necesita previamente la implementación del servicio de Directorio Activo
3. La implementación de políticas de control de acceso a información compartida en red reduce el riesgo y la vulnerabillidad de la información
4. Con el uso de las directivas de auditoría en conjunto con el servicio de Directorio Activo pueden extender el control de acceso a otros recursos dentro de la red de datos, como por ejemplo el uso de impresoras o de correo electrónico
5. Toda inversión que se realice; en la adquisición de hardware como de software, con el fin de asegurar la información de la Cooperativa de Ahorro y Crédito Coca Ltda. nunca será demasiada

6.12.2. Recomendaciones

1. Implementar en ambiente de producción un servidor de Directorio Activo y servidor de archivos
2. Implementar en ambiente de producción las políticas de acceso a información compartida en red, así como del buen uso del servidor de archivos
3. Socializar con el personal de la Cooperativa de Ahorro y Crédito Coca Ltda. las políticas de acceso a información compartida en red y del buen uso de los recursos de la institución
4. Revisar y actualizar periódicamente las políticas de acceso a información compartida en red y del buen uso de los recursos del servidor de archivos
5. Evaluar periódicamente los datos generados por las directivas de auditoría, de tal manera de poder establecer ajustes que sea necesario realizar para mejorar las políticas propuestas en la presente investigación

BIBLIOGRAFIA

Álvarez-Gayou, J. L. (2005). Cómo hacer investigación cualitativa. fundamentos y metodología. *Métodos básicos. Ed. Paidós. México.*, pages 127–128.

Ávila Baray, H. (2006). Introducción a la metodología de la investigación. edición electrónica. *Lectura en línea. Recuperado http://www.eumed.net/libros/2006c/203/.*

Betancur López, S. I. (2000). Operacionalización de variables. *[Lectura en Línea] Recuperado de: http://promocionsalud.ucaldas.edu.co/downloads/Revista 205_4.pdf*, pages 29–36.

Buades, G. (2002). Auditoría informática. *Ingeniería del Software. http://www.emagister.com/uploads_user_home/Comunidad_Emagister_8381_auditoria.pd*

(COIP) (2014). Código orgánico integral penal del ecuador. *[Lectura en Línea] Recuperado de: http://www.derechoecuador.com/articulos/detalle/archive/legislacion/codigos/2014/02/24/c organico-integral-penal.* Internet.

Cruz Jaramillo, M. B. (2011). Riesgo de liquidez y su incidencia en la rentabilidad de las oficinas operativas de la cooperativa de ahorro y crédito oscus cia ltda en la provincia de tungurahua en el año 2010. *http://repo.uta.edu.ec/bitstream/handle/123456789/1765/TA0085.pdf.*

Ecuadorinmediato (2013). Roban más de 13 millones de cuenta del municipio de riobamba. *http://www.ecuadorinmediato.com/index.php?module=Noticias&func=news_user_view&id=*

Enríquez Miranda, J. F. (2010). Políticas de seguridad informática y la vulnerabilidad de los entornos web de la empresa turbotech durante el año 2010. Master's thesis, Universidad Técnica de Ambato: Facultad de Ingeniería en Sistemas, Electrónica e Industrial. Internet.

Ferrer, J. (2010). Conceptos básicos de metodología de la investigación. *http://metodologia02.blogspot.com/p/operacionalizacion-de-variable_03.html*.

Franco, Y. (2011). Investigación de campo. manual upel. *http://tesisdeinvestig.blogspot.com/2011/07/investigacion-de-campo-manual-upel.html*.

FUNDACION DE ESTUDIOS SUPERIORES DR. PLACIDO MARIN, C. (s.f.). Estrategias de resolución de problemas. *http://www.cad.marin.edu.ar/pictures/novedades/MATERIAL17deMayo.doc*.

Grajales, T. (2000). Tipos de investigación. *http://www.iupuebla.com/Maestrias/M_E_GENERO/MA_Maestria_Genero/Jose_Migue de investigacion.pdf*.

