UNIVERSIDAD TÉCNICA PARTICULAR DE LOJA

La Universidad Católica de Loja

ÁREA TÉCNICA

TITULO DE INGENIERO EN INFORMÁTICA

Implementación de seguridades de la información y plan piloto para uso de Software Libre en la cooperativa de ahorro y crédito CACPE Manabí.

TRABAJO DE TITULACIÓN.

AUTOR: Burgos Alonso, Richard Fabián

DIRECTOR: Jaramillo H., Danilo, Msc.

CENTRO UNIVERSITARIO PORTOVIEJO

2017

Septiembre, 2017

APROBACIÓN DEL DIRECTOR DEL TRABAJO DE TITULACIÓN

Msc.
Danilo Jaramillo H.
DOCENTE DE LA TITULACIÓN

De mi consideración:

El presente trabajo de titulación: “Implementación de Seguridades de la Información y plan piloto para uso de Software Libre en la cooperativa de ahorro y crédito CACPE Manabí”, realizado por Burgos Alonso Richard Fabián, ha sido orientado y revisado durante su ejecución, por cuanto se aprueba la presentación del mismo,

Loja, mayo de 2017

f)……..

DECLARACIÓN DE AUTORÍA Y CESIÓN DE DERECHOS

Yo Burgos Alonso Richard Fabián declaro ser el autor del presente trabajo de titulación: "Implementación de Seguridades de la Información y plan piloto para uso de Software Libre en la cooperativa de ahorro y crédito CACPE Manabí", de la Titulación de ingeniero en informática, siendo Msc. Danilo Jaramillo H. director del presente trabajo; y eximo de forma expresa a la Universidad Técnica Particular de Loja y a sus representantes legales de posibles reclamos o acciones legales. Además certifico que las ideas, conceptos, procedimientos y resultados vertidos en el presente trabajo investigativo, son de mi exclusiva responsabilidad.

De forma adicional declaro conocer y aceptar la disposición del Art. 88 del Estatuto Orgánico de la Universidad Técnica Particular de Loja que en su parte pertinente de forma textual dice: "Forman parte del patrimonio de la Universidad la propiedad intelectual de investigaciones, trabajos científicos o técnicos y tesis de grado o trabajos de titulación que se realicen con el apoyo financiero académico o institucional (operativo) de la Universidad"

f.……..

Autor: Burgos Alonso Richard Fabián

Cédula 1306416874

DEDICATORIA

A mis Padres, esposa e hijos, fuente de fuerza y persistencia a través de estos años para alcanzar este sueño que empezó a los 13 años; titularme como profesional en el área de las Ciencias de la Computación.

El camino fue largo y difícil, primero como técnico en sistemas, tecnólogo en análisis de sistemas, certificado CCNA y finalmente Ingeniero.

Richard Fabián Burgos Alonso

AGRADECIMIENTO

A Dios por la bendición y salud que me ha brindado en cada día de mi vida, a mis padres Justina y Luis incondicionales siempre, a todos mis familiares y amigos, por el apoyo moral y económico durante el camino recorrido en estos años de estudios; para llevar a buen término mi carrera profesional.

Un agradecimiento también al Msc. Danilo Jaramillo, a la Ing. María Burgos, al Ing. Gabriel Morejón y al Sr. Víctor Andrade por el apoyo brindado durante el desarrollo de este proyecto.

Richard Fabián Burgos Alonso

ÍNDICE DE CONTENIDOS

LISTADO DE TABLAS

LISTADO DE GRÁFICOS

RESUMEN

Ante la constante evolución y a fin de mantener la competitividad para brindar facilidad al cliente, las empresas recurren a la automatización de sus procesos por medio de la implementación de paquetes de software de gestión integral.

Para lograr la interacción entre la organización y sus clientes o proveedores según el caso, se vuelve indispensable el uso de sistemas y redes informáticas que permitan la comunicación entre ellos.

La información a la que se da soporte en dichos sistemas, pasa a ser un factor de suma importancia, misma que se expone a un universo de amenazas y vulnerabilidades que conforme el tiempo pasa estos problemas suelen ir en aumento.

La disponibilidad, integridad y confidencialidad de la información, requiere en todo organismo del diseño e implementación de planes de seguridad lógicos y físicos para cumplir alcanzar dichos objetivos y la Cooperativa de Ahorro y Crédito CACPE Manabí se une a las exigencias del mundo globalizado con el uso de programas de seguridad de la información y el plan piloto para uso del Software Libre por medio de este trabajo de titulación.

PALABRAS CLAVES: Software libre, sistemas, redes informáticas,

ABSTRACT

Given the constant evolution and in order to maintain the competitiveness to provide ease to the customer, companies resort to the automation of their processes through the implementation of integral management software packages.

In order to achieve interaction between the organization and its customers or suppliers as the case may be, it becomes indispensable to use computer systems and networks that allow communication between them.

The information that is supported in such systems, becomes a very important factor, which is exposed to a universe of threats and vulnerabilities that as time passes these problems are increasing.

The availability, integrity and confidentiality of the information requires, in every body, the design and implementation of logical and physical security plans to meet these objectives and the Savings and Credit Cooperative. Manabí joins the demands of the globalized world with the use of information security programs and the pilot plan for use of Free Software by means of this titling work.

KEYWORDS; Free software, systems, computer networks,

INTRODUCCIÓN

Este proyecto “Implementación de Seguridades de la Información y plan Piloto para uso de software libre en la Cooperativa de Ahorro y Crédito CACPE Manabí”, tiene como objetivo dotar de las herramientas que permitan dar seguridad en la información y fomentar el uso de software libre en este organismo, y proteger la información de amenazas internas y externas, para reducir y optimizar gastos, permitir mejoras en el servicio y a la vez mantenerse a la par en innovación como las grandes entidades financieras.

El trabajo se subdivide en cinco capítulos, los cuales constan:

Capítulo I, hace referencia a la situación actual de la CACPE Manabí, en la que se constata la falta de políticas y controles a nivel de TI, entre otras falencias; así mismo se hace un inventario de los equipos que posee la entidad financiera, y el registro del Software, diseño de la red informática, los objetivos, el planteamiento del problema y la metodología a usarse para la solución del problema.

El Capítulo II, trata el estado del Arte, los ataques y peligros a los que están expuestos los sistemas y las redes, ya sean internos o externos; por lo que se requiere de seguridades que protejan los equipos, y por ende la información en ellos almacenada; concepto de redes informáticas, tipos de redes que existen y las funciones que desempeñan cada una, los objetivos que persigue la seguridad informática y la seguridad física, plan de contingencia, plan de diseño, basados en la normativa ITIL, las ventajas y desventajas, en qué cosiste el programa Estándar ISO 27001 y el Software Libre; el marco referencial que comprende de una forma práctica el planteamiento del problema, políticas de seguridad, gestión de la información, entre otros.

El Capítulo III, se refiere a la definición de las políticas de seguridad en la información aplicable en la CACPE – Manabí, los roles y responsabilidades de los colaboradores de la cooperativa, la aplicabilidad y factibilidad de uso del Software Libre, entre otros aspectos.

El Capítulo IV, se analizan las políticas de seguridad para la información, la ejecución de las mismas, la implementación de servidores, la implementación del plan piloto para la migración de estaciones de trabajo a Software libre, las pruebas y resultados de las encuestas aplicadas.

El Capítulo V, que hace referencia a las conclusiones y recomendaciones de este trabajo; la bibliografía, los anexos que forman parte de las evidencias del trabajo realizado, así como las encuestas y configuraciones.

Vale señalar que los objetivos de este trabajo se cumplieron, la implementación del Plan para la Seguridad de la Información y el Plan Piloto para uso de Software Libre en la estación de trabajo designada para el efecto; se implementó un servidor que permita centralizar y controlar el acceso al internet, control de identificación de usuarios, aplicación de firewall perimetral, y se implementó el Plan Piloto para Migración de Estaciones de trabajo a Software Libre.

El trabajo inicial fue complicado, por la falta de políticas y procesos claros en la CACPE – Manabí; sin embargo conforme se fue afianzando este proyecto, la obtención de información fue más sencilla, permitiendo formar una dinámica buena en el desarrollo del trabajo con la colaboración del personal de la Cooperativa.

En síntesis se puede decir que después del trabajo, se pudo solucionar el problema planteado, aplicando para el desarrollo del trabajo una metodología descriptiva, de campo y aplicada, siendo descriptiva porque se determinaron los problemas existentes en la entidad financiera, de campo porque se acudió al lugar donde funciona la CACPE – Manabí, y aplicada porque con la implementación de seguridades en la información y el plan piloto para uso de software libre, se resuelve el problema detectado.

CAPÍTULO I: SITUACIÓN ACTUAL

1.1. SITUACIÓN ACTUAL.

La Cooperativa de Ahorro y Crédito CACPE Manabí adquirió su personería jurídica mediante acuerdo Ministerial n° 01238 del 16 de julio de 1990, regulada por la Dirección Nacional de Cooperativas del Ministerio de Inclusión Económica y Social, domiciliada en la ciudad de Portoviejo, Provincia de Manabí, República del Ecuador, de derecho privado, su actividad principal es de intermediación monetaria realizada por Cooperativas, que funcionan en sus instalaciones propias ubicada en la ciudad de Portoviejo, calle Ricaurte entre Sucre y Bolívar.

La **misión** es ofrecer servicios cooperativistas de calidad a la colectividad para contribuir a su bienestar y desarrollo. Logrando una **visión** de una estructura organizacional sólida definida, con recurso humano capacitado, teniendo como **Objetivo General** el de lograr una gestión administrativa y financiera eficiente que permita competir y ganar un espacio en el mercado local y provincial. (Cooperativa CACPE Manabí., 1990)

Parte de este servicio de calidad es el ámbito informático que posee, ante lo cual es necesario conocer la situación actual de la misma en lo referente al ámbito informático.

De la verificación realizada se pudo constatar que la Cooperativa tiene:

- Una infraestructura de Hardware al alcance de cualquier usuario sin restricción alguna.
- No dispone de Políticas y Controles en Seguridades de TI
- Un sistema de red inseguro.
- No existe registro sobre el control de los equipos de cómputo, vigilancia y red.
- No hay definición de permisos de acceso a aplicativos por usuarios.
- Los computadores tienen conexión directamente al internet.
- La comunicación se realiza por medio de computadores que no tienen ningún control en lo referente a la conexión de Internet, no existe protección por firewall.
- Los computadores tienen todos los puertos USB, unidades lectoras de CD, habilitados.
- No hay inventario de los equipos de cómputo, ni equipos de red.

Dado este escenario no es viable que pueda ofrecer un servicio de calidad, ya que la utilización de herramientas informáticas que permitan la facilidad de obtención de la información de un cliente, en forma confidencial y eficaz por parte de la Cooperativa forma parte del servicio de calidad que se menciona.

1.1.1. INVENTARIO DE HARDWARE.

Como uno de los primeros pasos en la elaboración del proyecto, se identificó la necesidad de realizar una evaluación del hardware existente en la cooperativa, de esta evaluación se determinó que:

La organización no posee registros de los equipos con los que cuentan actualmente. Los equipos se han ido adquiriendo según la necesidad sin ningún ingreso a inventario, por lo que se procedió a realizar el registro del Hardware que posee la Cooperativa y se muestra en las tablas 1 y 2:

Tabla 1. Equipos de la Cooperativa

Área	Equipo	Procesador	Memoria RAM	Disco Duro
Gerencia	PC de Escritorio Clon	Intel Pentium 4 CPU 3.20 GHz	1 Gb	
Contabilidad – Financiero	PC de Escritorio Clon	Intel Core i3 540 3.07 GHz	2 Gb	500 Gb
Crédito – Cobranzas	PC de Escritorio Clon	Intel Celeron 430 1.8 GHz	2 Gb	300 Gb
Caja	PC de Escritorio Clon	Intel 2140 1.6 GHz	512 Mb	
Informática	IBM System X3200 M2	Xeon 2Ghz	8 Gb	1 Tb

Fuente: Coop. de Ahorro y Crédito CACPE Manabí.

Elaboración: Burgos Alonso Richard

Tabla 2. Equipos Adicionales de la Cooperativa.

Área	Equipo	Marca	Modelo
Contabilidad – Financiero	Impresora	Canon	Pixma MP280
Contabilidad – Financiero	Impresora	Epson	Fx-2190
Crédito – Cobranzas	Impresora	HP	LaserJet P1102W
Caja	Impresora	Lexmark	X1270

Caja	Impresora	Citizen	GSX-190
Informática	Switch	3COM	Baseline 2024
Informática	Router	D'Link	DIR-655

Fuente: Coop. de Ahorro y Crédito CACPE Manabí.

Elaboración: Burgos Alonso Richard

1.1.2. INVENTARIO DE SOFTWARE.

Continuando con la evaluación inicial con lo que se cuenta en la Cooperativa, se procedió a realizar el registro del Software existente en los equipos, en la tabla 3 se presentan los resultados:

Tabla 3. Software de la Cooperativa.

Área	**Equipo**	**Sistema Operativo**	**Software**
Gerencia	PC de Escritorio Clon	Windows 8.1 32 bits	ESET NOD32
Contabilidad – Financiero	PC de Escritorio Clon	Windows 7 32 bits	Microsoft Office 2010 SADFIN ESET NOD32
Crédito – Cobranzas	PC de Escritorio Clon	Windows XP SP3	Microsoft Office 2010 SADFIN
Caja	PC de Escritorio Clon	Windows 7 Starter 32 bits	Microsoft Office 2010 SADFIN
Informática	IBM System X3200 M2	Centos 5.0	

Fuente: Coop. de Ahorro y Crédito CACPE Manabí.

Elaboración: Burgos Alonso Richard

1.1.3 RED INFORMÁTICA.

Se evaluó la situación actual de la Cooperativa en lo referente a la Arquitectura de Red, misma que se representa en el gráfico 1.

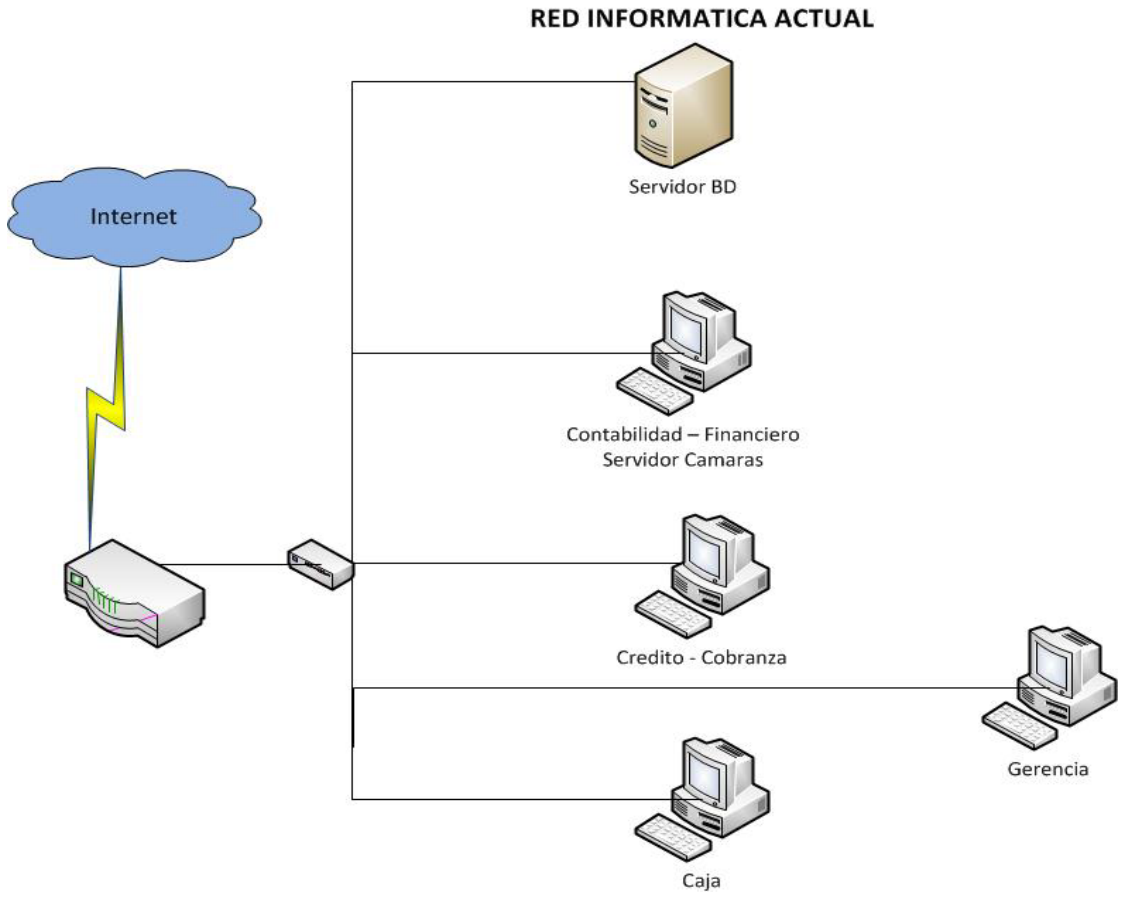


Gráfico 1. Red Informática Actual
Elaboración: Burgos Alonso Richard

Como se puede observar en el gráfico 1, la comunicación entre el internet y la red de la Cooperativa se da de forma directa, estableciendo una red LAN punto a punto, en donde todas las computadoras integrantes de la red pueden hacer el rol de cliente o servidor no dedicados, sin ningún filtro y/o control que pueda minimizar el riesgo de accesos no deseados, determinando así una falencia grave para la organización.

1.2 PLANTEAMIENTO DEL PROBLEMA.

La Cooperativa no cuenta con departamento de informática, ante lo cual la administración de la seguridad de la información que se maneja es nula, el software financiero que se utiliza

necesita actualizarse, las estaciones de trabajo no cuentan con software licenciado y están directamente enlazadas al internet sin ningún medio de defensa ante posibles ingresos indebidos, los empleados de la institución no tienen ningún conocimiento sobre seguridad de la información, tienen libre acceso a las máquinas de la institución y no hay definición de responsabilidades en el manejo de la información, por lo cual la institución se encuentra en estado vulnerable y en serio riesgo de ser víctima de ataques de diferente índole en el ámbito informático.

De acuerdo con los datos recopilados y visualizados en la cooperativa, han permitido detectar ciertas falencias en el ámbito informático, por lo que se hace necesario y recomendable la implementación de seguridades en la información y un plan piloto para fomentar el uso de software libre en la CACPE Manabí, que fortalezca el desarrollo de las actividades diarias financieras que realiza la Organización, planteándose la siguiente interrogante:

¿Cuál es el impacto que generaría en las actividades financieras de la CACPE Manabí, al no contar con políticas de Control y accesos internos y externos a los contenidos y aplicativos de la empresa Financiera?

1.3 OBJETIVOS.

1.3.1 OBJETIVO GENERAL

Diseñar e implementar el Plan para la Seguridad de la Información y el Piloto para uso de Software Libre en las estaciones de trabajo de la Cooperativa CACPE - Manabí.

1.3.2 OBJETIVOS ESPECÍFICOS.

- Determinar la situación actual de la red Informática, políticas y controles de TI en la Cooperativa.
- Diseñar, desarrollar e Implementar políticas de control y accesos tanto internos y externos a contenidos (información y datos), como a los aplicativos.
- Implementar un servidor que permita centralizar y controlar el acceso al internet, control de identificación de usuarios, aplicación de firewall perimetral.
- Implementar el Plan Piloto para migración de estaciones de trabajo a software libre.

1.4. PLANTEAMIENTO DE SOLUCIÓN AL PROBLEMA.

De lo expuesto se plantean alternativas como solución para la cooperativa:

- La implementación de un plan de seguridad de la información a través de políticas de control y accesos internos y externos, tanto a contenidos (información y datos), como a los aplicativos.
- La implementación de una Arquitectura de red para la seguridad y enrutamiento de la información de la Cooperativa como se establece en el gráfico 2.

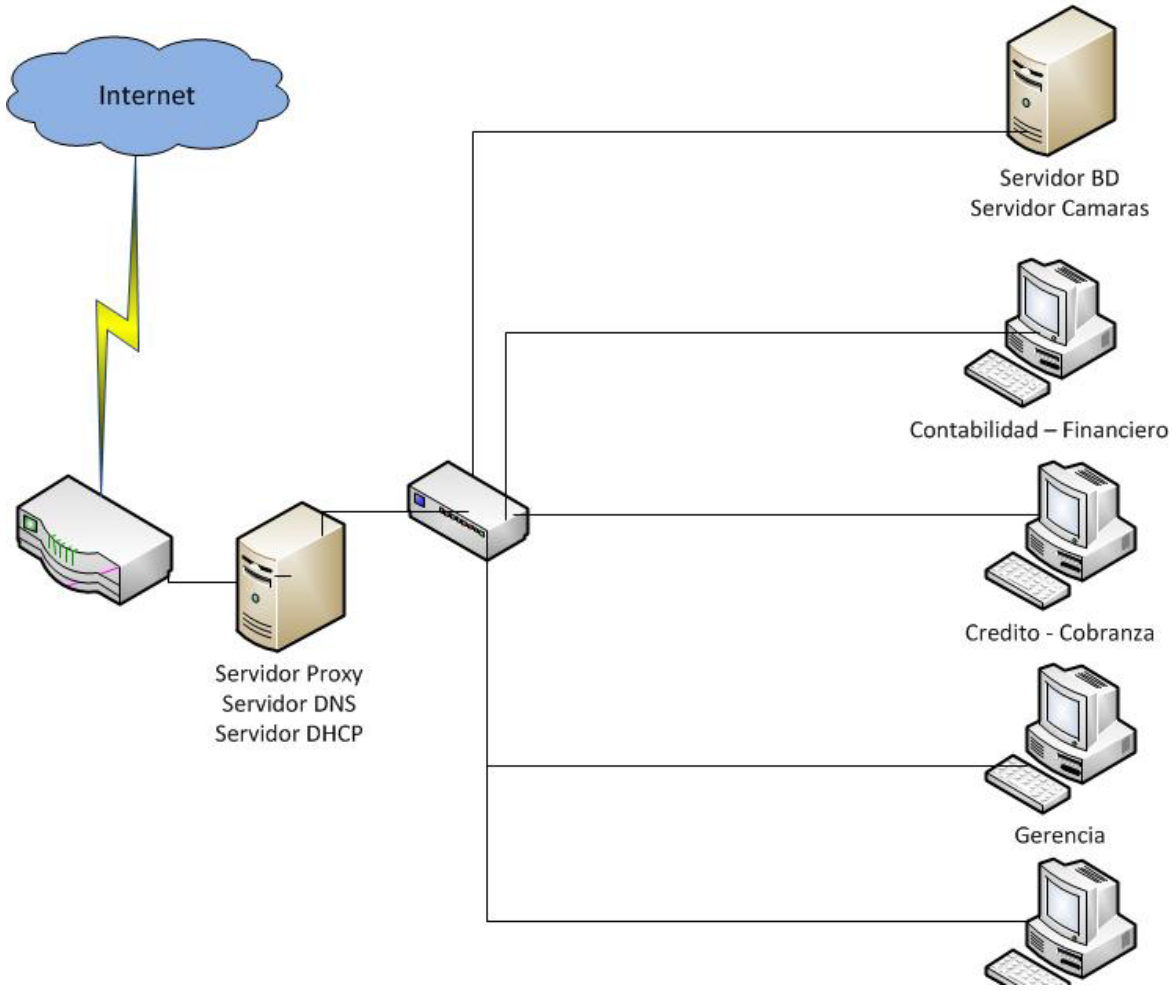


Gráfico 2. Red Informática Propuesta.

Título: Red Propuesta.

Elaboración: Burgos Alonso Richard

- La Aplicación de un Plan Piloto para fomentar el uso de software libre en el Departamento de Crédito y Cobranza, a fin de disminuir costos operativos asi como aprovechar los recursos de hardware existentes en la cooperativa, ofrecer una mayor garantía en seguridad de la información, flexibilidad en la adaptación e integración, contribuyendo en la optimización de la inversión y protección de los ahorros de los clientes de agentes externos e internos que representen potenciales riesgos para la cooperativa.

1.5. Metodología para la solución del problema.

La metodología aplicada para la solución del problema es la siguiente:

- Implementación del plan base para la seguridad de la informacion.
- Elección de las herramientas a utilizar.
- Desarrollo de las siguientes fases para obtener los objetivos propuestos:
    - Fase 1: Implementación de la red informática.
    - Fase 2: Implementación del plan base para la seguridad de la informacion.
    - Fase 3: Ejecución de políticas, servidores y controles en la red informática.
    - Fase 4: Implementación de Plan Piloto de software libre en la Organización.
    - Fase 5: Pruebas en la red informática.

Refiérase al Anexo 1 para verificar el cronograma de trabajo representado mediante un diagrama de Gantt.

CAPÍTULO II: MARCO TEÓRICO

2.1. ESTADO DEL ARTE.

En el mundo actual con una posibilidad de comunicación y distribución de información tan versátil, con un avance tecnológico que acorta distancias y reduce tiempos, lleva consigo riesgos de pérdida, robo, sustracción, modificación y alteración de la información.

En una organización la información que tiene, es uno de sus bienes mas preciados, por lo cual esta información debe ser protegida a través de mecanismos que garanticen su disponibilidad, integridad y confidencialidad. (G.Aucapiña, T. Guachi, 2012)

Los sistemas y redes, así como la información que fluye dentro de ellos, están de forma constante expuestos a varios ataques que pueden ser internos o externos, y la frecuencia de ocurrencia de los mismos que cada vez es mayor, nos pone en la necesidad de establecer políticas y controles de TI, para proteger nuestros equipos y los datos e información que en ellos se almacenan.

Es ahí donde cobra importancia el área de Tecnologías de la Información de una organización, pues en esta área se debe establecer los mecanismos para proteger la información que posee, asi como buscar la optimización continúa en recursos y las seguridades necesarias para minimizar los riesgos de ataques a los que la información pueda estar expuesta.

2.2. MARCO CONCEPTUAL.

Para la realización de este proyecto se va a tomar en cuenta conceptos sobre Red informática, la seguridad de la información, Control de Accesos, Cuenta de Usuario, Delimitación de Servicio, Niveles de Seguridad Informática, seguridad física, Plan de Contingencia, Plan de diseño basado en normas como ITIL, estándar ISO 27001, utilización de software libre, a continuación se realiza una descripción de ellos.

2.2.1 RED INFORMÁTICA.

Una Red informática, también denominada red de computadoras, es un conjunto de equipos informáticos y/o dispositivos móviles conectados entre sí a dispositivos físicos por medio de cables, ondas electromagnéticas o cualquier otro medio de transporte de datos, que les permite compartir información (archivos), recursos (impresoras, lectores de cd, unidades de almacenamiento) y servicios (acceso a internet, email, chat, juegos). (Dordoigne, 2015)

La red informática puede estar conformada de diferentes maneras, las cuales mencionaremos a continuación.

Tipos de Redes

Existen diferentes formas de clasificar los tipos de redes, es así que aquí hemos de mencionar el tipo de redes por alcance, por relación funcional, por topología física, por servicio.

Por Alcance

Red de área local o LAN (Local Area Network): Es una red que conecta equipos en un área geográfica limitada, como una oficina o edificio. De esta manera se tiene una conexión rápida, sin inconvenientes, donde todos tienen acceso a la información, recursos y servicios sin mayor inconveniente.

Red de área metropolitana o MAN (Metropolitan Area Network): Esta red abarca un área geográfica que puede alcanzar un equivalente a una ciudad. Utiliza una tecnología análoga a las redes LAN, y se basa en la utilización de dos buses de carácter unidireccional, independientes entre sí en lo que se refiere a la transmisión de datos.

Red de área amplia o WAN (Wide Area Network): Redes que conectan equipos ubicados en áreas geográficas extensas, por ejemplo distintos continentes, la conexión se realiza a través de fibra óptica o satelital.

Redes inalámbricas (Wireless Local Area Network): Un sistema de transmisión de información de forma inalámbrica, por medio de satélite o microondas, estas se pueden dividir en tres categorías: Interconexión de sistemas, LAN inalámbricas, WANs inalámbricas.

Redes domésticas: la conectividad doméstica, en el cual se tiene la posibilidad de que diversos dispositivos (televisores, consolas, celulares, entre otros) se conecten a la red y puedan acceder al internet.

Interredes: Diferentes redes interconectadas, por ejemplo, diferentes LANs conectadas por una WAN. (Tanenbaum, 2003)

Por relación funcional

Cliente - Servidor: este tipo de red establece la relación entre hardware y/o software, uno que hace el rol de cliente realizando una petición y uno que cumple el rol de Servidor que recepta y responde al pedido realizado.

Peer - to - Peer: red entre iguales, en el cual cualquier computador hacer las veces de cliente o servidor. (Tanenbaum, 2003).

Por topología física

Red de bus: se basa en un solo canal de comunicaciones, al cual se conectan los diferentes equipos.

Red de anillo: Cada equipo está conectado al siguiente y el último se conecta con el primero.

Red de estrella: Los equipos se encuentran conectados directamente a un equipo central y todas las comunicaciones se han de hacer necesariamente a través de éste.

Red de malla: Cada equipo está conectado a todos los equipos de la red.

Red en árbol: los equipos están colocados en forma de árbol, este tipo de red vendría a ser una serie de redes en estrella interconectadas solo que sin un nodo central.

Por Servicio

Red comercial: Proporciona soporte e información para una empresa u organización con fines de lucro.

Red educativa: Proporciona soporte e información para una organización con fines educativos.

Red para procesamiento de datos: Soporte para intercomunicación de equipos para procesamiento de datos. (Kuroe J., 2010)

2.2.2 SEGURIDAD DE LA INFORMACIÓN.

La mayoría de las actividades que se realizan cotidianamente en la actualidad, se ven influenciadas en mayor o menor medida por sistemas y redes informáticas.

Muchos de los servicios financieros, de transporte, suministro eléctrico entre otras son ejemplo latente de ellos y que en algunos casos han eliminado los procesos manuales.

Estos servicios para la sociedad tienen una dependencia de los sistemas y redes informáticas, que crean un espacio para ser blanco de ataques, por lo cual se hace necesaria la implementación de seguridades de la información.

Entendiéndose por seguridad de la información a las medidas adoptadas para la protección de un sistema o red informática. A continuación se mencionan otras definiciones:

“La ISO/IEC 17799 define la seguridad de la información como la preservación de su confidencialidad, su integridad y su disponibilidad (medidas conocidas por su acrónimo “CIA” en inglés: “Confidentiality, Integrity, Availability”).”

“La ISO 7498 define la Seguridad Informática como “una serie de mecanismos que minimizan la vulnerabilidad de bienes y recursos en una Organización”

INFOSEC GLOSSARY 2000: “seguridad Informática son las medidas y controles que aseguren la confidencialidad, integridad y disponibilidad de los activos de los sistemas de información, incluyendo Hardware, software, firmware y aquella información que procesan, almacenan y comunican” (Gómez A. , 2011).

Entre los objetivos que se persigue en la Seguridad de la información, podemos mencionar:

- Minimizar y Gestionar los riesgos, detectar los posibles problemas y amenazas a la seguridad.
- Confirmar la utilización correcta de los recursos, aplicativos e información del Sistema y red informática.
- Delimitar los accesos a los usuarios del sistema, impedir la alteración y/o manipulación de la información por personal no autorizado.
- Establecimiento de planes de contingencia para reactivación del sistema en caso de incidentes de seguridad.
- Verificar el cumplimiento del marco legal y requerimientos establecidos en los contratos.

2.2.3. CONTROL DE ACCESOS.

El control de acceso busca la autentificación de usuarios como medio de control para el acceso a un sistema o red informática, tratando de minimizar el acceso no autorizado a recursos e información de la organización.

Estos controles pueden ser aplicados al sistema operativo, base de datos, aplicativos específicos o equipos de la red informática que se encuentran dentro de la organización. (Gómez A. , 2011).

En una organización es deber del área de tecnologías de la información, establecer este tipo de control en colaboración con el personal, así como informar al mismo de las responsabilidades a los que están sujetos una vez les sea proporcionados su usuario y contraseña para el acceso a la información.

2.2.4 TIPO DE CUENTA.

El acceso a los equipos es posible también controlarlo a través de un tipo de cuenta, dependiendo de este se determina que privilegios puede tener un usuario sobre el sistema de información, en ciertos casos este privilegio determina control total sobre el sistema, así como en otros casos un acceso limitado. Para el caso del proyecto se establecen como:

Administrador: privilegios totales, siendo este tipo el encargado de la ejecución y verificación del cumplimiento de las políticas y controles de seguridad establecidos para el sistema y red informática.

Usuario: privilegios limitados, este tipo tendrá los privilegios y derechos establecidos por las políticas y controles de seguridad de la información. (Gómez A. , 2011).

2.2.5 DELIMITACIÓN DE SERVICIO.

El área de tecnologías de la información en coordinación con la dirección de la organizacion, establecen los límites que tendrán los colaboradores en el manejo de la información que posee.

Se establece los controles que determinan los privilegios que tiene determinado usuario según las características propias de los aplicativos del sistema o establecidos por el administrador del Sistema.

Con la delimitación de servicio que se establece para ser utilizable por los colaboradores en una organización, se busca tener una productividad efectiva en benficio de la organización. (Solarte, 2015)

2.2.6 NIVELES DE SEGURIDAD INFORMÁTICA.

Para establecer los niveles de seguridad es necesario conocer el TCSEC Orange Book[1], estándar reconocido internacionalmente y desarrollado por el Departamento de Defensa de los Estados Unidos entre 1983 - 1985.

[1] Trusted Computer System Evaluation Criteria (TCSEC) es un Departamento de Defensa (DoD) estándar que establece los requisitos básicos para evaluar la eficacia de los controles de seguridad informática integradas en un sistema informático del Gobierno de los Estados Unidos. El TCSEC se utilizó para evaluar, clasificar y seleccionar los sistemas informáticos considerando el procesamiento, almacenamiento y recuperación de información sensible o clasificada.

La base de desarrollo de Estándares como (ITSEC/ITSEM) y luego estándares internacionales como (ISO/IEC), han sido los niveles de seguridad, los que detallamos acontinuacion.

Los datos deben clasificarse, para llevar a cabo dicha clasificación se debe partir de la necesidad de la confidencialidad de los mismos. Los niveles globales fundamentados en la posibilidad de un potencial daño de ser comprometidos son los siguientes:

- Súper Secreto
- Secreto
- Confidencial
- No Clasificado:
    - ➢ Sensible pero no clasificada.
    - ➢ Solo para uso oficial.

Nivel D: Protección mínima.

Se clasifica como nivel D aquellos sistemas que siendo evaluados, no tienen mayores políticas de seguridad y por ende no brindan mayor protección ante posibles ataques. Son sistemas poco confiables, sin ninguna protección o seguridad para el hardware, que contiene un sistema operativo inestable y sin ninguna validación en relacion a los usuarios y sus derechos para el acceso a la información. Podemos mencionar como sistemas operativos que responden a este nivel a MS-DOS y System 7.0 de Macintosh. (Sosa, 2012)

Nivel C1: Protección discrecional

En este nivel la identificación de usuarios es requerida y permite el acceso a diversa información. Cada usuario maneja su información de forma privada y se ejecuta la clasificacion entre el nivel usuario y el nivel administrador del sistema, en el nivel de administrador del sistema se tiene acceso y control total al sistema. La mayoria de las tareas cotidianas de administración del sistema solo pueden ser realizadas por este “súper usuario” mismo que conlleva una gran responsabilidad en la seguridad del sistema. Con la actual descentralización de los sistemas de cómputo, es comun encontrar en una organización dos o tres personas cumpliendo el rol de adminstrador. Esto es un problema, pues no hay forma de distinguir entre los cambios que hizo cada usuario.

Según (Sosa, 2012) los requerimientos mínimos que debe cumplir la clase C1, se detallan acontinuacion:

- Acceso de control discrecional: clasificación entre tipos de usuarios y recursos. Mediante la definicion de grupos de usuarios (con los mínimos privilegios) y grupos de objetos (archivos, directorios, disco) sobre los cuales podrán interactuar usuarios o grupos de ellos.
- Identificación y autenticación: Un usuario necesitara identificarse antes de poder comenzar a ejecutar acciones sobre el sistema. El dato de un usuario no podrá ser accedido por un usuario sin autorización o identificación.

Nivel C2: Protección de acceso controlado

El diseño de este Subnivel se basa en solucionar las debilidades del C1. Adiciona características que permiten crear un ambiente de acceso controlado. En la que se debe llevar una auditoria de accesos e intentos fallidos de acceso a objetos.

- Se puede restringir aún más el que los usuarios ejecuten ciertos comandos o tengan acceso a ciertos archivos, permitir o denegar informacion a usuarios especificos con base no solo en los permisos sino también en los niveles de autorización.
- Es necesario que se audite el sistema. Dicha auditoría se utiliza para llevar registros de todas las acciones relacionadas con la seguridad, como las actividades efectuadas por el administrador del sistema y sus usuarios.
- Se requiere de identificación adicional en la auditoria, para garantizar que la persona que ejecuta el comando es quien dice ser, la mayor desventaja reside en los recursos adicionales requeridos por el procesador y el subsistema de discos.
- Los usuarios de un sistema C2 poseen la autorización para realizar algunas tareas de administración del sistema sin necesidad de ser administradores.
- Se establece un mejor registro de las tareas relacionadas con la administración del sistema, debido a que cada usuario ejecuta la tarea y no el administrador del sistema. (Sosa, 2012)

Nivel B1: Seguridad etiquetada.

Este subnivel, es el primero de los tres con que cuenta el nivel B.

- Permite el soporte en seguridad multinivel, como la secreta y ultra secreta. El dueño del un archivo no puede modificar los permisos de un objeto que está bajo control de acceso obligatorio.

- A cada objeto del sistema (usuario, dato, etc.) se le asigna una etiqueta, con un nivel de seguridad jerárquico (alto secreto, secreto, reservado, etc.) y con unas categorías (contabilidad, nomina, ventas, etc.).
- Para acceder a un objeto determinado cada usuario debe poseer un permiso expreso para hacerlo y viceversa. Es decir que cada usuario tiene sus objetos asociados.
- Se establecen controles para limitar la propagación de derecho de accesos a los distintos objetos. (Kizza, 2013)

Nivel B2: Protección estructurada.

- La etiquetación en cada objeto de nivel superior por ser padre de un objeto inferior, siempre sera requerida.
- La protección debe ser estructurada, ya que es la primera que empieza a referirse al problema de un objeto a un nivel más elevado de seguridad en comunicación con otro objeto a un nivel inferior, de esta forma por ejemplo un disco rígido será etiquetado por almacenar archivos que son accedidos por distintos usuarios.
- El sistema es capaz de alertar a los usuarios si sus condiciones de accesibilidad y seguridad son modificadas y el administrador es el encargado de fijar los canales de almacenamiento y ancho de banda a utilizar por los demás usuarios.

Nivel B3: Dominios de seguridad.

- Los dominios de seguridad son reforzados mediante la instalación de hardware: por ejemplo el hardware de administración de memoria se usa para proteger el dominio de seguridad de acceso no autorizado a la modificación de objetos de diferentes dominios de seguridad.
- Existe un monitor de referencia que recibe las peticiones de acceso de cada usuario y las permite o las deniega según las políticas de acceso que se hayan definido.
- Todas las estructuras de seguridad deben ser lo suficientemente pequeñas como para permitir análisis y testeos ante posibles violaciones.
- En este nivel es importante que la terminal del usuario se conecte al sistema por medio de una conexión segura.
- Cada usuario tiene asignado los lugares y objetos a los que puede acceder. (Kizza, 2013)

Nivel A: Protección verificada.

> El Nivel A viene siendo el nivel mas alto de los niveles que conforman esta clasificación de la informacion, donde se incluye un proceso de diseño, control y verificación mediante métodos formales (matemáticos), para asegurar todos los procesos que realiza un usuario sobre el sistema. Para llegar a este nivel de seguridad, todos los componentes de los niveles inferiores deben incluirse. El diseño requiere ser verificado de forma matemática y también se deben realizar análisis de canales encubiertos y de distribución confiable. El software y el hardware son protegidos para evitar infiltraciones ante traslados o movimientos del equipamiento. (Kizza, 2013)

2.2.7 SEGURIDAD FÍSICA.

(Gómez A. , 2011) La seguridad Física de la oficina donde se ubicarán los servidores y equipos de la red informática, generalmente es olvidada en el diseño de un sistema informático.

Sin embargo es importante dotar de una especial protección, de tal forma que se garantice la confidencialidad integridad y disponibilidad de los datos y aplicaciones más críticas. La oficina donde se ubiquen los equipos de servidores y red informática debe disponer de condiciones mínimas de seguridad que minimicen los riesgos de indisponibilidad que pudieran producirse por accidentes involuntarios o predeterminados.

Este tipo de seguridad se basa en minimizar las amenazas que pudieran presentarse por medio del hombre o la naturaleza al medio físico donde se encuentran ubicados los equipos y periféricos del sistema y red informática de la organización:

Entre las amenazas que podemos mencionar en la prevención de la seguridad física, tenemos:

- Amenazas ocasionadas por el hombre (robos, daños).
- Sabotajes deliberados, pudiendo ser estos internos o externos.
- Desastres naturales, incendios, inundaciones, terremotos.

2.2.8 EL USO DE LOS SERVICIOS DE INTERNET EN EL TRABAJO.

En la actualidad el uso del internet se ha vuelto necesario en la mayoría de las organizaciones, situación generada para acortar distancias en un mundo cada vez más globalizado gracias al avance de la tecnología.

Es claro que así como los avances tecnológicos como el caso del internet tienen sus beneficios, también crean puntos negativos, en este caso para las empresas, ya que el empleado al tener libre acceso al internet, puede llegar a caer en la tentación de no solo utilizarlo para beneficio de la empresa sino también para el beneficio propio.

El problema se suscita en una baja en la productividad del empleado, “en un estudio realizado por la empresa de seguridad informática Internet Security Systems (ISS), entre el 30 y el 40 por ciento del uso del internet en la empresa no está relacionado con la actividad laboral, y que dos de cada tres accesos a páginas pornográficas se realizan durante el horario laboral” (Gómez A. , 2011).

El abuso en los accesos al internet y utilización de correos electrónicos, para fines ajenos al trabajo para el cual un empleado fue contratado en una empresa, puede traerle serios problemas que incluso pudieran a llegar ser causal de despido.

2.2.9 HERRAMIENTAS PARA EL CONTROL Y VIGILANCIA DEL ACCESO A LOS SERVICIOS DE INTERNET.

Ante la problemática que pudiera existir por el abuso y mal uso de las herramientas tecnológicas, entendiéndose como una de las más destacadas los servicios que ofrece el internet, por parte de los colaboradores de una organización, esta puede optar por buscar herramientas de control y vigilancia del acceso a los servicios de internet.

- Estas herramientas de control y vigilancias entre sus funciones principales podrían contemplar:
- Bloqueo de direcciones Web a las que la empresa desee impedir el acceso.
- Asignación de los servicios de internet en función del cargo del empleado, según sea el criterio de la organización.
- Utilización de diferentes tecnologías para el filtrado de contenido.

De ser el caso que la empresa opte por la utilización de estas herramientas, la empresa está en la obligación de advertir a los empleados que el uso de los servicios de internet debe ser para fines laborales, y establecer en sus políticas claramente para que fin se tiene los servicios de internet. (Gómez A. , 2011)

De no darse esta advertencia desde el inicio el empleado puede creer tener una privacidad total sobre todas las acciones que realice con los servicios de internet, desde su estación de trabajo. Con lo cual si la empresa intentara realizar un llamado de atención por el mal uso de los servicios, el empleado podría argumentar que nadie le informo que los servicios de internet eran estrictamente para fines laborales.

La falta de delimitación por parte de la empresa hacia sus empleados en lo referente al uso de los servicios de internet, podría acarrear conflictos laborales.

2.2.10 PLAN DE CONTINGENCIA.

En la organización el departamento de tecnologías de la información en conjunto con la dirección, deben definir un plan de contingencia que establezcla un procedimiento de notificación y gestión de incidencias, de tal forma que se pueda realizar una serie de actividades enfocadas a la prevención, predicción y reacción ante posibles situaciones de emergencia que se puedan dar en la entidad.