Gross, M. (2010). Conozca 3 tipos de investigación: Descriptiva, exploratoria y explicativa. *Pensamiento Imaginativo. Blog.[Lectura en Línea] Recuperado de: http://manuelgross.bligoo.com/conozca-3-tipos-de-investigacion-descriptivaexploratoria-y-explicativa*.

Hernández Sampieri, R., Fernández Collado, C., and Baptista Lucio, P. (2010). Metodología de la investigación. *México: Editorial Mc Graw Hill. Recuperado de: http://www.upsin.edu.mx/mec/digital/metod_invest.pdf*.

Herrera, L., Medina, A., and Naranjo, G. (2004). Tutoría de la investigación científica. *Quito–Ecuador.*, 107.

ISACA (2013). Gestión del riesgo de la información ejemplos reales. *http://www.isaca.org/Education/Conferences/Documents/Latin-CACS-2013-Presentations/242.pdf*.

Leydiani, M. G. (2011). Directorio activo. *http://www.ecured.cu/index.php/Directorio_Activo*.

Markus, E. (2009). Gestión de riesgo en la seguridad informática. *http://protejete.wordpress.com/gdr_principal/amenazas_vulnerabilidades/*.

Martinez Alegre, F. (2011). ¿qué es el directorio activo de microsoft? *http://www.martinezalegre.com/2011/03/que-es-el-directorio-activo-de-microsoft/*.

Mayorga Jácome, T. C. (2013). Seguridad informática y la relación en la utilización de internet como herramienta de apoyo en la formación de niños, niñas y

adolescentes de educación inicial y básica del centro educativo "la pradera". Master's thesis, Universidad Técnica de Ambato.

Microsoft (2005). Función de servidor de archivos. *http://msdn.microsoft.com/es-es/library/cc780253 28v=ws.10 29.aspx*.

Microsoft (2008). Guía paso a paso de la directiva de auditoría de seguridad avanzada. *http://technet.microsoft.com/es-es/library/cc770946 28v=ws.10 29.aspx*.

Mieres, J. (2009). Ataques informáticos. *Debilidades de seguridad comúnmente explotadas. http://proton. ucting. udg. mx/tutorial/hackers/hacking. pdf*. Internet.

Namakforoosh, M. N. (2000). Metodología de la investigación. *http://books.google.es/books?hl=es&lr=&id=ZEJ7-0hmvhwC&oi=fnd&pg=PA219&ots=i-3DwUTf43&sig=PVumier3P7zJhifinItDqxM7qKk#v=*

Ochoa Correa, V. A. (2010). Auditoría de redes. *http://vochoa84.files.wordpress.com/2011/10/auditoria-en-redes.pdf*.

Ortin, J. M. (2013). ¿qué es un sistema de gestión de seguridad de la información (sgsi)? *http://blog.firma-e.com/que-es-un-sgsi-sistema-de-gestion-de-seguridad-de-la-informacion/*.

Ortiz, J. R. (1998). La educación a distancia en el umbral del nuevo paradigma telemático. *Informe de Investigaciones Educativas. http://biblo.una.edu.ve/ojs/index.php/UNADO/article/view/305/291*, 12(1-2):139–153.

Pita Fernández S., P. D. S. (2002). Investigación cuantitativa. *http://www.fisterra.com/mbe/investiga/cuanti_cuali/cuanti_cuali.asp*.

Rivas, G. A. (1989). *Auditoría informática*. Ediciones Díaz de Santos.

Rivero, D. (2013). Configurar directorio activo (active directory) en gnu/linux centos 6.3 con samba 4.0.1. *https://www.lastdragon.net/?p=709*.

RTVE.es (2013). Sitio web televisión española. *http://www.rtve.es/noticias/20130507/pentagono-acusa-china-ataques-informaticos-contra-sistema-defensa/657500.shtml*.

Salazar, J. B. and Campos, P. G. (sf). Modelo para la seguridad de la información en tic. *http://ceur-ws.org/Vol-488/paper13.pdf*. Internet.

Sampieri, R. H., Collado, C. F., Lucio, P. B., and Pérez, M. d. l. L. C. (1998). *Metodología de la Investigación*. McGraw-Hill México.

ANEXOS

Anexo A

Otro Anexo

Texto del segundo anexo