El Plan de Contingencia podría estar conformado en la siguiente forma:

- **Respaldo:** refiriéndose a todas las medidas preventivas antes de que se presente y/o ejecute una amenaza.
- **Emergencia:** Contempla las medidas necesarias a tomar durante la efectivización de la amenaza o inmediatamente después de que esta haya sido ejecutada.
- **Recuperación:** Son las medidas necesarias a realizar después de haber sido ejecutada la amenaza y posteriormente controlada. (Kizza, 2013)

2.2.11 PLAN DE DISEÑO ITIL.

ITIL **(information Technology Infrastructure Library)** ofrece una colección de mejores prácticas en la administración de servicios de TI para los diferentes tipos de organizaciones.

ITIL no es una metodología de desarrollo de software, ITIL ofrece métodos de control y mejoras a los servicios que se encuentran en producción dentro del negocio.

ITIL genera una descripción detallada de mejores prácticas por medio de procedimientos, roles, tareas y responsabilidades que bien se pueden adaptar a cualquier departamento de TI, dando los elementos necesarios para una mejor comunicación y administración del departamento en la Organización. (Bailey, 2015)

Ventajas de ITIL:

- Mejora la comunicación y calidad de los servicios para con los clientes y usuarios finales a través de los diversos puntos de contacto acordados.
- Se administra mejor la calidad y costos de los servicios.
- Mayor flexibilidad y adaptabilidad de los servicios.

- A través de las mejores prácticas de ITIL se apoya al cambio en la cultura de TI y su orientación hacia el servicio, y se facilita la introducción de un sistema de administración de calidad.
- ITIL proporciona un marco de referencia uniforme para la comunicación interna y con proveedores.

Desventajas:

- Tiempo y esfuerzo necesario para su implementación.
- Que no se dé el cambio en la cultura de las áreas involucradas.
- La mejora del servicio y la reducción de costos puede llegar a no ser visible.

2.2.12 ESTÁNDAR ISO 27001.

La Organización Internacional de Normalización (ISO), es un desarrollador de normas internacionales, estas normas determinan especificaciones del arte de productos, servicios y buenas prácticas, en búsqueda de hacer organizaciones más eficientes y eficaces. Estas normas son desarrolladas a través de un consejo global, y abarcan diferentes áreas del conocimiento.

En el ámbito de la informática, entre diferentes normas existentes, tomaremos en mención la ISO 27001 la que se fundamenta en los SGSI (Sistema de Gestión de Seguridad de la Información). La gestión de la seguridad de la información debe realizarse mediante un proceso sistemático, documentado y conocido por toda la organización.

Con la implementación de ISO 27001 una Organización puede evaluar los riesgos a los que está expuesto e implementar los controles necesarios para mantener la confidencialidad, integridad y disponibilidad de la información. (Portal ISO 27001, 2005)

2.2.13 SOFTWARE LIBRE.

El software libre brinda la libertad a los usuarios para ejecutar, distribuir, copiar, estudiar, mejorar y/o cambiar el software.

Richard Stallman pionero en la defensa de las libertades en el uso del software y quien acuñó el término “Software Libre”, en 1984 creó la Free Software Foundation con el objetivo de crear el sistema Unix libre GNU y la Potenciación del Software libre.

Free Software Foundation, define el Software Libre basado en 4 libertades básicas:

1. Libertad para utilizar el programa para cualquier propósito.
2. Libertad para poder estudiar cómo funciona el programa, implica acceso al código fuente del mismo.
3. Libertad para redistribuir el programa.
4. Libertad para hacer modificaciones y distribuir las mejoras, implica también acceso al código fuente del mismo.

El software libre se fundamenta en la cooperación, transparencia y garantía para una serie de libertades a los usuarios. (Hernández, 2005).

El software libre no significa que no sea no comercial. Un programa libre debe estar disponible para su uso, desarrollo y distribución a nivel comercial, el software comercial libre es muy importante en los negocios.

2.3. MARCO REFERENCIAL.

De forma base; el proyecto tiene sustento en las normativas ISO 27001, Libro de servicios de ITIL, estándares OSI relacionados con temas de red, los manifiestos GNU y licenciamientos GPL en todas sus versiones respecto del uso de Software Libre, y otros mencionados a lo largo de este trabajo de titulación.

2.3.1. POLÍTICAS DE SEGURIDAD.

Las políticas de seguridad se pueden definir como una “declaración de intenciones de alto nivel que cubren la seguridad de los sistemas informáticos” y que proporcionan las bases para definir y delimitar responsabilidades para las diversas actuaciones técnicas y organizativas que se requieran. (Gómez A. , 2011).

La definición y aplicabilidad de las políticas de seguridad quedan establecidas en los planes, procedimientos, normas o reglamento de seguridad a seguir para la protección del sistema y/o red informática de la organización.

Siendo que la política de seguridad debe garantizar la integridad, disponibilidad y privacidad como parte del objetivo para el cual fue creada.

2.3.2 VULNERABILIDADES DEL SISTEMA.

La vulnerabilidad de un sistema puede deberse a diferentes factores, entre algunos de ellos podemos mencionar:

- Debilidad en el diseño de los protocolos utilizados en las redes.

- Errores de programación.
- Configuración inadecuada de los sistemas informáticos.
- Políticas de seguridades deficientes o inexistentes.
- Desconocimiento o falta de concientización de los usuarios y/o de los responsables de informática
- Disponibilidad de herramientas que facilitan los ataques
- Existencias de “puertas traseras” en los sistemas informáticos.

La existencia de estas vulnerabilidades da oportunidad a que la organización sea víctima de ataques que afecten la confidencialidad, integridad, disponibilidad y/o consistencia del sistema. (García PG, Vidal LMJ, 2016)

2.3.3 GESTIÓN DE LA INFORMACIÓN.

La información es parte vital de una organización, ante las amenazas a las que puede estar expuesta tanto interna como externa, provocan que la misma sea revelada o mal utilizada.

Ante tal situación y a fin de mantener la rentabilidad y operatividad de una organización, es necesario tener un correcto uso de la información, para esto la organización debe implementar estándares, mejores prácticas, metodologías y herramientas que faciliten la gestión de la información.

Podemos definir la gestión de la información como un conjunto de procesos y procedimientos que determinan la extracción, tratamiento, manipulación, depuración, control y acceso de la información que posee la organización.

Siendo la misión de la gestión de la información poder garantizar la integridad, disponibilidad y confidencialidad de la información. (A. García, F. García, 2015)

CAPÍTULO III: DEFINICIÓN DE POLÍTICAS DE SEGURIDAD EN LA INFORMACIÓN

3. Definiciones a ser implantadas.

La gran cantidad de información que posee y utiliza una organización, debe ser protegida, para esto se debe definir e implementar políticas de seguridad.

Con este proyecto, se busca proponer políticas que permitan conseguir una gestión de la información adecuada, acorde a la realidad de la Cooperativa, frente a posibles amenazas internas o externas que puedan existir.

Para tener una buena seguridad de la información en cualquier organización, es primordial comenzar estableciendo la situación actual, evaluando sus fortalezas y debilidades en seguridad de la información, de esta forma poder implantar un plan de políticas en seguridad de la información que compagine entre las necesidades y situación económica de la organización.

Por lo cual en este capítulo se evaluarán la existencia de ser el caso de la arquitectura de red, las políticas y controles de seguridad de TI utilizados actualmente para la seguridad de la información en la Cooperativa.

Una vez realizada la evaluación se definirán las mejoras a implementar en la Arquitectura de red, políticas y controles de seguridad de TI y aplicabilidad de Software Libre que mejor se adapten a la realidad y presupuesto de la Cooperativa CACPE Manabí.

3.1 DEFINICIÓN DE POLÍTICAS Y CONTROLES DE SEGURIDAD DE TI APLICABLES A LA COOPERATIVA CACPE MANABÍ.

Para realizar la definición de Políticas y Controles de Seguridad de TI aplicables a la Cooperativa, se realizó la evaluación de las mismas, se realizó una encuesta al Gerente, encargado de Fianciero y Contabilidad y encargado de Cobranzas (ver anexo 2: Encuesta) sobre su conocimiento, aplicación y/o la existencia de estudios sobre políticas de seguridad en la red actual, se determinó:

- La Cooperativa en el tiempo que lleva de creada, no ha realizado estudios para la aplicación de políticas de seguridad de la información.
- La Cooperativa tiene cierto conocimiento sobre los beneficios que ofrecería la implementación de servidores para la seguridad lógica, pero no se ha aplicado ninguno por falta de información y asesoramiento en el tema.
- La distribución de la red no fue diseñada antes de su implementación, se utilizaron solo conocimientos empíricos sin tomar en cuenta alguna norma o estándar para su aplicación.

Para encaminar a la Cooperativa hacia un manejo de la información más seguro en el ámbito informático, y con el fin de lograr:

- El establecimiento de políticas que fomenten las buenas prácticas en lo referente a la gestión de seguridad.
- Políticas que sean aplicables a cualquier entorno de la organización utilizando las tecnologías de la información para la consecución de los objetivos propuestos.
- Mejorar y optimizar la seguridad para elevar su competitividad y funcionamiento.
- Promover servicios que permitan introducirse en la autopista de la información más eficientemente.

En virtud de lo expresado se analizó la aplicación de estándares para la aplicación de políticas y controles de Seguridad de TI, para esto se busco en el estandar ISO normas que permitan cumplir los objetivos del proyecto, se identificó las siguientes:

ISO/IEC 27001: [4] Norma Internacional desarrollada por ISO (International Organization for Standardization) e IEC (International Electrotechnical Commission), que indica cómo implementar un sistema de gestión de seguridad de la información (SGSI) por medio de controles y procedimientos aplicables a una organización. La primera versión fue publicada el 15 de octubre del 2005, y tiene una revisión y publicación el 25 de septiembre de 2013.

En la misma se consideran los aspectos técnicos, organizacionales y legales, mismos que se establecen en aquellos activos de la organización que son elegibles para gestionar y medir, con el fin de minimizar los riesgos que pueden darse por la falta de confidencialidad, integridad y disponibilidad.

ISO/IEC 17799: [6] Norma Internacional Desarrollada por ISO (International Organization for Standardization) e IEC (International Electrotechnical Commission), que compila una serie de recomendaciones de buenas prácticas para la seguridad de la información en una organización, independientemente del tamaño de la misma y que puede ser aplicada a toda o una parte de la organización, siendo importante el “grado de dependencia informática” que esta tenga.

Analizado las normas ISO/IEC 27001 e ISO/IEC 17799, se eligió la norma ISO/IEC 27001 como la norma bajo la cual se fundamenta la aplicación de Políticas y Controles de seguridad de TI, así como también fundamentado en los recursos con que se cuentan en la Cooperativa.En el gráfico 3 se muestra el proceso para la selección e implementación de la norma ISO/IEC 27001, de acuerdo a las necesidades y posibilidades de la Cooperativa.

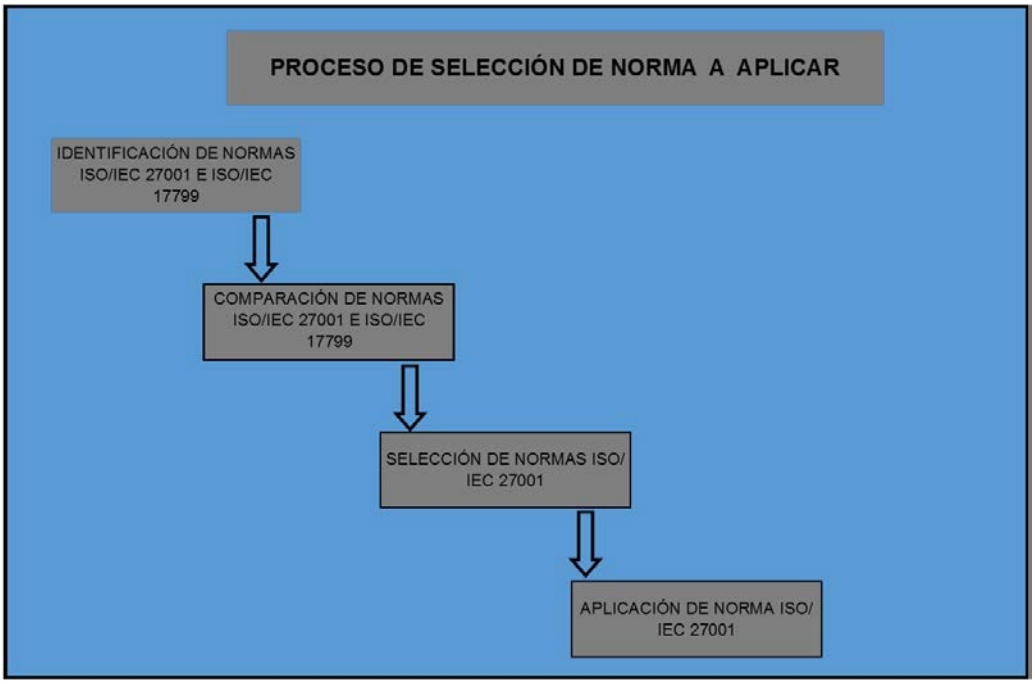


Gráfico 3. Proceso de Selección de Norma a Aplicar.
Título: Selección Norma ISO. Elaboración: Burgos Alonso Richard

Bajo este contexto se procede a detallar lo siguiente:

3.1.1 ROLES Y RESPONSABILIDADES.

Se definen tres Roles: Administrador, Dirección y Usuarios.

Administrador: Se establece este rol a la persona que tendrá la responsabilidad de la gestión de la seguridad de la información, el mismo que deberá aplicar y difundir las políticas y controles establecidos, fomentar la capacitación de los usuarios y la Dirección, administrar el control de acceso a la información, registro y verificación de inventario de equipos, registro y gestión de incidencias, revisión de los procedimientos establecidos, asesoramiento a la Dirección en los contratos con los proveedores relacionados a los sistemas y red informática de la Organización.

Dirección: Este rol pertenece al Gerente, el mismo que tendrá la responsabilidad de analizar y de ser el caso aprobar las políticas y controles propuestos por el administrador del sistema, así como la coordinación de fechas de implementación, evaluación de contratos y servicios de proveedores con el asesoramiento del Administrador.

Usuarios: Son las personas que utilizan en su labor cotidiana los equipos y recursos informáticos de la cooperativa para el cumplimiento de sus labores, ellos tendrán el derecho y obligación de conocer, entender y aplicar las políticas y controles definidos por el

Administrador y aprobadas por la Dirección de la Cooperativa, así como la comunicación al administrador ante cualquier duda o incidencia.

3.1.2 CLASIFICACIÓN Y ETIQUETADO DE LA INFORMACIÓN.

La mayoría de la información que maneja la Organización es de carácter personal, ante esto es importante clasificar la información en niveles: básico, medio y alto.

En cualquiera de los tres niveles la información es considerada sensible ya que:

Si existe fallo en la confidencialidad, se vulnera un derecho de las personas.

La falta de Integridad puede acarrear pérdidas económicas.

La falla en la disponibilidad a más de producir pérdidas económicas, impide el derecho de las personas al uso de sus ahorros.

La etiquetación de la información es muy importante sea cual sea el formato en que se encuentre, y se aplicará en un formato previamente establecido entre la administración y la Dirección.

La comunicación de información en cualquier formato solo se entenderá implícitamente autorizada cuando sea al titular de los datos o a un tercero debidamente autorizado. En cualquier otro caso, debe ser autorizada por la dirección previa supervisión y estudio por parte del Administrador.

3.1.3 CONTROL DE ACCESO A LA INFORMACIÓN.

Al ser la información el bien más preciado de la Cooperativa, nos conlleva a la implementación de controles que minimicen el acceso no autorizado hacia la misma. Por ello se implementarán los siguientes controles:

Servidores: Los servidores tendrán control de acceso por medio de cuenta de administrador y usuario con su correspondiente contraseña, dicha contraseña tendrá una longitud entre 6 y 12 caracteres, que deben contener letras mayúsculas, minúsculas, caracteres especiales y números, evitando usar palabras comunes.

La cuenta usuario estará habilitada para fines de tareas rutinarias y la cuenta administrador se utilizará en la modificación de configuraciones. La contraseña estará en conocimiento del administrador y la Dirección, siendo el principal responsable de ésta el administrador.

Estaciones de trabajo: Todas las estaciones de la organización tendrán control de acceso por medio de cuenta de administrador y usuario con su correspondiente contraseña, dicha contraseña tendrá una longitud entre 6 y 12 caracteres, que deben contener letras mayúsculas, minúsculas, caracteres especiales y números, evitando usar palabras comunes.

La cuenta usuario estará limitada a las competencias del colaborador, y determinadas por la Dirección y administración, el cuidado y buen uso de la contraseña será responsabilidad del colaborador.

Las unidades de CD-ROM, puertos USB, están deshabilitadas, y quedan a consideración de la dirección y administración, su habilitación en alguna estación de trabajo específica.

Software Financiero: Para el acceso al sistema se tendrá usuario y contraseña, misma que será independiente de las existentes para entrar a las estaciones de trabajo, el usuario y contraseña se regirá a las especificaciones del Software Financiero.

Los módulos del sistema serán habilitados de acuerdo a las competencias que posea el colaborador, y determinadas por la Dirección y administración, el cuidado y buen uso de la contraseña será responsabilidad del colaborador.

Información en Físico: Entendiendo esto como aquella información que se encuentra en papel, es menester del colaborador custodiar la información que su cargo le permite manipular, manteniéndolo fuera del alcance a personas extrañas al área en que labora, llevando a la práctica la política de puesto despejado.

3.1.4. TEMAS A CONSIDERAR POR EL COLABORADOR.

Se implementará para los actuales y futuros colaboradores la entrega de un documento de medidas de seguridad de TI y se recoge una carta de compromiso firmada por el colaborador. En el documento se explica la sensibilidad de la información que su cargo le permite tener acceso, así como podrían ser indagadas las acciones que realice en los equipos de la organización.

Se le recuerda al colaborador el sigilo y protección de la información, a la que tiene acceso en el desempeño de su cargo.

Para la compartición y respaldo de la información de autoría del colaborador y temática laboral, la información será almacenada en las carpetas de red asignadas y no en los discos duros de las estaciones de trabajo.

La creación de soportes queda en manos del Administrador y la aprobación de la dirección, no debiendo el colaborador sacar información en cualquier formato, peor aún permitir el acceso a terceros.

No es permitido sacar los equipos de la organización sin conocimiento, caso excepcional tenga autorización del administrador y la dirección en conjunto.

Se reserva la capacidad de supervisión de los contenidos en las estaciones de trabajo, bajo el respeto a la confidencialidad de los puestos de trabajo fijada en el código de los trabajadores.

3.1.5. ACCESO A INTERNET.

Como Política general los usuarios de la organización no tendrán acceso a internet desde sus estaciones de trabajo, esto solo será posible bajo la petición al administrador y la dirección, y la debida justificación de las necesidades del colaborador para tener acceso a internet.

En caso del usuario que tenga autorizado el acceso al internet, se prohíbe la descarga de contenido (tenga o no derechos de autor) y el uso del mismo en línea (YouTube, etc.).

Los usuarios no tendrán permisos de administrador para la instalación de software, sea estos actualizaciones de sistema operativo, aplicativos, antivirus, entre otros.

3.1.6. SEGURIDAD FÍSICA Y DEL ENTORNO.

El ambiente donde se encuentran los equipos que alojan la información deberá estar suficientemente protegido. Esta protección será tanto contra acciones intencionadas como ante situaciones accidentales, el ambiente debe tener las medidas adecuadas en cuanto a la protección eléctrica, electromagnética, contraincendios y negación de acceso a personal no autorizado.

Para nuestro Proyecto se debe instalar:

- Un UPS de 1Kva para protección de los servidores y equipos del área de informática
- Reforzar la Seguridad para acceso al área de los servidores.

Si bien se establece la necesidad de lo indicado en el párrafo anterior, va a depender del presupuesto de la Organización, la implementación de esto.

3.1.7. GESTIÓN DE LA INFORMACIÓN.

Disponibilidad: El sistema informático deberá estar plenamente operativo durante las fechas y horarios de trabajos establecidos, las tareas de mantenimiento deberán realizarse bajo programación y en horarios mínimos de impacto.

Confidencialidad: El sistema informático debe mantenerse actualizado, se adoptarán medidas para mitigar la posible salida no autorizada de información bajo cualquier formato, ningún colaborador deberá sacar información de la Cooperativa sin motivo justificable.

Integridad: Se establecerá la realización de copias de seguridad una vez por semana de los datos contenidos en los servidores de los sistemas de información una vez terminada la jornada laboral.

3.1.8. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN.

Ante la posibilidad de que se pueda afectar la seguridad de la información de la organización ante alguna anomalía como:

- Robos o intento de robos de contraseña.
- Utilización de usuarios y contraseña por personal no autorizado.
- Descarga de información no autorizada.
- Intentos de acceso no autorizados por terceros.
- Pérdida de datos o corrupción del contenido de la base de datos.
- Accesos no autorizados a datos, tanto en aplicativos como en físico.

Se establece seguir un procedimiento de notificación de incidencias:

1. Colaborador que detecte una posible anomalía o suceso, deberá comunicar al administrador, tratando de detallar lo ocurrido y el tiempo en que ocurrió.
2. El administrador deberá analizar la situación, de considerarla una incidencia, procederá a comunicar la misma a la Dirección, mediante un informe que contenga las causas y consecuencias, sugerencias de medidas a tomar para rectificar y evitar futuras incidencias.
3. La Dirección evaluará el informe, y de ser el caso aprobará la aplicación de medidas dirigidas a mitigar futuras incidencias, así como disponer al administrador el registro de la incidencia ocurrida, el cual deberá tener una bitácora sobre la gestión de incidencias ocurridas en la Cooperativa.

3.2. DEFINICIÓN PARA APLICABILIDAD DE SOFTWARE LIBRE.

El Software que fue descrito en la Tabla 3 de la sección 1.1.2 inventario de software, nos permite comentar que el mismo, es un software privativo, en ninguna de las estaciones de trabajo de la Cooperativa se poseen licencias del software que es propiedad de Microsoft, esto es algo que a pesar del conocimiento de la Dirección, no ha sido corregido por razones de presupuesto.

Ante tal situación y tratando de optimizar los recursos de la Cooperativa, se propone realizar un plan piloto de software libre como parte del proyecto, el cual tendrá su implementación y ejecución en la estación de trabajo de Gerencia; en un principio se consideró esta implementación en la estación de trabajo del área de Crédito y Cobranzas, pero en conversación con la Dirección y a solicitud de la misma se estableció hacerlo en el área de Gerencia.

Existe variedad de distribuciones de software libre disponibles, dependiendo de la necesidad se determina cuál distribución aplicar.

Para este caso considerando la utilización de Centos para los servidores de la Cooperativa, y tratando de mantener la misma red de distribución que tenia la Coopertiva al iniciar el proyecto, elegimos la distribución Fedora que al igual que Centos se derivan de la Familia Red Hat (asle.com, s.f.), y es una opción amigable para aplicar a la estación de trabajo que se encuentra en Gerencia.

CAPÍTULO IV: METODOLOGÍA APLICADA EN LAS POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

4. METODOLOGÍA APLICADA.

La metodología que se aplicó en el desarrollo del presente trabajo de titulación fue una metodología descriptiva, de campo y aplicada, siendo *descriptiva* porque se determinaron los problemas existentes en la entidad financiera, de *campo* porque se acudió al lugar donde funciona la Cacpe, Manabí para poder realizar un inventario de los programas informáticos con que cuenta la misma y poder detectar el problema existente, y *aplicada* porque con la implementación de seguridad de la información y el plan piloto para uso de software libre, se resuelve el problema detectado y a la vez se cumple con los objetivos planteados.

Basado en la norma ISO 27001 y considerando el presupuesto asignado por parte de la Cooperativa para el desarrollo de este proyecto, se muestra a continuación una tabla resumen de las implementaciones ejecutadas en la organización:

Tabla 4. Resumen de Implementaciones Ejecutadas

Implementación	Descripción
4.1 Implementación de la red Informática.	La administración de la seguridad en la red es importante, por tal motivo parte inicial para este objetivo es tener una buena estructura de red.
4.2 Ejecución de las políticas y sus controles.	Se basa en el control de la seguridad en la información, así como su gestionamiento, pero de acuerdo a las políticas de la cooperativa. La definición de los roles y responsabilidades, declaraciones de confidencialidad de la información, la clasificación y etiquetación de la información.
4.3 Implementación de Servidores.	La protección de la red con un buen manejo y control, para la seguridad de las aplicaciones que se encuentran dentro de la red y que incluyen el tránsito de información.
4.4 Implementar el Plan Piloto para Migración de Estaciones de trabajo a Software libre.	Buscando la optimización de recursos en beneficio de la organización, se establece la implementación del uso de software libre como plan piloto.
4.5 Pruebas y Resultados.	Se realiza las pruebas de satisfacción de los colaboradores de la Cooperativa y tabulación de resultados. Para evaluación de los objetivos propuestos en el proyecto.

Elaborado por: Richard Burgos A.

4.1. IMPLEMENTACIÓN DE LA RED INFORMÁTICA.

Para la mejora de la red informática existente en la organización, se consideró necesario la adquisición de un servidor HP ML310, este se utilizará en la migración de la base de datos del sistema AFC de la Cooperativa que se encuentra actualmente en el servidor IBM System X3200 M2 que tiene la organización, este servidor IBM servirá para la implementación de los servidores en que se fundamenta el trabajo de fin de titulación.

Pero ante el terremoto ocurrido en el país el sábado 16 de abril del 2016 (16A), que afectó principalmente a las provincias de Esmeraldas y Manabí, siendo la ciudad de Portoviejo una de las más afectadas, la planificación realizada para el presente proyecto tuvo que ser modificada en los siguientes aspectos:

- Las oficinas de la Cooperativa tuvieron que ser trasladadas a otra dirección, donde realicé los siguientes trabajos:
    - Instalación del Cableado de la red con topología física tipo estrella.
    - Instalación del sistema de Cámaras

En el gráfico 4 se muestra un plano de distribución de la Cooperativa.

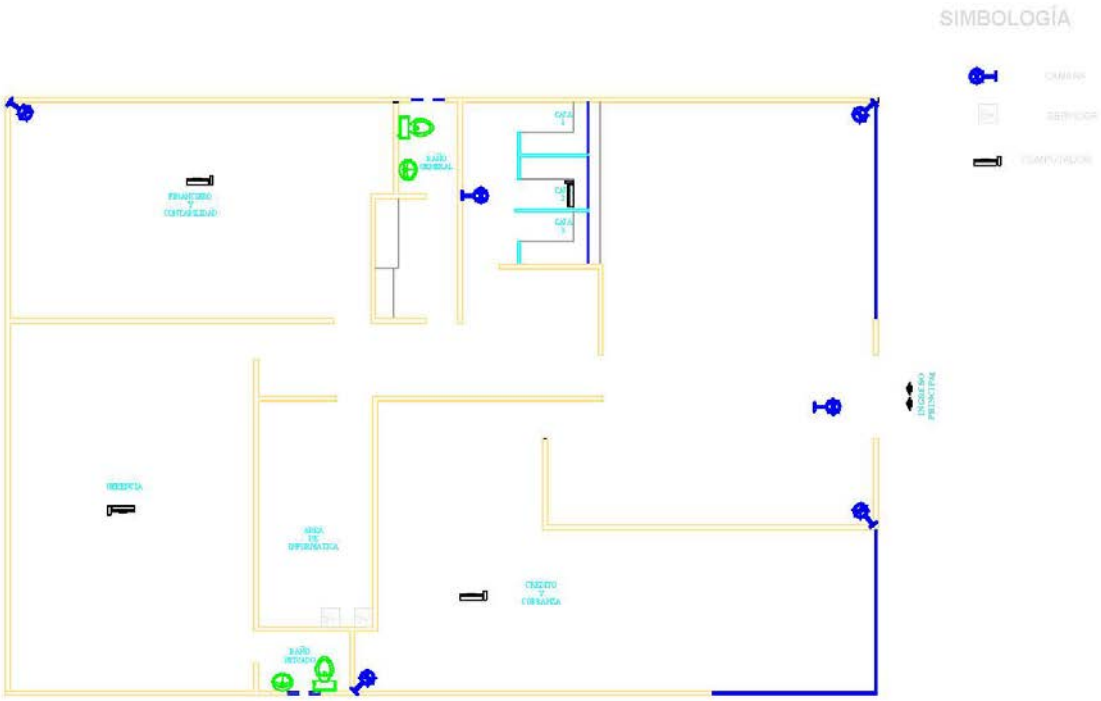


Gráfico 4. Plano de distribucion de la Cooperativa.

Título: Plano de Distribución.
Elaboración: Burgos Alonso Richard

- Se Mantiene el servidor IBM System X3200 M2 como Servidor de Base de Datos.
- El presupuesto para comprar el servidor HP ML310 tuvo que ser reducido, ante lo cual se procedió a la adquisición de un CPU Clon con las siguientes características:

    - Procesador Core i5
    - Tarjeta madre Gigabyte
    - Memoria RAM 16Gb
    - Doble tarjeta de red
    - Disco Duro 1Tb

  Este equipo se lo preparó para montar los servicios de servidor proxy, firewall. La topología lógica de la red informática se establece como tipo estrella.

La implementación de estos servicios de red tiene la finalidad de que los usuarios puedan utilizar de mejor manera los equipos, tener control sobre los accesos a la red, en pos de la optimización para un mejor rendimiento de la organización.

4.2. EJECUCIÓN DE LAS POLÍTICAS Y SUS CONTROLES.

4.2.1. ROLES Y RESPONSABILIDADES.

Una vez presentado al Gerente de la cooperativa el plan de implementación de políticas y controles para la red informática. Se procedió a convocar una reunión con los colaboradores de la entidad financiera; se explicó e informó sobre el plan a implementar, dando a conocer las responsabilidades, obligaciones y derechos que les compete de acuerdo a las funciones que desempeñan en la Cooperativa.

Se estableció como administrador temporal al Sr. Richard Burgos Alonso que tendrá la responsabilidad de la gestión de la seguridad de la información, el mismo que deberá aplicar y difundir las políticas y controles establecidos, fomentar la capacitación de los usuarios y la Dirección, administrar el control de acceso a la información, registro y verificación de inventario de equipos, registro y gestión de incidencias, revisión de los procedimientos establecidos, asesoramiento a la Dirección en los contratos con los proveedores relacionados a los sistemas y red informática de la Cooperativa.

Como Dirección se asignó al Sr. Víctor Andrade, el mismo que tendrá la responsabilidad de analizar y de ser el caso aprobar las políticas y controles propuestos por el administrador del sistema, así como la coordinación de fechas de implementación, evaluación de contratos y servicios de proveedores con el asesoramiento del Administrador.

Como usuarios se encuentran los colaboradores de la cooperativa que son las personas que utilizan en su labor cotidiana los equipos y recursos informáticos de la Cooperativa para el cumplimiento de sus labores, ellos tendrán el derecho y obligación de conocer, entender y aplicar las políticas y controles definidos por el Administrador y aprobadas por la Dirección de la Cooperativa, así como la comunicación al administrador ante cualquier duda o incidencia.

4.2.2. CLASIFICACIÓN Y ETIQUETADO DE LA INFORMACIÓN.

Se procedió a la clasificación y etiquetado de la información en un trabajo conjunto entre el administrador y los usuarios, en cada uno de los computadores.

Con esto se obtuvo una documentación ordenada y clasificada de tal forma que de ser necesario sea fácilmente ubicable por el personal de la Cooperativa.

Misma que tuvo buena acogida por los colaboradores de la organización, mostrando la predisposición para mantener la información organizada y clasificada.

4.2.3. CONTROL DE ACCESO A LA INFORMACIÓN.

Se implementaron los siguientes controles:

Servidores: Se actualizan las contraseñas siguiendo las recomendaciones sugeridas en cuanto a longitud, tipo de caracteres y evitando usar palabras comunes.

Estaciones de trabajo: Se actualizaron las contraseñas siguiendo las recomendaciones sugeridas en cuanto a longitud, tipo de caracteres y evitando usar palabras comunes.

Se establece entre el Administrador y la Dirección la deshabilitación de las unidades de CD-ROM, puertos USB, en la estación de Caja, Crédito y Cobranzas, en las demás estaciones quedan habilitados.

Software Financiero: Se actualizó la contraseña regida a las especificaciones del Software Financiero.

Los módulos del sistema siguen habilitados de acuerdo a las competencias que posea el colaborador, y determinadas por la Dirección y administración, el cuidado y buen uso de la contraseña será responsabilidad del colaborador.

Información en Físico: Se procedió a ejecutar un plan de aseguramiento del archivo físico de la organización.

4.2.4. ACCESO A INTERNET.

Se cambiaron las claves de acceso para la red inalámbrica. Los colaboradores que tienen acceso al internet, tienen prohibido la descarga de contenido (tenga o no derechos de autor) y el uso del mismo en línea (YouTube, etc.).

No tienen permisos de administrador para la instalación de software, sean estos actualizaciones de sistema operativo, aplicativos, antivirus, entre otros.

En un principio tuvo cierta resistencia la aplicación de esta normativa, pero a través del diálogo y explicaciones respectivas en conjunto entre las partes involucradas, se llegó a la concientización y aceptación para la aplicación de la misma.

4.2.5. SEGURIDAD FÍSICA Y DEL ENTORNO.

Debido al movimiento sísmico suscitado el 16A, la Cooperativa de Ahorro y Crédito CACPE Manabí tuvo que cambiar de ubicación física, por tanto se tomaron las medidas adecuadas para la protección eléctrica, electromagnética, contraincendios y negación de acceso al personal no autorizado.

En esta aplicación se contó con todo el apoyo necesario de parte de la Gerencia y Directorio de la Cooperativa, así como la opinión de los colaboradores para mejorar la seguridad física de la organización.

4.3. IMPLEMENTACIÓN DE SERVIDORES.

Para concretar la propuesta del proyecto para beneficio de la Cooperativa, se procedió a preparar el CPU adquirido, para lo cual se establece:

- La instalación de Centos 7 como sistema operativo.

La instalación de WEBMIN como herramienta gráfica opcional para la configuración en los Servidores.**Centos**

La distribución Centos Linux es una plataforma estable, predecible, manejable y reproducible derivado de las fuentes de Red Hat Enterprise Linux (RHEL).

Su última versión es Centos 7, este se ajusta plenamente a la política de redistribución de Red Hat y apunta a tener compatibilidad funcional completa con el producto anterior. (CentOS.7, s.f.)

Debido a las características mencionadas, este sistema se instaló en el equipo destinado para servidor.

Webmin.

Esta aplicación es una interfaz web que nos permite la configuración de aspectos internos de los sistemas operativos con que es compatible, y para nuestro caso la configuración de permisos para usuarios, por medio de una estructura de módulos, que facilita la administración de herramientas como Apache, DNS, SAMBA, DHCP, PROXY, teniendo una interfaz amigable. (Webmin.com, s.f.)

Se instaló la herramienta Webmin como opción para realizar configuraciones pertinentes en el servidor de ser el caso.

4.3.1. SERVIDOR PROXY.

El Servidor Proxy es un servicio que hace de intermediario entre equipos internos y otras redes externas a la organización. El proxy se encarga de realizar las peticiones de los equipos internos hacia los servidores de internet, con lo cual los equipos y servidores de internet no conocen la identidad del equipo en nombre del cual actúa el proxy. (Gómez A. , 2011)

Previo la implementación del Servidor Proxy, se establece entre la administración y la Dirección, las páginas web a ser bloqueadas, así como los usuarios que tendrán acceso al internet.

Squid: Es la aplicación seleccionada para la implementación del Proxy, por considerar que cumple con las expectativas como un servidor intermedio de alto desempeño, confiable, robusto y versátil.

Con esta implementación se buscó restringir el acceso a páginas web en sus diferentes categorías que interfieren con la productividad de los colaboradores y consumen ancho de banda que restan el rendimiento de la organización.

Se instaló la herramienta Squid en el equipo desde los repositorios comunitarios.

```
#yum install Squid
Configuración del servicio del Proxy
#vi /etc/Squid/squid.conf
```

Y se colocó el script con la configuración necesaria para el cumplimiento de los objetivos con que se decidió la implementación del servidor proxy.

Refiérase al Anexo 3 para ver registro de la configuración.

4.3.2. SERVIDOR DNS.

Para acceder a una página web del internet, es necesario tener la dirección IP del servidor donde se encuentra almacenada.

El DNS (Domain Name System, sistema de nombres de dominio) es el que provee la resolución de nombres de dominio a direcciones IP, permitiendo su fácil localización dentro de la red informática.

Cuando un usuario digita un dominio, se crea una entrada WHOIS en el registro correspondiente y queda almacenada en el DNS, el DNS tiene una base de datos donde se almacenan todos los registros de los nombres de dominio que se van gestionando.

Para los usuarios o el administrador de la red es más fácil recordar un nombre de dominio fijo a una dirección IP cambiante.

El servidor DNS, utiliza la base de datos del DNS para responder a las peticiones que guarden relación con el espacio de nombres de dominio.

Para la habilitación del servidor DNS se realizó un script, para que funcione dentro de la red de la organización y pueda utilizar las características y funcionalidades que proporciona el servicio de DNS en beneficio de la Cooperativa.

Refiérase al Anexo 4 para ver el registro de la configuración.

4.3.3. SERVIDOR DHCP.

El protocolo de configuración dinámica de host (Dynamic Host Configuration Protocol, DHCP) es un estándar TCP/IP creado para simplificar la administración de la configuración IP de los equipos en una red.

Con el servicio DHCP, una computadora tendrá una dirección IP determinada durante cierto periodo de tiempo, la duración de la dirección dependerá de la frecuencia con que esa estación accede a internet.

El servidor DHCP le permite al administrador de la red supervisar y asignar las direcciones IP de forma automática al momento que un computador se conecta de una parte diferente a la habitual en el área de la red.

El servidor asigna direcciones IP dentro de un rango prefijado, cuando configuramos una dirección IP manualmente en una estación, dicha dirección podría estar gestionándose dentro de nuestro servidor DHCP, entonces existe la posibilidad de que resulte un error ya que esta dirección puede estar asignada a dinámicamente a otra estación, provocando un conflicto de IP, en este caso el usuario tendrá que solicitar y comprobar la disponibilidad de otra dirección IP.

Se realizó un script para implementar y aplicar el servidor DHCP en beneficio de la Cooperativa.

Refiérase al Anexo 5 para ver registro de la configuración.

4.3.4. FIREWALL PERIMETRAL UTILIZANDO IPTABLES

Una red informática o computadora siempre podría ser víctima de un ataque informatico, más aún si permanece habilitada para el acceso al internet.

El firewall o corta fuego, es aquel que permite proteger una red informática o computadora de las instrucciones que provienen del internet u otra red informática. Este firewall permite filtrar los paquetes de datos que circulan desde el internet, es un muro que ayuda en el filtrado del tráfico entre las redes informáticas.

Por medio de reglas predefinidas que contiene el firewall podemos:

- Autorizar una conexión
- Bloquear una conexión
- Redireccionar un pedido de conexión sin avisar al emisor.

Estas reglas permiten usar un método de filtración, mismo que se fundamenta en la política de seguridad adoptada por la organización. Aquí podemos configurar de dos maneras: permitir únicamente las comunicaciones autorizadas explícitamente o impedir cualquier comunicación que fue explícitamente prohibida.

Se instaló el Firewall con el Objetivo de redireccionar el tráfico de la red de la Organización. Este redireccionamiento se realiza con la acogida de todo el tráfico que llega al puerto 80 hacia el puerto 3128 del proxy.

Utilizamos IPTABLES para realizar el enmascaramiento de los equipos que se encuentran en la red informática hacia el internet.

Configuración del guion (script) de iptables

vi /root/firewall #Fuente externa

Para la implementación del firewall se creó un script para ver la configuración del mismo, refiérase al Anexo 6.

4.3.5 IMPLEMENTACIÓN DE SERVICIO DE FILTRADO DE CONTENIDO.

Los usuarios de una red informática o computadoras acceden regularmente al internet, por lo cual el hardware está expuesto a que en él se introduzca de manera inadvertida software malicioso, que puede llegar a causar graves daños.

Ante esta situación surge la necesidad de controlar el acceso al internet por parte de los usuarios de una empresa, los administradores de red pueden recurrir a la implementación de restricciones a ciertas páginas no adecuadas para el entorno en que se maneja el negocio de la empresa.

Entre estas restricciones se puede optar por la aplicación del servicio de filtrado de contenido. Para el proyecto se optó por el Dansguardian apoyado en el Proxy.

El Dansguardian es una utilidad que nos ayuda en el filtrado de contenidos de sitios web muy potente que trabaja en conjunto con el servidor proxy Squid.

Dansguardian es un código abierto, desarrollado en C++, el cual nos permite una configuración adaptable a las necesidades del administrador de la red.

Por defecto ya viene configurado la limitación de visitas a páginas prohibidas para menores, pero dispone de gran cantidad de archivos de configuración para llevar a cabo un ajuste del servicio personalizado.

Los usuarios mediante sus navegadores web hacen peticiones de páginas que son recibidas por el Dansguardian y redireccionadas al servidor proxy Squid aquellas que superan la fase de filtrado.

Siendo que esta herramienta nos permite filtrar el contenido con mayor granularidad.

El mismo que se descargó de los repositorios comunitarios:

A continuación, en la tabla 5 se muestran algunas páginas y palabras claves que serán restringidas con la implementación del Dansguardian.

Tabla 5. Tipo Paginas Restringir.

Categoría	Páginas o Palabras Claves
Redes Sociales	Facebook, Instagram, Twitter, Hi5
Pornografía	sexo, lolitas, Pornografía, videos porno, xxx, sex, porno
Servidores de Descargas	Softonic, taringa, uptodown, descargas, free download
Juegos	juegos, mini juegos, juegos online, mundijuegos

Fuente: Administrador y Dirección de la Cooperativa.

Elaboración: Burgos Alonso Richard

Proceso de implementación:

Instalación del Dansguardian desde las fuentes externas: www.rpmfind.net

Se descargó el paquete dansguardian-2.12.0.3-1.1.x86_64.rpm

#rpm -ivh dansguardian-2.12.0.3-1.1.x86_64.rpm

Configuración de Dansguardian

vi /etc/Dansguardian/dansguradian.conf

Edición de las listas

vi /etc/Dansguardian/lists/exceptionphraselist

vi /etc/Dansguardian/lists/exceptionphraselist

Edición de los diversos archivos contenidos dentro del directorio:

/etc/dansguradian/lists/phraselists

Refiérase al Anexo 7 para ver registro de la configuración.

4.4. IMPLEMENTAR EL PLAN PILOTO PARA MIGRACIÓN DE ESTACIONES DE TRABAJO A SOFTWARE LIBRE.

El software libre se refiere a la libertad de los usuarios para ejecutar, copiar, distribuir, estudiar, cambiar y mejorar el software. Teniendo como principio cuatro libertades:

- La libertad de usar el programa para cualquier propósito.
- Libertad de estudiar cómo funciona el programa, y adaptarlo a sus necesidades.
- La libertad de distribuir copias.
- La libertad de mejorar el programa y hacer públicas las mejoras a los demás, de modo que toda la comunidad se beneficie.

Basado en esto, cualquier persona u organización puede usarlo en cualquier tipo de sistema informático, para cualquier clase de trabajo, y sin tener obligación de comunicárselo al desarrollador o a alguna entidad específica.

Para el proyecto con la finalidad demostrar las ventajas que podría representar la implementación de software libre en la organización.

Se inició un plan piloto para migración de estaciones de trabajo a Software libre, el cual en principio estaba establecido implementar en todas las estaciones de trabajo de la cooperativa.

Sin embargo, después de las conversaciones con la Dirección y colaboradores de la Cooperativa, se determinó iniciar el Plan solo en la estación del área de crédito y cobranza.

4.4.1. VISIÓN Y OBJETIVOS DEL PLAN

Visión:

Que todas las estaciones de trabajo de la organización utilicen software libre.

Objetivos:

- Difundir y fomentar los beneficios en el uso de software libre.
- Inducir a la organización al uso de software libre en los sistemas de información.

4.4.2. INFORMACIÓN Y CAPACITACIÓN AL PERSONAL.

Con la finalidad de garantizar el correcto cambio de software privativo que existía en la estación elegida para la implementación del plan piloto de software libre, se estableció en conjunto con la dirección de la cooperativa, proceder a informar y capacitar al personal involucrado en el área, sobre el procedimiento y calendarización de la migración hacia el uso de software libre.

Esta difusión según conversación con la dirección estuvo bajo la responsabilidad del Sr. Richard Burgos.

4.4.3. MIGRACIÓN A SOFTWARE LIBRE.

Con la finalidad de establecer un orden en la migración a software libre, en conjunto con la dirección se estableció una secuencia de migración de aplicaciones de la siguiente forma:

- Navegador de internet, de internet Explorer para Mozilla Firefox.
- Suit de ofimática, Microsoft office 2010 a Apache OpenOffice 4.1.
- Software Especializado, sistema AFC propio de la Cooperativa
- Sistema Operativo, Microsoft Windows XP SP3 a Fedora 20

Cabe resaltar que la selección del sistema operativo Fedora 20, se dio por la robustez del mismo, así como por ser una distro derivada de la familia de Red Hat, a la cual también pertenece el sistema Operativo Centos que se usa en los servidores de la Cooperativa, considerando que esto nos es de gran ayuda para la interoperabilidad entre los equipos.

Para lograr realizar una transición lo más amigable posible de software privativo a software libre, se realizó la virtualización del software privativo en el software libre, hasta que se tenga una adaptabilidad adecuada que permita pasar definitivamente al uso de software libre.

Para realizar la virtualización se utilizó como herramienta el VirtualBox 5.1.4.

VirtualBox es un software de virtualización tipo 2 donde los usuarios pueden cargar múltiples sistemas operativos invitados en un solo sistema operativo anfitrión. Cada invitado se puede configurar, iniciar, pausar o parar de forma independiente, como se mencionó al comienzo de la sección 4.4.3. se utilizo como sistema operativo Fedora 20, navegador de internet Mozilla FireFox, como paquete de ofimática apache OpenOffice 4.1.

La migración se ejecutó en un lapso de 4 días, en coordinación con la dirección y colaboradores de la Cooperativa.

4.4.4. DISTRIBUCIÓN DE SOFTWARE LIBRE.

El software libre en si consiste en la posibilidad de ser manipulado y/o adaptado a las necesidades del usuario especializado.

Existen organizaciones que se dedican a recopilar el software libre requerido para que una computadora funcione, dependiendo la organización esto puede implicar un valor a pagar si es de tipo comercial, o gratuito de ser una organización oficial.

El volumen de software libre disponible en la red es inmenso, por lo cual generalmente las organizaciones se especializan en un determinado tipo de negocio, para solventar las necesidades del usuario final y basado en el hardware disponible.

Como sistema operativo de software libre para el plan piloto, siguiendo la línea de Red Hat, se escogió la distro estable de Fedora 20 para la implementación del Plan Piloto.

Fedora es un sistema operativo pulido y fácil de usar, para ordenadores portátiles y de escritorio, con un conjunto completo de herramientas para el usuario. Debido a esto se consideró una distro adecuada para la aplicación del plan piloto en la cooperativa.

Se acordó con la gerencia, realizar un taller de capacitación a los colaboradores involucrados para el manejo del sistema Operativo Fedora a nivel usuario, dicha capacitación consistía en el manejo del escritorio del sistema Fedora y el OpenOffice como paquete de ofimática.

La versión del sistema operativo Fedora escogida se denomina Heisenbug con una arquitectura para 32bits, esta arquitectura fue escogida por el tipo de hardware que posee la Cooperativa.

El sistema operativo Fedora Workstation, fue instalado en su entorno grafico GNOME, y para el uso en la Cooperativa, se consideró la Capacitación del personal en el uso del escritorio de Fedora, y para la realización de las tareas diarias de los colaboradores la aplicación Apache Open Office como paquete de ofimática.

Refiérase al Anexo 8 para ver la encuesta a los colaboradores en referencia al uso del sistema operativo Fedora.

4.4.5. EFECTOS EN LA IMPLEMENTACIÓN DEL PLAN PILOTO.

Se puede mencionar que, con la aplicación del plan piloto de implementación de software libre, se tiene un ahorro económico en lo referente al pago de licencias de uso del software privativo, mayor garantía en seguridad puesto que se puede auditar el código en uso, flexibilidad en la adaptación e integración ya que se puede modificar el código.

Sin embargo, el uso de software libre también conlleva la aplicación de procedimientos para la organización como para los colaboradores de la misma.

La Cooperativa:

- Capacitación de su personal de TI en lo referente a solución de posibles problemas en el uso del software libre, como incompatibilidad de periféricos, infección de troyanos, asi como en el uso y modificación de ser el caso del código del software.

- Creación de una comunidad interna, donde el usuario remita sus problemas y pueda recibir la solución al mismo por medio de correo electrónico, por parte del personal técnico.

El Usuario:

- Cuando tenga un problema, se dirija a la comunidad creada por la organización, para que revise lo publicado en su comunidad al respecto, ya que ahí puede encontrar la solución.
- La participación dinámica que debe tener en la aplicación del plan piloto del software libre, para un mejor entendimiento del mismo.

4.4.6. AMPLIACIÓN DE PLAN PILOTO EN LA COOPERATIVA.

Una vez que se ejecutó el plan piloto en la estación del área de crédito y cobranza, teniendo la buena acogida por el personal que participó en el plan, se consideró que el objetivo de optimizar los recursos en lo referente a liberarse del uso de software privativo, en primera instancia podría alcanzarse.

En base a lo revisado sobre la seguridad de la información en la norma ISO 27001, se considera que el uso de software libre en la Cooperativa, beneficia a los objetivos que se persiguen de brindar seguridad de la información, permitiendo mayor garantía en seguridad, asi como la adaptabilidad e interoperabilidad entre las estaciones de trabajo y los servidores de la Cooperativa.

Sin embargo, se acordó en conjunto con la Dirección, realizar un análisis sobre las ventajas y desventajas que podría conllevar utilizar el software libre en todas las áreas de la cooperativa.

Análisis de la ampliación.

Se conversó con la gerencia sobre la ampliación del plan piloto hacia todas las áreas de la Cooperativa, de esta conversación se establecieron las ventajas y desventajas que esto les implicaría.

Ventajas:

Reducción de costes por licencias en estaciones de trabajo, se evitaría la inversión en compra de licencias para las estaciones de trabajo de las áreas de la Cooperativa.

Estandarización en el uso de software libre en las áreas de la cooperativa, permitiendo con esto que los archivos y documentación se manejen bajo formatos iguales.

Ajustes de configuración a las necesidades de la organización mediante el desarrollo de aplicaciones, siendo un software libre se podrían ajustar ciertos aplicativos a la conveniencia de la organización.

Mejora en rendimiento del sistema operativo y sus aplicativos, el software libre requería menores recursos de hardware, mismo que con software privativo no ocurre por la cantidad de recursos hardware que requiere, esto debido al hardware que posee la Cooperativa.

Desventajas:

- Incompatibilidad con el software financiero que posee la Cooperativa, ya que este software actualmente está diseñado para un entorno de software privativo como Windows.
- Incompatibilidad con ciertos dispositivos existentes en la Cooperativa, como impresoras y escáneres.

Aplicación de Ampliación:

Una vez analizadas las ventajas y desventajas que conlleva la ampliación del uso de software libre a todas las áreas de la Cooperativa. Se estableció dar un tiempo de prueba de dos meses, posterior a esto se acordó con la Dirección de la Cooperativa las siguientes acciones:

- Se establece proceder a la ampliación del uso de software libre en la estación de Gerencia.
- Para realizar la ampliación del uso de software libre en las demás áreas de la Cooperativa es necesario realizar lo siguiente:
  - Consultar al proveedor del software financiero la viabilidad y costes para que el mismo funcione en entorno de un software libre.
  - Buscar actualizaciones de drivers compatibles para el uso de dispositivos con el software libre.

4.5. PRUEBAS Y RESULTADOS.

Una vez realizada la implementación del proxy y el plan piloto de software libre en la red informática, se procedió a la monitorización de la red, pruebas y nivel de satisfacción de los colaboradores de la Cooperativa.

Se realizó una encuesta sobre el software libre aplicado en el plan piloto, una encuesta sobre las políticas de seguridad aplicadas a la Cooperativa y una declaración de confidencialidad.

4.5.1. RESUMEN DE PRUEBAS REALIZADAS A LAS HERRAMIENTAS CONFIGURADAS BAJO LINUX.

Con la finalidad de verificar la funcionalidad de las configuraciones realizadas bajo Linux, y el cumplimiento de estas configuraciones con los requerimientos necesarios para el desarrollo del proyecto.

Se establecio realizar ciertas pruebas, a continuación se detalla el tipo de prueba que se realizó:

- Prueba 1: Procesos e interface de Usuario.
- Prueba 2: Interfaces con otras redes
- Prueba 3: Volumen

Recursos a utilizar:

Como recurso de hardware para la ejecución de las pruebas se utilizó una estación de escritorio Intel Celeron 430 1.8 GHz. con 2 Gb de memoria y una laptop Dell inspiron 14 – Core i 5 1.7 GHz. con memoria de 8 Gb.

Como recurso de software para la ejecución de las pruebas se utilizo en la estación de escritorio el sistema operativo Fedora 20, como navegador Mozilla Firefox; en la laptop el sistema operativo Windows 8, como navegador Google Chrome.

Como recurso humano para la ejecución de la pruebas estuvo de responsable el Sr. Richard Burgos Alonso.

Ejecucion y evaluación de las pruebas

Prueba 1: Procesos e interface de Usuario:

La prueba verificó el procesamiento lógico en el servidor y la actualización de la configuración. Aquí se procedió a hacer uso del internet, probando las funciones del servidor.

Escenario: Ingreso de usuarios

Módulo: Proxy Server

Caso de prueba: Ingreso usuario a internet.

Tipo de prueba: Interface con otras redes.

Descripción: ingreso al internet con un usuario previamente definido.

La prueba se corrió por 12 oportunidades, siendo satisfactorios los resultados en lo referente a validación y registro del navegador.

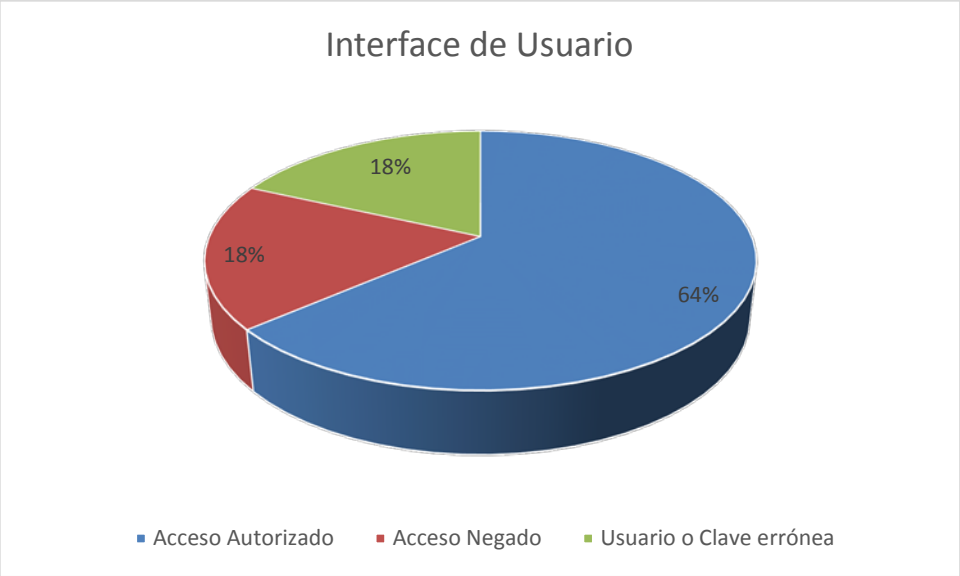


Gráfico 5. Interface de Usuario.
Título: Resultados de pruebas.
Elaboración: Burgos Alonso Richard

Prueba 2: Interfaces con otras redes:

La prueba verificó la respuesta a peticiones de páginas web por las redes remotas. Se usó el internet en puntos remotos, probando así las funciones del servidor con redes remotas.

Escenario: Permisos de navegación.

Módulo: Filtro de Contenidos (Dansguardian)

Caso de prueba: Ingreso a páginas web no permitidas.

Tipo de prueba: Procesos e interfaces de usuario.

Descripción: ingreso a páginas web previamente autorizadas.

La prueba se corrió por 19 oportunidades, en las primeras 4 se detectaron el acceso a páginas no permitidas, por lo cual se realizaron los ajustes respectivos, pudiendo solventar los inconvenientes presentados, de esta forma las demás oportunidades que se corrió la prueba se obtuvo los resultados esperados al no dar paso a las páginas web prohibidas y así mismo ingresar a aquellas permitidas.

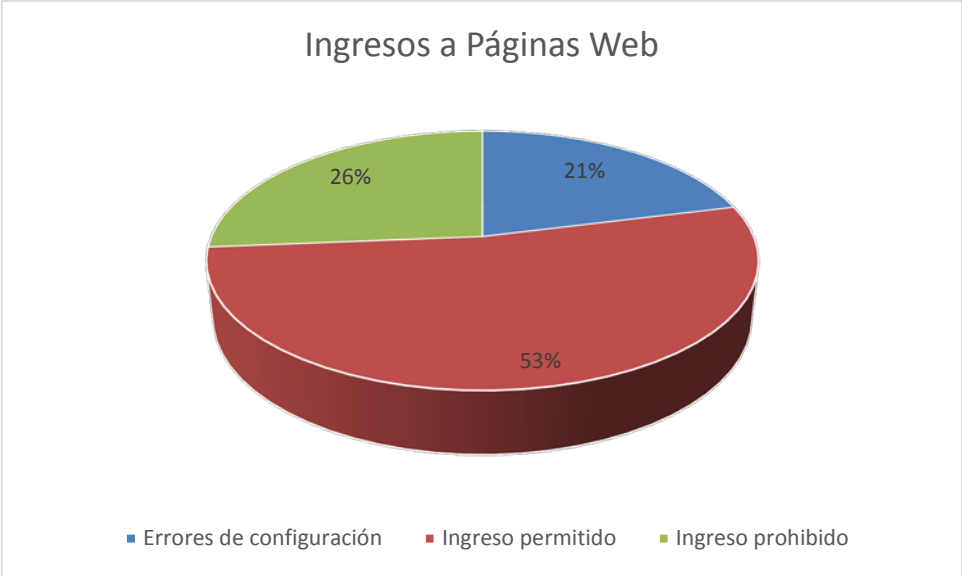


Gráfico 6. Ingreso a páginas Web.

Título: Resultado de Pruebas.

Elaboración: Burgos Alonso Richard

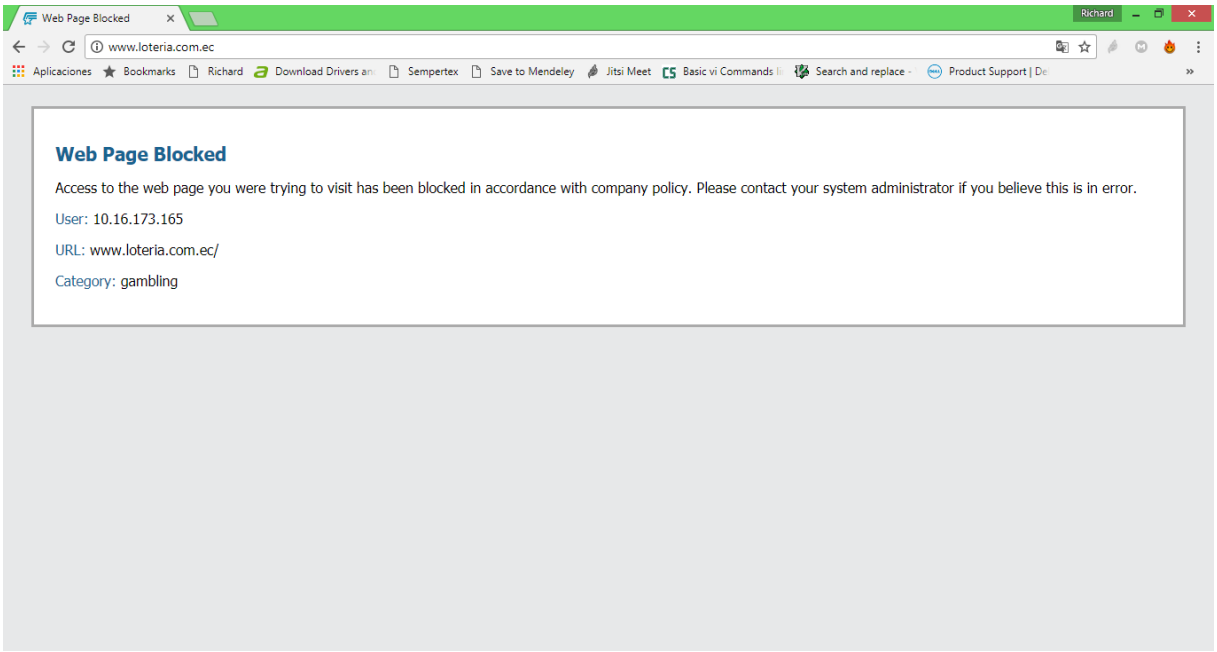


Gráfico 7. Página no permitidas.

Título: Prueba 2.

Elaboración: Burgos Alonso Richard

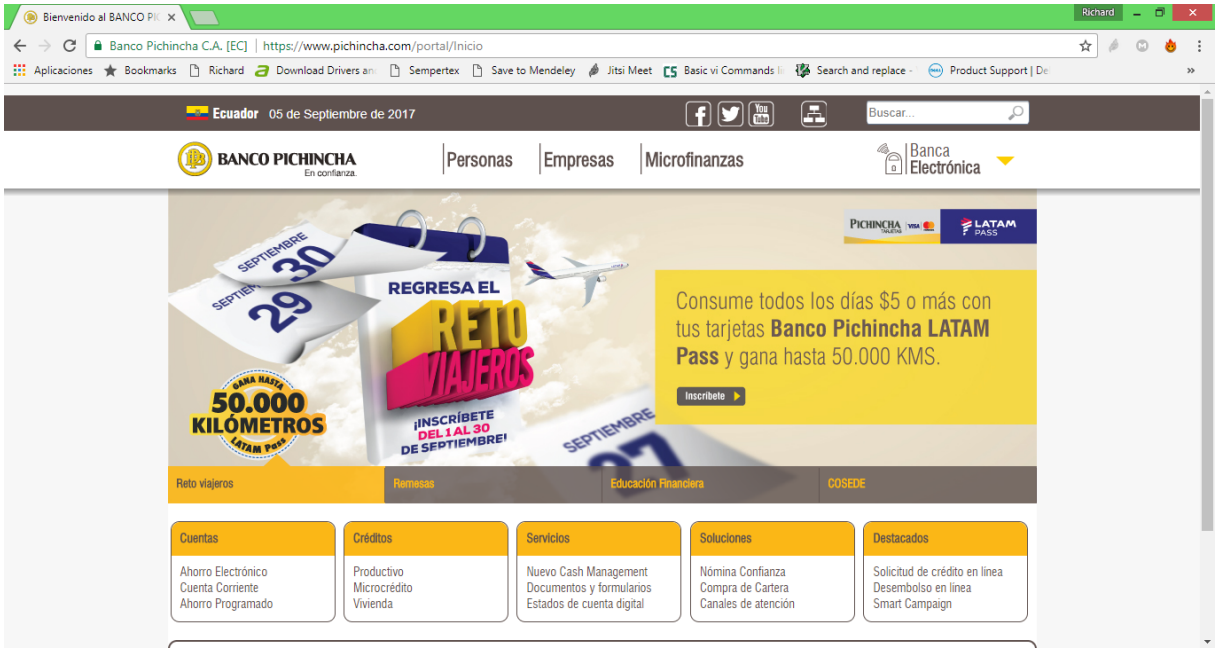


Gráfico 8. Página permitida.

Título: Prueba 2.

Elaboración: Burgos Alonso Richard

Prueba 3: Volumen:

Esta prueba consistía en la simulación de volúmenes para peticiones de páginas web. Acceder al internet de todas las maquinas posibles para probar el rendimiento de los módulos de configuración.

Escenario: Intento de ingreso al servidor por puertos

Módulo: Firewall

Caso de prueba: Intento de ataque exterior hacia el servidor por puerto.

Tipo de prueba: Seguridad.

Descripción: Intento de ingreso al servidor utilizando puertos bloqueados por IPTABLES.

La prueba se corrió por 10 oportunidades, aquí se pudo observar resultados satisfactorios al comprobar que todos los puertos se encuentran cerrados excepto el 22 que pertenece al de SSH mismo que está abierto por cuestiones de validación.

La prueba demostró que un usuario externo que trate de ingresar al servidor por algún puerto no autorizado por el firewall será rechazado de inmediato.

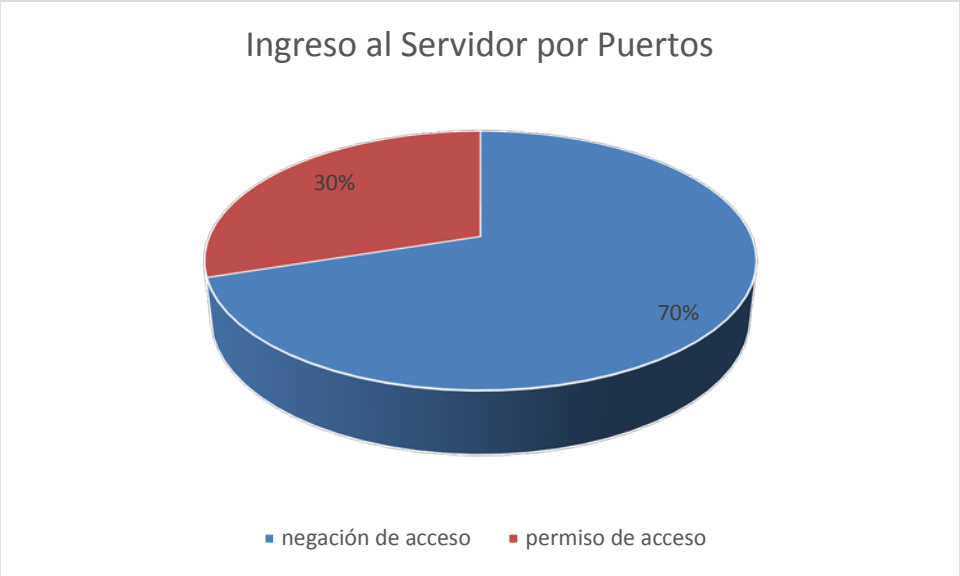


Gráfico 9. Ingreso al Servidor.

Título: Prueba 3.

Elaboración: Burgos Alonso Richard

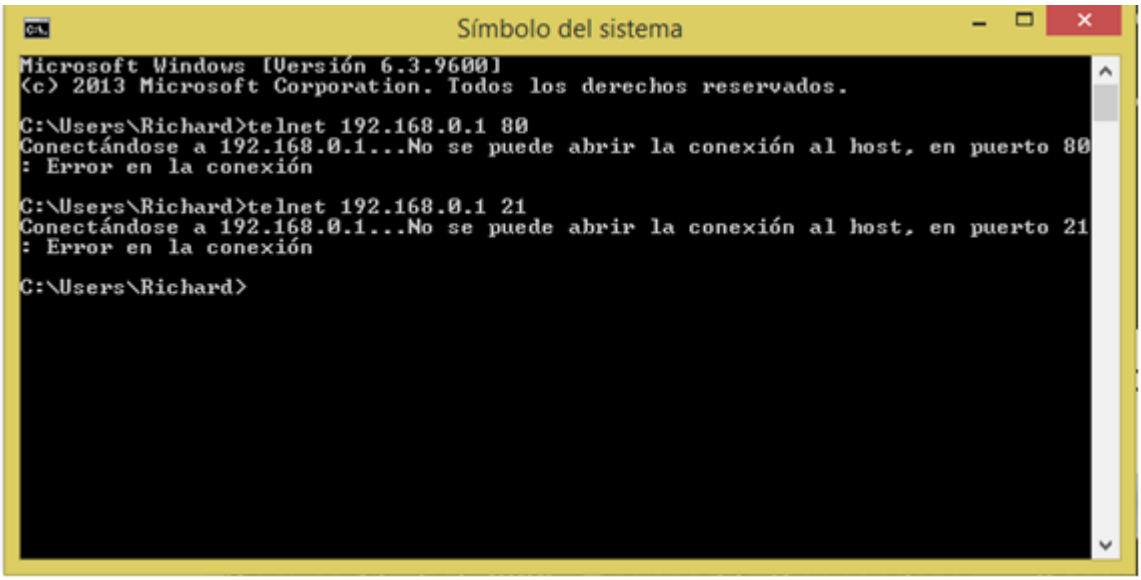


Gráfico 10. Intento de ingreso al servidor por puertos.

Título: Prueba 3.

Elaboración: Burgos Alonso Richard

Interpretaciones:

La configuración del Firewall debe ser establecido para la realidad de cada organización.

Para el desarrollo de la tesis se toma como base la teoría, pero al momento de la práctica no es tan valida, ya que la teoría debe adaptarse a la situación que se encuentra en el momento del trabajo.

El sistema operativo basado en Linux nos permite tener gran flexiblidad en las diferentes configuraciones.

4.5.2. ENCUESTA SOBRE LA IMPLEMENTACIÓN DE SOFTWARE LIBRE.

Como parte de las pruebas para ver la acogida del proyecto realizado en la Cooperativa se estableció realizar una encuesta sobre la implementación de software libre, con el objetivo de medición para el cumplimento de objetivos por lo cual se realizó el proyecto.

En este apartado procedemos a realizar la tabulación e interpretación de los datos obtenidos en la aplicación de esta encuesta, la misma que se realizó a 6 colaboradores que intervinieron en el plan piloto de software libre.

Refiérase al Anexo 8 para ver registros de la encuesta realizada.

Análisis de la pregunta número 1.

Pregunta	Respuestas		Interpretación
1.¿Conoce Ud. que es el softare ibre?	Si	67%	De las encuestas realizadas se recoge los datos siguientes: el 33% de los encuestados no conocían lo consultado y el 67% si tenían conocimiento. Tomando estos datos podemos mencionar que la mayoría de los colaboradores conocen sobre software libre.
	NO	33%	

Análisis de la pregunta número 2.

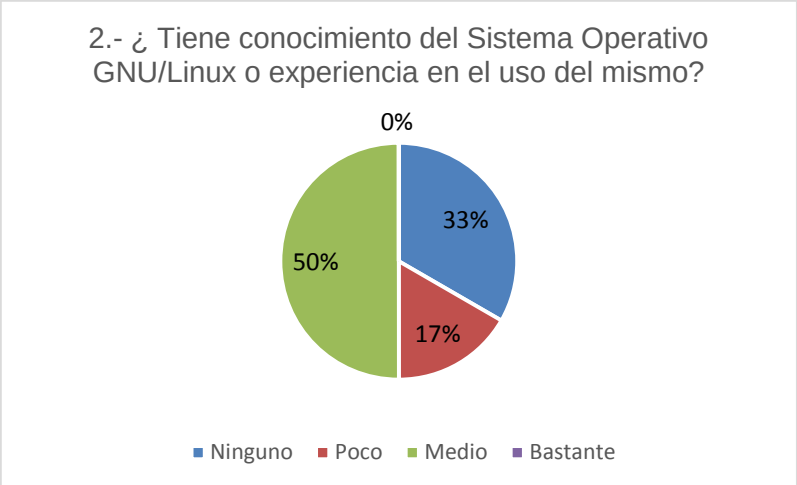


Gráfico 11. Encuesta 1 – Pregunta 2.

Elaborado por: Burgos Alonso Richard.

De los datos obtenidos, el 33% escogió la opción ninguno, el 17% la opción poco y el 50% la opción medio. Basados en estos datos podemos inferir que la mayoría de los encuestados tienen algún conocimiento sobre lo consultado, sin embargo en ciertos casos aun no haberlo utilizado. Se considera proporcionar más información sobre el sistema operativo GNU/Linux al personal de la institución.

Análisis de la pregunta número 3.

Pregunta	Respuestas		Interpretación
3.- ¿ De ser afirmativa la segunda pregunta, sabe que distribucion GNU/Linux utiliza para sus aplicaciones?	Si	67%	El 33% respondió como no y el 67% respondió como sí. Estos datos nos indican que la mayoría de los encuestados saben el tipo de distribución de software libre utiliza, así como también que generalmente se inclinan por alguna distro de una misma familia. Se proporcionó más información sobre las diferentes distro que existen.
	NO	33%	

Análisis de la pregunta número 4.

Pregunta	Respuestas		Interpretación
4.- ¿ Sabia usted que el trabajo de desarrollar software libre, es apoyado de forma comunitaria (comunidades de informáticos alrededor del mundo sin fines de lucro, para beneficio de los usuarios?	Si	67%	El 33% respondió como no y el 67% respondió como sí. Estos datos nos indican que la mayoría de los encuestados conocen sobre las comunidades de desarrollo, y tienen un conocimiento básico sobre los beneficios que estas comunidades tratan de ofrecer a los usuarios, se reforzó con información acerca de los beneficios que buscan las comunidades de desarrolladores de software libre en beneficio de los usuarios.
	NO	33%	

Análisis de la pregunta número 5.

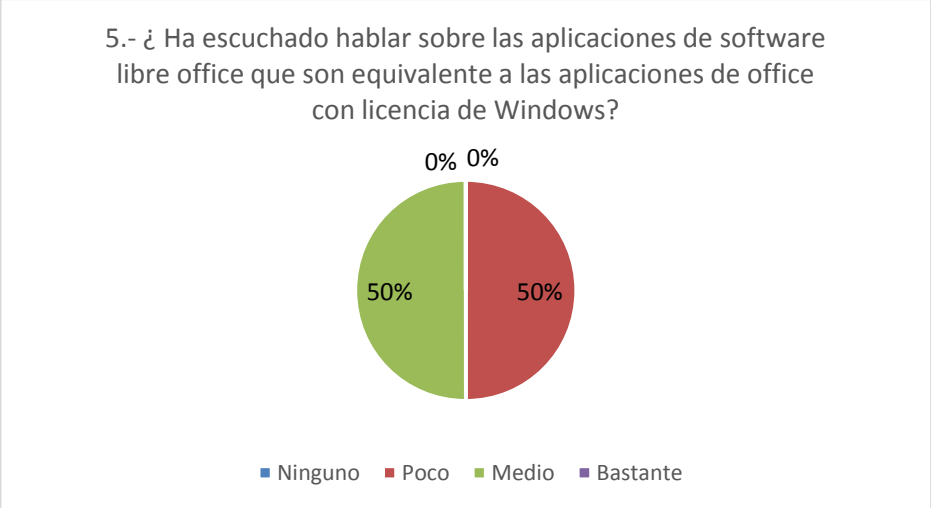


Gráfico 12. Encuesta 1 – Pregunta 5.

Elaborado por: Burgos Alonso Richard.

El 50% respondió como poco y el otro 50% respondió como medio. Estos datos nos indican que se tiene un conocimiento básico sobre estas aplicaciones, aunque no han tenido mayor interacción con estas aplicaciones, se informa la aplicación disponible en la distro de Fedora como es libre office, y otras como open office.

Análisis de la pregunta número 6.

Pregunta	Respuestas		Interpretación
6.- ¿ La Capacitación del uso del software libre en el plan piloto iniciado en la Cooperativa le ayudo en sus tareas diarias?	Si	83%	El 17% respondió como no y el otro 83% respondió como sí. De estos datos podemos considerar que la capacitación aunque en un principio tuvo algo de resistencia en los participantes, con el desarrollo de la misma fue teniendo la acogida necesaria, como para inferir que se cumplió con el objetivo por el cual se realizó el plan piloto. Se acordó con la gerencia realizar una segunda capacitación para el refuerzo de los conocimientos.
	NO	17%	

Análisis de la pregunta número 7.

Pregunta	Respuestas		Interpretación
7.- ¿Para la aplicación del plan piloto se utilizó el sistema operativo Fedora, tenía conocimiento de este sistema de software libre?	Si	50%	El 50% respondió como no y el otro 50% respondió como sí. Estos datos nos demuestran que la mitad de los colaboradores conocían del sistema operativo Fedora, así como se dio la oportunidad de ver el conocimiento de otros sistemas operativos de software libre que tenía el personal encuestado.
	NO	50%	

Análisis de la pregunta número 8.

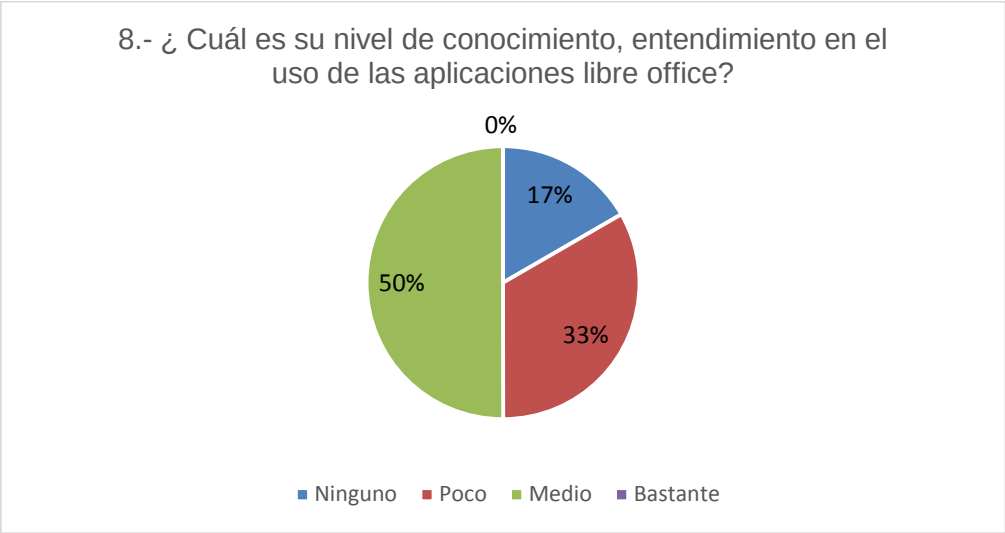


Gráfico 13. Encuesta 1 – Pregunta 8.
Elaborado por: Burgos Alonso Richard.

El 17% respondió como ninguno, el 33% respondió como medio y el 50% respondió como medio. De estos resultados, se considera un grado de entendimiento aceptable después de la capacitación impartida a los colaboradores, se realizó una segunda capacitación para reforzar los conocimientos adquiridos en la primera capacitación.

Análisis de la pregunta número 9.

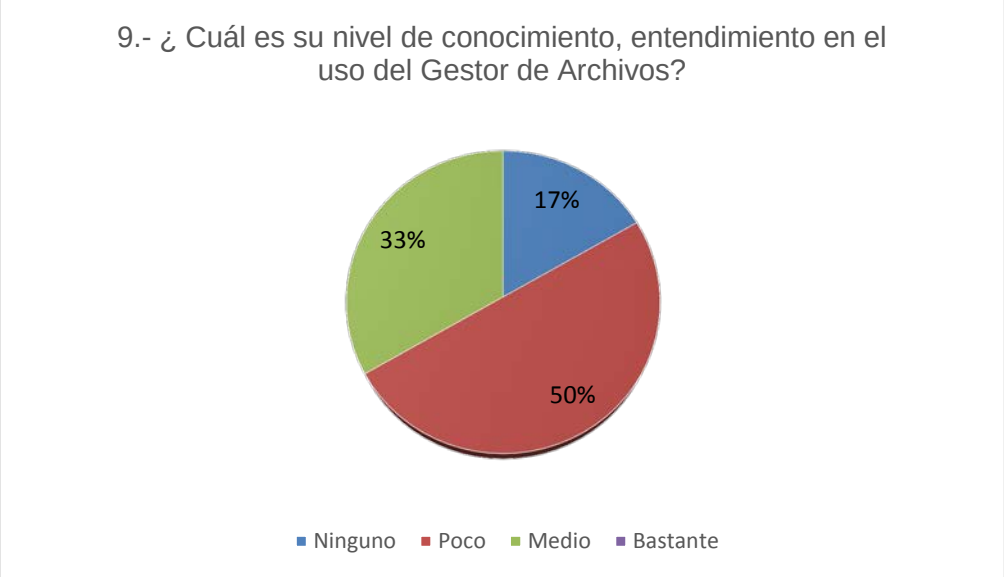


Gráfico 14. Encuesta 1 – Pregunta 9.

Elaborado por: Burgos Alonso Richard.

El 17% respondió como ninguno, el 33% respondió como medio y el 50% respondió como poco. Se considera un grado de entendimiento pobre, por lo cual se realizó un reforzamiento del tema con los colaboradores de la Cooperativa.

Análisis de la pregunta número 10.

Pregunta	Respuestas		Interpretación
10.- ¿ Se adaptó a la interfaz del sistema operativo fedora y sus aplicativos en relacion a lo experimentado en el sistema operativo Windows?	Si	83%	El 83% respondió con un sí, el 17% respondió con un no. Como todo conocimiento nuevo, se tuvo un recelo inicial que fue desapareciendo y permitiendo que los colaboradores se adapten al nuevo entorno del sistema Fedora, se considera con los datos obtenidos que el plan piloto tuvo buena acogida entre los colaboradores.
	NO	17%	

Análisis de la pregunta número 11.

Pregunta	Respuestas		Interpretación
11.- ¿El uso de software libre le beneficio en la optimiz60ptimización de recursos en la Cooperativa?	Si	83%	El 83% respondió con un sí, el 17% respondió con un no. Se considera con los datos obtenidos que los colaboradores entendieron el objetivo que se buscaba con el uso de software libre. Y la importancia para la organización de que ellos tengan este conocimiento para su posterior aplicación.
	NO	17%	

Análisis de la pregunta número 12.

Pregunta	Respuestas		Interpretación
12.- ¿En base a la capacitación, desenvolvimiento obtenido recomendaría el uso de software libre a usuarios que utilizan software con licencia?	Si	83%	El 83% respondió con un sí, el 17% respondió con un no. De los datos obtenidos, los colaboradores han tenido buena aceptación y piensan que el uso de software libre puede beneficiar a otros usuarios, existen colaboradores que tienen la iniciativa de aplicar en sus hogares el uso de software libre
	NO	17%	

Análisis de la pregunta número 13.

Pregunta	Respuestas		Interpretación
13.- ¿ Cree usted que sería factible aplicar el uso de software libre en todas las estaciones de la Cooperativa?	Si	83%	El 83% respondió con un sí, el 17% respondió con un no. Se considera por los datos obtenidos que el plan piloto tuvo buena acogida y la mayoría de los usuarios ven factible su aplicación en todas las estaciones de la Cooperativa.
	NO	17%	

4.5.3. ENCUESTA SOBRE LA IMPLEMENTACIÓN DE POLÍTICAS DE SEGURIDAD.

Se estableció realizar una encuesta sobre la implementación de políticas de seguridad, como medio de medición para el cumplimento de objetivos por lo cual se realizó el proyecto.

En este apartado procedemos a realizar la tabulación e interpretación de los datos obtenidos en la aplicación de esta encuesta, la misma que se realizó a 15 colaboradores que se encuentran involucrados en la organización.

Refiérase al Anexo 9 para ver registros de la encuesta realizada.

Análisis de la pregunta número 1.

Pregunta	Respuestas		Interpretación
1.- Conoce sobre políticas de seguridad en la información aplicables a organizaciones o instituciones financieras	Si	80%	De los datos obtenidos en la encuesta realizada, tenemos que el 80% respondió que sí y un 20% respondieron que no, de lo cual apreciamos que la mayoría tiene
	NO	20%	

			conocimiento sobre políticas de seguridad en la información, este conocimiento en la mayoría de los casos ha sido adquirido a través de la interacción con personal de otras instituciones financieras, en los talleres que sabe dar las instituciones públicas, como por ejemplo el SRI, Banco Central entre otras.

Análisis de la pregunta número 2.

Pregunta	Respuestas		Interpretación
2.- ¿La Cooperativa tenía definidas e implementadas políticas de seguridad en la información?	Si	80%	De los datos obtenidos el 67% de los colaboradores escogieron el no y el 33% escogieron el sí, con estos resultados se manifiesta un desconocimiento mayoritario de si poseían y tenían implementadas políticas de seguridad en la Cooperativa, se evidencia que no existían políticas de seguridad estructuradas y debidamente informadas al personal de la institución.
	NO	20%	

Análisis de la pregunta número 3.

Pregunta	Respuestas		Interpretación
3.- ¿Recibió información sobre las políticas de seguridad en la información implementadas en la Cooperativa?	Si	87%	El 87% de consultados manifestó haber recibido dicha información, mientras el 13% de los consultados negó haber recibido la información, el personal en su totalidad fue informado sobre la implementación de las políticas de seguridad de la información en la Cooperativa, por lo que se realizó una nueva difusión sobre las políticas que se implantaron en la Cooperativa.
	NO	13%	

Análisis de la pregunta número 4.

Pregunta	Respuestas		Interpretación
4.- El rol de usuario administrativo esta autentificado en cada estación de trabajo de la Cooperativa.	Si	53%	El 53% de los encuestados contesto sí, mientras el 47% respondió no, con estos resultados se establece que la mayoría tiene conocimiento que las estaciones de trabajo tienen la autentificación de usuario administrativo de las estaciones, se reforzó sobre los beneficios que trae la aplicación de esta política en la seguridad de la información de la institución.
	NO	47%	

Análisis de la pregunta número 5.

Pregunta	Respuestas		Interpretación
5.- Es necesario la aplicacion de la Carta de Confidencialidad de la información para definir roles de Usuarios.	Si	73%	El 73% respondió que sí y el 27% respondieron que no, ante lo cual se determina que la mayoría de los colaboradores de la Cooperativa, cree en la aplicación de las políticas de seguridad de la información, se reforzó el motivo por el cual deben ser aplicadas en la Cooperativa mediante el proyecto implementado.
	NO	27%	

Análisis de la pregunta número 6.

Pregunta	Respuestas		Interpretación
6.- Cree beneficioso la aplicacion del restringir las unidades de almacenamiento externos, como medida implementada para mantener la confidencialidad de la información del cliente y seguridad del sistema informático.	Si	53%	El 53% de los encuestados manifestó que si y el 47% de los encuestados manifestó que no, de los resultados obtenidos se concluye que en ese punto que es una política aplicable de seguridad en la información, que algunos usuarios tienen resistencia a la aplicación de esta clase de políticas en la organización.
	NO	47%	

Análisis de la pregunta número 7.

Pregunta	Respuestas		Interpretación
7.- Cree beneficioso la aplicación del acceso restringido a sitios WEB, para evitar posibles infecciones por virus, robo de información, delitos informáticos.	Si	53%	El 53% de los colaboradores manifestó que si y el 47% de los encuestados manifestó que no, de los resultados obtenidos se visualiza que hay resistencia a la aplicación de esta clase de políticas en la organización en algunos colaboradores, y se difundió los beneficios que conlleva para la Cooperativa este tipo de políticas.
	NO	47%	

Análisis de la pregunta número 8.

Pregunta	Respuestas		Interpretación
8.- Cree beneficioso la aplicación de la clasificación y etiquetado de la información para la facil ubicación de la documentación en el momento que sea requerida.	Si	93%	El 93% de los colaboradores respondieron que sí y el 7% respondieron que no, de esto se concluye que esta política de seguridad en la información aplicada tuvo excelente acogida de parte de los colaboradores de la Cooperativa.
	NO	7%	

Análisis de la pregunta número 9.

Pregunta	Respuestas		Interpretación
9.- El tiempo de acceso a páginas web actualmente es rapido para sus tareas diarias.	Si	67%	El 67% de los encuestados respondió que sí y el 33% manifiesta que no, de esto se determina que la mayoría de los usuarios creen en la mejora de acceso a la información del internet con la aplicación de la red propuesta en el proyecto aplicado en la Cooperativa.
	NO	33%	

Análisis de la pregunta número 10.

Pregunta	Respuestas		Interpretación
10.-La restricción a páginas de redes sociales contribuye en la productividad del colaborador, medible en tiempo de desarrollo de las tareas.	Si	80%	De la encuesta realizada se obtuvo un 80% contesto que sí y un 20% contesto que no, de lo cual podemos mencionar que la mayoría de los colaboradores creen en una mejora en su productividad para el desarrollo sus tareas, con la aplicación de esta política de seguridad implementada en el proyecto.
	NO	20%	

Análisis de la pregunta número 11.

Pregunta	Respuestas		Interpretación
11.- La compartición de archivos entre las estaciones es más agíl actualmente en la ejecucion de las tareas.	Si	93%	El 93% contesto que sí y el 7% contesto que no, con lo que se establece que el personal de la Cooperativa está satisfecho con la nueva distribución de red que se realizó a través del proyecto ejecutado.
	NO	7%	

Análisis de la pregunta número 12.

Pregunta	Respuestas		Interpretación
12.- El uso de los dispositivos como escáner e impresoras con la nueva distribución de la red es satisfactorio, con relación a la distribución de la red antes de la ejecución del Proyecto.	Si	87%	El 87% contesto que sí y el 13% contesto que no, al igual que en el análisis de la pregunta número 11, se establece que el personal de la cooperativa está satisfecho con la nueva distribución de red que se realizó a través del proyecto ejecutado.
	NO	13%	

Análisis de la pregunta número 13.

Pregunta	Respuestas		Interpretación
13.- Los cambios realizados para el manejo de la información en la Cooperativa es.	Positivo	87%	El 87% contesto que es positivo y el 13% contesto que es negativo, podemos establecer que el personal de la Cooperativa está satisfecho con los resultados obtenidos en la aplicación del proyecto en la organización, se difunde y hace la concientización hacia el personal, de los beneficios que con lleva la aplicación de este proyecto en la Cooperativa.
	Negativo	13%	

CAPITULO V

CONCLUSIONES

Con la ejecución del proyecto realizado en la Cooperativa de ahorro y crédito CACPE Manabí, se ha logrado:

- Siendo que la información que posee la cooperativa es de vital importancia, se logró mejorar las políticas de seguridad de la información, así como se concientizo al personal en el uso responsable y adecuado de la información que poseen de los clientes y que reposa en los archivos de la Institución.
- Se organizó la estructura de la red, de tal manera que permitió establecer normativas que ayudaron a mejorar el desempeño de la red, la reducción del consumo de ancho de banda y mejora en la navegabilidad, todo esto en beneficio de la cooperativa.
- La aplicación del plan piloto en el uso de software libre, permitió fomentar el uso de software libre en los colaboradores, obteniendo un nivel de aceptación favorable de parte de ellos, a tal punto que algunos piensan aplicar en sus hogares este tipo de software. Para la dirección de la cooperativa ha sido una aplicación llamativa, que les permite optimizar recursos y de esta optimización, poder redireccionar los mismos a otras necesidades de la Cooperativa.
- Se estableció el análisis y evaluación en conjunto con la dirección de la organización para la ampliación del uso de software libre en todas las estaciones de la Institución.
- Se permitió con el desarrollo de este proyecto, concientizar a la dirección en la importancia de realizar la inversión para mejorar la seguridad de la información así como mejorar los recursos en el área de tecnología de la información, que la Cooperativa dispone.
- Se establece el compromiso de los colaboradores para con sus clientes en mantener la confidencialidad de la información. Para lo cual se realizó una declaración de confidencialidad, el registro de esta declaración se puede ver en el Anexo 10.
- Con lo realizado en este proyecto se benefició a la cooperativa, sus colaboradores y sus clientes, en un mejor uso de los recursos y la información.

RECOMENDACIONES

Como recomendaciones se establece:

- El área de tecnología de la información, debe mantener el uso de las políticas de seguridad implementadas, como la revisión constante y dinámica de la red, para garantizar la confidencialidad, integridad y disponibilidad de la información.
- Incorporar personal diestro en informática, para reforzar el área de tecnología de la información, en beneficio de la Cooperativa.
- Pedir estudio de factibilidad para el uso del sistema financiero que posee la cooperativa en entornos de software libre, con la finalidad de llegar a establecer el uso de software libre en todas las estaciones de la Cooperativa.
- Realizar planificación de auditoria informática, como mínimo una vez al año, con el objetivo de poder establecer la eficacia de las políticas de seguridades implementadas, y de ser el caso mejorarlas.
- Programar y fortalecer el conocimiento en el personal, a través de capacitaciones regulares en el uso de software libre.

Por lo indicado en los párrafos anteriores se recomienda la contratación de una persona que cumpla el perfil para desempeñarse como responsable del área informática de la Cooperativa, esto permitirá un mejor desempeño en el área de tecnología de la información.

BIBLIOGRAFÍA

(Diciembre de 2013). *ReCIBE, 2*(3), 1-17.

A. García, F. García. (2015). *ESTUDIO SOBRE LA EVOLUCIÓN DE LAS SOLUCIÓNES TECNOLÓGICAS PARA DAR SOPORTE A LA GESTIÓN DE LA INFORMACIÓN.* SALAMANCA: GRIAL.

asle.com. (s.f.). *Asociación de Software libre Ecuador*. Recuperado el 03 de marzo de 2016, de http://www.asle.ec

Bailey, S. M. (2015). INFORMATION TECHNOLOGY SERVICE MANAGEMENT FRAMEWORKS. *ProQuest LLC.*, 24. Recuperado el 12 de enero de 2016, de http://www.soporteremoto.com.mx/help_desk/articulo04.html

Bolaños, S., González, R., Medina, V., & Barón, J. (Junio de 2014). Conceptual framework language – CFL –. *Dyna, 81* (185), 124-131.

Bolaños, S., Medina, V., & Aguilar, J. (2009). Principios para la Fromalización de la Ingeniería de Software. *Ingeniería*, 31-37.

Booch, G. R. (2005). *The Unified Modeling Language User Guide.* Addison-Wesley.

Carrera, E. (2012). El Costo de la Seguridad en Disposotivos Móviles. *EIDOS*, 1-7.

Castellaro, M., Romaniz, S., Ramos, J., & Pessolani, P. (s.f.). Hacia la Ingeniería de Software Seguro. 1-10.

CentOS.7. (s.f.). *www.centos.org*. Recuperado el 25 de julio de 2016, de http://www.centos.org/

Cooperativa CACPE Manabí. (1990). *Estatuto de conformación.* Portoviejo.

Dordoigne, J. (2015). *Redes Informáticas. Nociones Fundamentales.* Barcelona: Eni.

Ekuni, R., Vaz, L., & Amodeo Bueno, O. F. (2011). Levels of processing: the evolution of a framework. *Psychology & Neuroscience, 4*(3), 333-339.

G.Aucapiña, T. Guachi. (julio de 2012). *Seguridad informática Normas ISO. Sistemas de Información. Redes Cooperativas.* Obtenido de Repositorio interno de la Univ. Técnica de Ambato: http://redi.uta.edu.ec/jspui/handle/123456789/2361

Gamma, E., Helm, R., Johnson, R., & Vlisides, J. (1995). *Design Patterns.* Addison-Wesley.

García PG, Vidal LMJ. (2016). La informática y la seguridad. Un tema de importancia para el directivo. *INFODIR*, 47-58.

Gasca, M., Camargo, L., & Medina, B. (Abril-Junio de 2014). Metodología para el desarrollo de aplicaciones móviles. *Tecnura, 18*(40), 20-35.

Gasca, M., Camargo, L., & Medina, B. (Abril - Junio, de 2014). Metodología para el desarrollo de aplicaciones móviles. *Tecnura, 18*(40), 20 - 35 .

Gómez, A. (2011). Enciclopedia de la seguridad informática. México: Alfombra.

Gómez, A. (2011). *Enciclopedia de la Seguridad Informática.* México: Alfaomega.

Gutiérrez, J. (s.f.). *¿Qué es un framework web?* Recuperado el 12 de septiembre de 2016, de http://www.lsi.us.es/~javierj/investigacion_ficheros/Framework.pdf

Hatton, R. (2005). *Swt: A Developer's Notebook.* O'Reilly & Associates.

Heller, E. (2007). *Psicología del Color.* Gustavo Gili.

Hernández, J. (2005). *Software Libre: Técnicamente viable, Económicamente sostenible y socialmente justo.* Recuperado el 15 de enero de 2016, de https://gent.softcatala.org/jmas/swl/llibrejmas.pdf

Jarillo, J., & Martínez, J. (1991). The international expansion of Spanish firms: towards an integrative framework for international strategy. *Corporate and industry strategies for Europe*, 282-302.

Kizza, J. (2013). *Standardization and Security Criteria: Security Evaluation of Computer Products.* London: Springer.

Kuroe J., R. K. (2010). Redes de computadoras un enfoque descendente. Madrid: Pearson Educación.

Leiva, I., & Villalobos, M. (2015). Método ágil híbrido para desarrollar software en dispositivos móviles. *Ingeniare. Revista Chilena de Ingeniería, 23*(3), 473-488.

Macia, N., Lanfranco, E., & Venosa, P. (2014). Seguridad en dispositivos móviles: un enfoque práctico. *Workshop de Investigadores en Ciencias de la Computación*, 837-841.

Maeda, J. (2005). *Las Leyes de la Simplicidad.* Gedisa S.A.

Marulanda, C., & Ceballos, J. (2012). UNA REVISIÓN DE METODOLOGÍAS SEGURAS EN CADA FASE DEL CICLO DE VIDA DEL DESARROLLO DE SOFTWARE . *Ing. USBMed*, 1-8.

Meyer, B. (1999). *Construcción de Software Orientado a Objetos.* Prentice Hall.

Montiel, J., Hernández, E., & López, J. (Diciembre de 2012). Computación Móvil. *Ingeniare. Revista Chilena de Ingeniería, 20*(3), 282-283.

Morin, E. (2005). *Introducción al Pensamiento Complejo.* Gedisa S.A.

Pimienta, R., Aguilar, G., Ramírez, M., & Gallegos, G. (noviembre de 2014). Métodos de programación segura en Java para aplicaciones móviles en Android. *Ciencia Ergo Sum, 21*(3), 243-248.

Portal ISO 27001. (2005). *Sistema de la gestión de la seguridad de la información.* Recuperado el 12 de enero de 2016, de http://www.iso27000.es/sgsi.html

Ramírez, G. (s.f.). La seguridad en aplicaciones móviles: estrategias en el mundo actual. *Escuela de Ciencias Básicas Tecnología e Ingeniería*, 1-17.

Rezende, S. (Abril - Junio de 2003). Internationalisation Processes: an Analytical Framework. *RAC - Revista de Administração Contemporânea, 7*(2), 137-156.

Rodriguez, M. (2003). Definición de una arquitectura para teléfonos móviles. *IBM*.

Rosen, K. (2004). *Matemática Discreta.* Mc Graw Hill.

Software Assurance. (18 de Mayo de 2012). Software Assurance Pocket Guide Series. *Development, Volume V – Version 2.0, May 18, 2012*, 1-37.

Solarte, F. (2015). Metodología de análisis y evaluación de riesgos aplicados a la seguridad informática y de información bajo la norma ISO/IEC 27001. *RTE - Revista Tecnológica ESPOL*, 16.

Sosa, J. (27 de enero de 2012). *Clasificación de la Información*. Recuperado el 11 de enero de 2016, de http://pegasus.javeriana.edu.co/~CIS1130SD03/Documentos_files/Clasificacion_de_la_Informacion.pdf

Stallings, W. (2010). *Cryptography and Network Security: Principles and Prac tice.* New York: Prentice Hall.

Tanenbaum, A. S. (2003). *Redes de Computadoras.* México: Pearson.

Teufel, B. S. (1995). *Compiladores conceptos fundamentales.* Addison: Wesley.

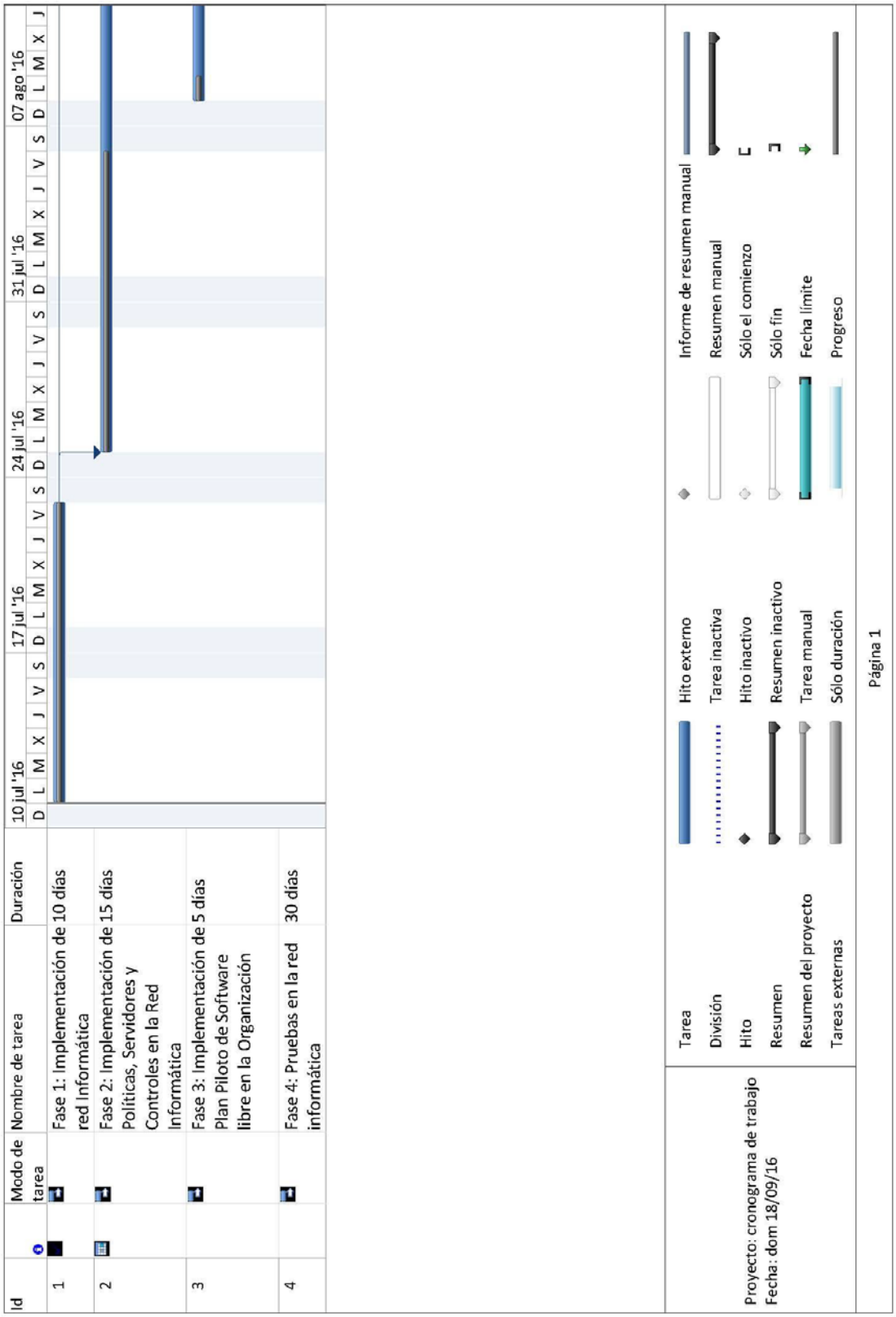
Tucker, A., & Noonan, R. (2002). *Programming Languages Principles and Paradigms.* McGraw Hill.

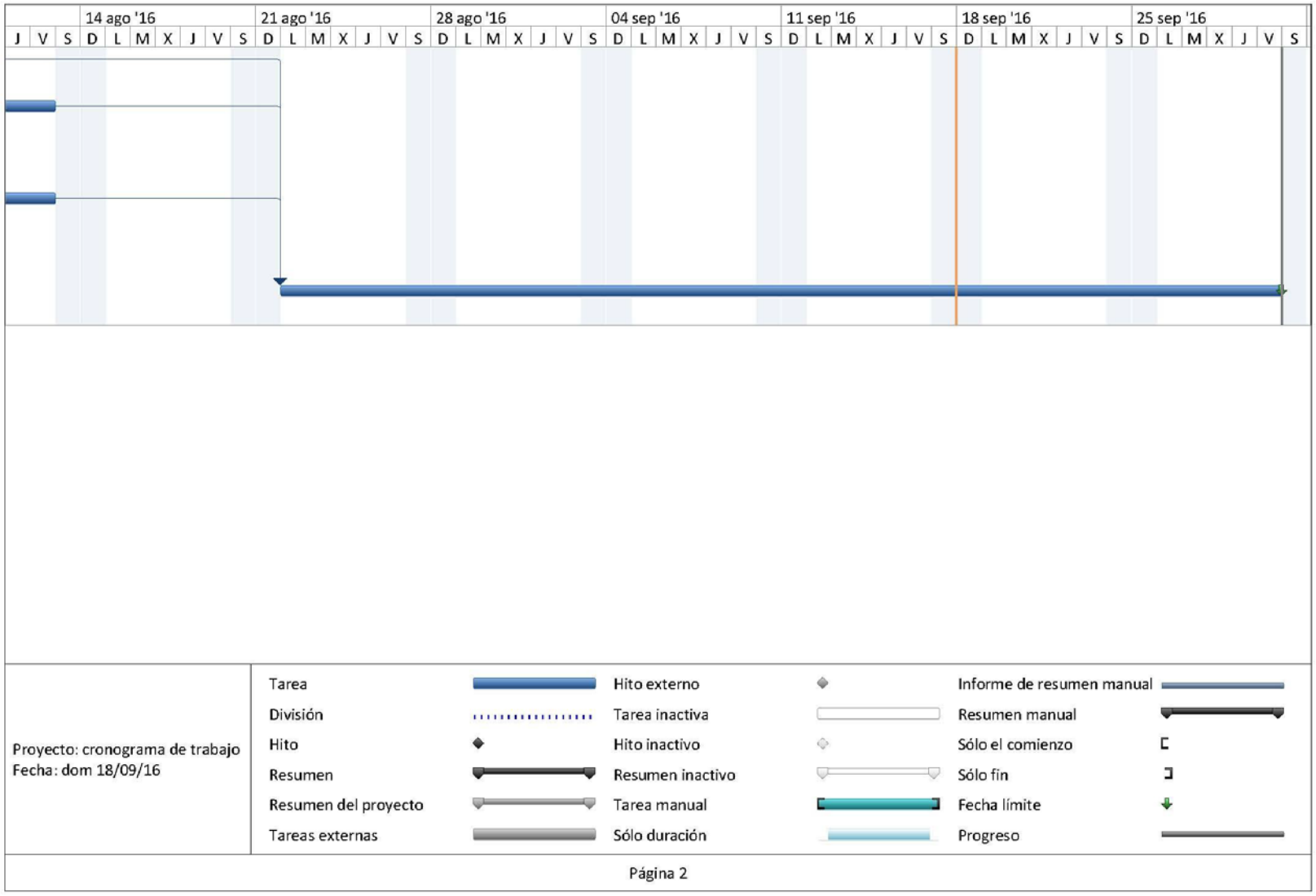
Webmin. (25 de julio de 2016). Recuperado el 15 de octubre de 2016, de http://www.webmin.com

Webmin.com. (s.f.). Recuperado el 25 de julio de 2016, de http://www.webmin.com/

ANEXOS

ANEXO 1: CRONOGRAMA DE IMPLEMENTACIONES




14 ago '16
21 ago '16
28 ago '16
04 sep '16
11 sep '16
18 sep '16
25 sep '16
J V S D L M X J V S D L M X J V S D L M X J V S D L M X J V S D L M X J V S D L M X J V S
Proyecto: cronograma de trabajo
Fecha: dom 18/09/16
Tarea
División
Hito
Resumen
Resumen del proyecto
Tareas externas
Hito externo
Tarea inactiva
Hito inactivo
Resumen inactivo
Tarea manual
Sólo duración
Informe de resumen manual
Resumen manual
Sólo el comienzo
Sólo fin
Fecha límite
Progreso
Página 2

ANEXO 2: CONOCIMIENTO DE SEGURIDAD EN LA INFORMACIÓN

Encuesta sobre la Seguridad en la información

Organización: Cooperativa CACPE-Manabí. **Fecha:** 03 de Agosto 2016.

Encuestado: Carlos Eduardo Ochoa Figueroa.

Encuestador: _____

1.- Que Entiende por Seguridad en la Información.

Son metodos que se utilizan para protejer los sistemas informaticos sobre terceros para que no ya haken o sustrayan información valida del sistema informativo.

2.- La Organización ha tenido o tienen un presupuesto destinado a la Seguridad en la Información.

Si

3.- La Organización cuenta con Políticas o normativas de Seguridad en la información.

Si de acuerdo al departamento de informatica.

4.- Se tiene un área o Departamento de Seguridad en la Información? De ser positiva la Respuesta a que nivel Jerárquico se encuentra?

Si jerarquicamente de nivel 5.

5.- La Organización sigue algún estándar o norma para la gestión de la seguridad en la información?

Si.

6.- La Organización sigue algún estándar o norma para la gestión de riesgos?

(Si) No tengo conocimiento

7.- La Organización sigue alguna norma o política para la clasificación de información?

No solo impiricamente.

8.- La Organización tiene establecidos Acuerdos de Confidencialidad?

No tengo conocimiento.

9.- La Organización tiene definido los roles y responsabilidades de los colaboradores en el uso de los sistemas?

No hemos seguidos normas en gestion de riesgos

10.- La Organización ha realizado evaluaciones de seguridad a sus sistemas?

No en el tiempo que e laborado.

Encuestado

Encuestador

Encuesta sobre la Seguridad en la Información

Organización: Coop. Coopa Manolo **Fecha:** Potrerillos Agosto 03/2016

Encuestado: Nohemi Elizabeth Zambrano Rivera

Encuestador: _____

1.- Que Entiende por Seguridad en la Información.

Son técnicas utilizadas que se aplican a los sistemas informáticos y externos para q' la información q se maneja en ambas instituciones esté protegida y no caiga en manos inescrupulosas

2.- La Organización ha tenido o tienen un presupuesto destinado a la Seguridad en la Información.

No

3.- La Organización cuenta con Políticas o normativas de Seguridad en la Información.

La institución si cuenta con políticas y normativas de Seguridad Informáticas

4.- Se tiene un área o Departamento de Seguridad en la Información? De ser positiva la Respuesta a que nivel jerárquico se encuentra?

Nivel 5

5.- La Organización sigue algún estándar o norma para la gestión de la seguridad en la información?

No

6.- La Organización sigue algún estándar o norma para la gestión de riesgos?

Si

7.- La Organización sigue alguna norma o política para la clasificación de información?

Si de acuerdo al Departamento de Defensa las políticas de enforcement

8.- La Organización tiene establecidos Acuerdos de Confidencialidad?

Si

9.- La Organización tiene definido los roles y responsabilidades de los colaboradores en el uso de los sistemas?

Si

10.- La Organización ha realizado evaluaciones de seguridad a sus sistemas?

No

Encuestado

Encuestador

Encuesta sobre la Seguridad en la información

Organización: Coop. Cacpe Manabi **Fecha:** 3 Agosto 2016

Encuestado: Victor Andrade Granda

Encuestador: _____

1.- Que Entiende por Seguridad en la Información.

Es una Manera de tener Seguridad en los Sistemas Informaticos para que personas ajenas no puedan sacar información de la institución

2.- La Organización ha tenido o tienen un presupuesto destinado a la Seguridad en la *Información.*

Si

3.- La Organización cuenta con Políticas o normativas de Seguridad en la información.

Si Existen si tiene las políticas adecuadas de la Seguridad de la Información

4.- Se tiene un área o Departamento de Seguridad en la Información? De ser positiva la Respuesta a que nivel Jerárquico se encuentra?

Si en el Nivel 5

5.- La Organización sigue algún estándar o norma para la gestión de la seguridad en la información?

Si

6.- La Organización sigue algún estándar o norma para la gestión de riesgos?

SI

7.- La Organización sigue alguna norma o política para la clasificación de información?

De acuerdo al departamento se realizan las políticas de Información

8.- La Organización tiene establecidos Acuerdos de Confidencialidad?

SI

9.- La Organización tiene definido los roles y responsabilidades de los colaboradores en el uso de los sistemas?

SI

10.- La Organización ha realizado evaluaciones de seguridad a sus sistemas?

NO

Encuestado **Encuestador**

ANEXO 3: CONFIGURACIÓN SQUID

```
#
# Configuración básica
#
# Example rule allowing access from your local networks.
# Adapt to list your (internal) IP networks from where browsing
# should be allowed
#acl localnet src 10.0.0.0/8    # RFC1918 possible internal network
#acl localnet src 172.16.0.0/12    # RFC1918 possible internal network
#acl localnet src 192.168.0.0/16    # RFC1918 possible internal network
#acl localnet src 192.168.189.0/22 # 189
#acl localnet src 192.168.190.0/22 # 190
#acl localnet src 192.168.191.0/22 # 191
acl localnet src 192.168.0.0/16 #Permitir todo el rango de red 192.168.x.x/16
acl localnet src fc00::/7 # RFC 4193 local private network range
acl localnet src fe80::/10 # RFC 4291 link-local (directly plugged) machines
acl SSL_ports port 443
acl Safe_ports port 80 # http
acl Safe_ports port 21 # ftp
acl Safe_ports port 443 # https
acl Safe_ports port 70 # gopher
acl Safe_ports port 210 # wais
acl Safe_ports port 1025-65535 # unregistered ports
acl Safe_ports port 280 # http-mgmt
acl Safe_ports port 488 # gss-http
acl Safe_ports port 591 # filemaker
acl Safe_ports port 777 # multiling http
acl CONNECT method CONNECT

#
# Recommended minimum Access Permission configuration:
#
# Deny requests to certain unsafe ports
http_access deny !Safe_ports

# Deny CONNECT to other than secure SSL ports
http_access deny CONNECT !SSL_ports

# Only allow cachemgr access from localhost
http_access allow localhost manager
http_access deny manager

# We strongly recommend the following be uncommented to protect innocent
# web applications running on the proxy server who think the only
# one who can access services on "localhost" is a local user
#http_access deny to_localhost
#
# INSERT YOUR OWN RULE(S) HERE TO ALLOW ACCESS FROM YOUR CLIENTS
#
# Example rule allowing access from your local networks.
# Adapt localnet in the ACL section to list your (internal) IP networks
# from where browsing should be allowed
http_access allow localnet
http_access allow localhost
# And finally deny all other access to this proxy
http_access deny all
# Squid normally listens to port 3128
http_port 3128 transparent #Permitir operar en el puerto 3128 de forma transparente

# Uncomment and adjust the following to add a disk cache directory.
cache_dir ufs /var/spool/squid 1024 16 256
# Leave coredumps in the first cache dir
coredump_dir /var/spool/squid
#
# Add any of your own refresh_pattern entries above these.
#
refresh_pattern ^ftp:                1440    20%    10080
refresh_pattern ^gopher:    1440    0%    1440
refresh_pattern -i (/cgi-bin/|\?) 0    0%    0
refresh_pattern .        0    20%    4320
```

ANEXO 4: CONFIGURACIÓN DNS

1.168.192.in-addr.arpa.zone

```
$TTL 86400
@ IN SOA ns1.cacpe.fin.ec. admin.cacpe.fin.ec. (
                                        2016091701 ; serie
                                        28800 ;
                                        7200 ;
                                        604800 ;
                                        86400 ; tiempo total
)
@       IN NS     ns1.cacpe.fin.ec.
1       IN PTR    proxy.cacpe.fin.ec.
1       IN PTR    dns.cacpe.fin.ec.
```

cacpe.fin.ec.zone

```
$TTL   86400
@          IN SOA ns1 admin.cacpe.fin.ec. (
                        2016091701     ; serie
                        28800          ; refresco
                        7200           ; reintento
                        604800         ; expiracion
                        86400          ; tiempo total
)
; Servidor DNS
@                   IN NS                ns1
ns1                 IN A                 192.168.1.1
dns                 IN CNAME ns1

proxy               IN A                 192.168.1.1
base                IN A                 192.168.0.100

; Equipo WLAN
wlan                IN          A        192.168.1.100
```

named.conf

```
options {
        directory "/var/named";
        dump-file "/var/named/data/cache_dump.db";
    statistics-file "/var/named/data/named_stats.txt";

        query-source address * port 53;
};

controls {
    inet 127.0.0.1 allow { localhost; } keys { rndckey; };
};

zone "." IN {
        type hint;
        file "named.ca";
};

zone "localdomain" IN {
        type master;
        file "localdomain.zone";
        allow-update { none; };
};

zone "localhost" IN {
        type master;
        file "localhost.zone";
        allow-update { none; };
};

zone "0.0.127.in-addr.arpa" IN {
        type master;
        file "named.local";
        allow-update { none; };
};
```

```
zone "0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.ip6.arpa" IN {
      type master;
            file "named.ip6.local";
            allow-update { none; };
};

zone "255.in-addr.arpa" IN {
            type master;
            file "named.broadcast";
            allow-update { none; };
};

zone "0.in-addr.arpa" IN {
            type master;
            file "named.zero";
            allow-update { none; };
};


zone "cacpe.fin.ec" IN {
            type master;
            file "cacpe.fin.ec.zone";
            allow-update { none; };
};

// Rerversos de las redes en la LAN

zone "1.168.192.in-addr.arpa" IN {
            type master;
            file "1.168.192.in-addr.arpa.zone";
            allow-update { none; };
};

include "/etc/rndc.key";
```

ANEXO 5: CONFIGURACIÓN DHCP

```
option domain-name "cacpe.local";
log-facility local7;
shared-network red_1 {
   subnet 192.168.0.0 netmask 255.255.0.0 {
            #interface enp1s1;
            option routers 192.168.1.1;
            option subnet-mask 255.255.255.0;
            #option broadcast-address 192.168.190.255;
            option domain-name "cacpe.local";
            #option domain-name-servers 208.67.222.222, 208.67.220.220;
            #option domain-name-servers 192.168.190.6, 192.168.190.11;
            option domain-name-servers 8.8.8.8, 192.168.105.3;
            option netbios-name-servers 192.168.1.1;
            range 192.168.1.10 192.168.1.100;
            default-lease-time 21600;
            max-lease-time 43200;
            #default-lease-time 19353600;
            #max-lease-time 43200;
            #max-lease-time 1814400; # 3 semanas
            #max-lease-time 29030400;
            #max-lease-time 58060800;
            }
   host financiero1 { #Reserva para un equipo del área financiera.
             option host-name "financiero1.cacpe.local";
             hardware ethernet  44:87:FC:EF:6F:83;
             fixed-address 192.168.1.143;
   }
}
```

ANEXO 6: CONFIGURACIÓN DE FIREWALL

```
#Breve detalle del contenido del script.
IPT="/sbin/iptables"
ROUTE="/sbin/route"
$ROUTE del -net 0.0.0.0/32 2>/dev/null
$ROUTE add -net 0.0.0.0/32 gw 181.39.42.161 2>/dev/null
$IPT -F FORWARD
$IPT -F
$IPT -X
$IPT -Z
$IPT -t nat -F
$IPT -t nat -X
$IPT -t nat -Z
$IPT -t mangle -F
$IPT -t mangle -X
INTEXT="enp2s0"
INTLAN="enp5s0"
REDLAN="192.168.0.0/16"
echo 1 > /proc/sys/net/ipv4/ip_forward
$IPT -A INPUT   -p icmp --icmp-type any -j ACCEPT
$IPT -A OUTPUT  -p icmp --icmp-type any -j ACCEPT
$IPT -A FORWARD -p icmp --icmp-type any -j ACCEPT
$IPT -P INPUT ACCEPT
$IPT -P OUTPUT ACCEPT
$IPT -P FORWARD ACCEPT
$IPT -t nat -P PREROUTING ACCEPT
$IPT -t nat -P POSTROUTING ACCEPT

$IPT -t nat -A POSTROUTING -s 192.168.0.0/16 -o $INTEXT -j MASQUERADE
$IPT -A FORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT
#Proxy Transparente
echo -e "Habilitando el Proxy Transparente..."
#Squid
$IPT -t nat -A PREROUTING -i $INTLAN -p tcp --dport 80 -j REDIRECT --to-port 3128
$IPT -A INPUT -i $INTLAN -p tcp --dport 3128 -j ACCEPT
$IPT -A OUTPUT -o $INTEXT -p tcp --dport 80 -j ACCEPT
$IPT -A INPUT -i $INTEXT -p tcp --sport 80 -j ACCEPT
$IPT -A OUTPUT -o $INTLAN -p tcp --sport 80 -j ACCEPT
#Squid
$IPT -I INPUT -s 192.168.0.0/16 -p tcp --dport 3128 -j ACCEPT
$IPT -I INPUT -s 192.168.1.0/16 -p tcp --dport 3128 -j ACCEPT
```

ANEXO 7: CONFIGURACIÓN DE FILTRADO DE CONTENIDO

Dansguardian.conf

```
# DansGuardian config file for version 2.12.0.0
# **NOTE** as of version 2.7.5 most of the list files are now in dansguardianf1.conf
# Web Access Denied Reporting (does not affect logging)
#
# -1 = log, but do not block - Stealth mode
#  0 = just say 'Access Denied'
#  1 = report why but not what denied phrase
#  2 = report fully
#  3 = use HTML template file (accessdeniedaddress ignored) - recommended
#
reportinglevel = 3
# Language dir where languages are stored for internationalisation.
# The HTML template within this dir is only used when reportinglevel
# is set to 3. When used, DansGuardian will display the HTML file instead of
# using the perl cgi script.  This option is faster, cleaner
# and easier to customise the access denied page.
# The language file is used no matter what setting however.
#
languagedir = '/usr/share/dansguardian/languages'

# language to use from languagedir.
#language = 'ukenglish'
language = 'mxspanish'

# Logging Settings
#
# 0 = none  1 = just denied  2 = all text based  3 = all requests
loglevel = 2
# Log Exception Hits
# Log if an exception (user, ip, URL, phrase) is matched and so
# the page gets let through.  Can be useful for diagnosing
# why a site gets through the filter.
# 0 = never log exceptions
# 1 = log exceptions, but do not explicitly mark them as such
# 2 = always log & mark exceptions (default)
logexceptionhits = 2
# Log File Format
# 1 = DansGuardian format (space delimited)
# 2 = CSV-style format
# 3 = Squid Log File Format
# 4 = Tab delimited
logfileformat = 1
# truncate large items in log lines
# 0 = no truncating (default)
#maxlogitemlength = 0
# anonymize logs (blank out usernames & IPs)
#anonymizelogs = off
# Syslog logging
#
# Use syslog for access logging instead of logging to the file
# at the defined or built-in "loglocation"
#logsyslog = off
# Log file location
#
# Defines the log directory and filename.
#loglocation = '/var/log/dansguardian//access.log'
# Statistics log file location
#
# Defines the stat file directory and filename.
# Only used in conjunction with maxips > 0
# Once every 3 minutes, the current number of IPs in the cache, and the most
# that have been in the cache since the daemon was started, are written to this
# file. IPs persist in the cache for 7 days.
#statlocation = '/var/log/dansguardian//stats'
# Network Settings
#
# the IP that DansGuardian listens on.  If left blank DansGuardian will
```

```
# listen on all IPs.  That would include all NICs, loopback, modem, etc.
# Normally you would have your firewall protecting this, but if you want
# you can limit it to a certain IP. To bind to multiple interfaces,
# specify each IP on an individual filterip line.
# You can have the same IP twice so long as it has a different port.
filterip =
# the ports that DansGuardian listens to.  Specify one line per filterip
# line.  You can specify different authentication mechanisms per port but
# only if the mechanisms can co-exist (e.g. basic/proxy auth can't)
filterports = 8080
#filterports = 8081
# the ip of the proxy (default is the loopback - i.e. this server)
proxyip = 127.0.0.1
# the port DansGuardian connects to proxy on
proxyport = 3128
# Whether to retrieve the original destination IP in transparent proxy
# setups and check it against the domain pulled from the HTTP headers.
#
# Be aware that when visiting sites which use a certain type of round-robin
# DNS for load balancing, DG may mark requests as invalid unless DG gets
# exactly the same answers to its DNS requests as clients.  The chances of
# this happening can be increased if all clients and servers on the same LAN
# make use of a local, caching DNS server instead of using upstream DNS
# directly.
#
# See http://www.kb.cert.org/vuls/id/435052
# on (default) | off
#!! Not compiled !! originalip = on
# accessdeniedaddress is the address of your web server to which the cgi
# dansguardian reporting script was copied. Only used in reporting levels 1 and 2.
#
# This webserver must be either:
#  1. Non-proxied. Either a machine on the local network, or listed as an exception
#     in your browser's proxy configuration.
#  2. Added to the exceptionsitelist. Option 1 is preferable; this option is
#     only for users using both transparent proxying and a non-local server
#     to host this script.
#
# Individual filter groups can override this setting in their own configuration.
#
accessdeniedaddress = 'http://YOURSERVER.YOURDOMAIN/cgi-bin/dansguardian.pl'
# Non standard delimiter (only used with accessdeniedaddress)
# To help preserve the full banned URL, including parameters, the variables
# passed into the access denied CGI are separated using non-standard
# delimiters. This can be useful to ensure correct operation of the filter
# bypass modes. Parameters are split using "::" in place of "&", and "==" in
# place of "=".
# Default is enabled, but to go back to the standard mode, disable it.
nonstandarddelimiter = on
# Banned image replacement
# Images that are banned due to domain/url/etc reasons including those
# in the adverts blacklists can be replaced by an image.  This will,
# for example, hide images from advert sites and remove broken image
# icons from banned domains.
# on (default) | off
usecustombannedimage = on
custombannedimagefile = '/usr/share/dansguardian/transparent1x1.gif'
#Banned flash replacement
usecustombannedflash = on
custombannedflashfile = '/usr/share/dansguardian/blockedflash.swf'
# Filter groups options
# filtergroups sets the number of filter groups. A filter group is a set of content
# filtering options you can apply to a group of users.  The value must be 1 or more.
# DansGuardian will automatically look for dansguardianfN.conf where N is the filter
# group.  To assign users to groups use the filtergroupslist option.  All users default
# to filter group 1.  You must have some sort of authentication to be able to map users
# to a group.  The more filter groups the more copies of the lists will be in RAM so
# use as few as possible.
filtergroups = 1
filtergroupslist = '/etc/dansguardian/lists/filtergroupslist'
# Authentication files location
```

```
bannediplist = '/etc/dansguardian/lists/bannediplist'
exceptioniplist = '/etc/dansguardian/lists/exceptioniplist'
# Per-Room blocking definition directory
# A directory containing text files containing the room's name followed by IPs or ranges
# Think of it as bannediplist on crack
perroomblockingdirectory = '/etc/dansguardian/lists/bannedrooms/'
# Show weighted phrases found
# If enabled then the phrases found that made up the total which excedes
# the naughtyness limit will be logged and, if the reporting level is
# high enough, reported. on | off
showweightedfound = on
# Weighted phrase mode
# There are 3 possible modes of operation:
# 0 = off = do not use the weighted phrase feature.
# 1 = on, normal = normal weighted phrase operation.
# 2 = on, singular = each weighted phrase found only counts once on a page.
#
# IMPORTANT: Note that setting this to "0" turns off all features which
# extract phrases from page content, including banned & exception
# phrases (not just weighted), search term filtering, and scanning for
# links to banned URLs.
#
weightedphrasemode = 2
# Positive (clean) result caching for URLs
# Caches good pages so they don't need to be scanned again.
# It also works with AV plugins.
# 0 = off (recommended for ISPs with users with disimilar browsing)
# 1000 = recommended for most users
# 5000 = suggested max upper limit
# If you're using an AV plugin then use at least 5000.
urlcachenumber = 1000
#
# Age before they are stale and should be ignored in seconds
# 0 = never
# 900 = recommended = 15 mins
urlcacheage = 900
# Cache for content (AV) scan results as 'clean'
# By default, to save CPU, files scanned and found to be
# clean are inserted into the clean cache and NOT scanned
# again for a while.  If you don't like this then choose
# to disable it.
# on = cache results; do not re-scan
# off = do not cache; always re-scan
# (on|off) default = on.
scancleancache = on
# Smart, Raw and Meta/Title phrase content filtering options
# Smart is where the multiple spaces and HTML are removed before phrase filtering
# Raw is where the raw HTML including meta tags are phrase filtered
# Meta/Title is where only meta and title tags are phrase filtered (v. quick)
# CPU usage can be effectively halved by using setting 0 or 1 compared to 2
# 0 = raw only
# 1 = smart only
# 2 = both of the above (default)
# 3 = meta/title
phrasefiltermode = 2
# Lower casing options
# When a document is scanned the uppercase letters are converted to lower case
# in order to compare them with the phrases.  However this can break Big5 and
# other 16-bit texts.  If needed preserve the case.  As of version 2.7.0 accented
# characters are supported.
# 0 = force lower case (default)
# 1 = do not change case
# 2 = scan first in lower case, then in original case
preservecase = 0
# Note:
# If phrasefiltermode and preserve case are both 2, this equates to 4 phrase
# filtering passes. If you have a large enough userbase for this to be a
# worry, and need to filter pages in exotic character encodings, it may be
# better to run two instances on separate servers: one with preservecase 1
# (and possibly forcequicksearch 1) and non ASCII/UTF-8 phrase lists, and one
# with preservecase 0 and ASCII/UTF-8 lists.
```

```
# Hex decoding options
# When a document is scanned it can optionally convert %XX to chars.
# If you find documents are getting past the phrase filtering due to encoding
# then enable.  However this can break Big5 and other 16-bit texts.
# off = disabled (default)
# on = enabled
hexdecodecontent = off
# Force Quick Search rather than DFA search algorithm
# The current DFA implementation is not totally 16-bit character compatible
# but is used by default as it handles large phrase lists much faster.
# If you wish to use a large number of 16-bit character phrases then
# enable this option.
# off (default) | on (Big5 compatible)
forcequicksearch = off
# Reverse lookups for banned site and URLs.
# If set to on, DansGuardian will look up the forward DNS for an IP URL
# address and search for both in the banned site and URL lists.  This would
# prevent a user from simply entering the IP for a banned address.
# It will reduce searching speed somewhat so unless you have a local caching
# DNS server, leave it off and use the Blanket IP Block option in the
# bannedsitelist file instead.
reverseaddresslookups = off
# Reverse lookups for banned and exception IP lists.
# If set to on, DansGuardian will look up the forward DNS for the IP
# of the connecting computer.  This means you can put in hostnames in
# the exceptioniplist and bannediplist.
# If a client computer is matched against an IP given in the lists, then the
# IP will be recorded in any log entries; if forward DNS is successful and a
# match occurs against a hostname, the hostname will be logged instead.
# It will reduce searching speed somewhat so unless you have a local DNS server,
# leave it off.
reverseclientiplookups = off
# Perform reverse lookups on client IPs for successful requests.
# If set to on, DansGuardian will look up the forward DNS for the IP
# of the connecting computer, and log host names (where available) rather than
# IPs against requests.
# This is not dependent on reverseclientiplookups being enabled; however, if it
# is, enabling this option does not incur any additional forward DNS requests.
logclienthostnames = off
# Build bannedsitelist and bannedurllist cache files.
# This will compare the date stamp of the list file with the date stamp of
# the cache file and will recreate as needed.
# If a .processed file exists for an item (e.g. domain/URL) list, then that
# will be used instead, if it is up to date (i.e. newer than the unprocessed
# list file).
# This can increase process start speed on slow computers.
# Fast computers do not need this option.
# on | off, default = on
createlistcachefiles = on
# Prefer cached list files
# If enabled, DansGuardian will always prefer to load ".processed" versions of
# list files, regardless of their time stamps relative to the original
# unprocessed lists.  This is not generally useful unless you have a specific
# list update process which results in - for example - up-to-date, pre-sorted
# ".processed" list files with dummy unprocessed files.
# on | off, default = off
prefercachedlists = off
# POST protection (web upload and forms)
# does not block forms without any file upload, i.e. this is just for
# blocking or limiting uploads
# measured in kibibytes after MIME encoding and header bumph
# use 0 for a complete block
# use higher (e.g. 512 = 512Kbytes) for limiting
# use -1 for no blocking
#maxuploadsize = 512
#maxuploadsize = 0
maxuploadsize = -1
# Max content filter size
# Sometimes web servers label binary files as text which can be very
# large which causes a huge drain on memory and cpu resources.
# To counter this, you can limit the size of the document to be
```

```
# filtered and get it to just pass it straight through.
# This setting also applies to content regular expression modification.
# The value must not be higher than maxcontentramcachescansize
# The size is in Kibibytes - eg 2048 = 2Mb
# use 0 to set it to maxcontentramcachescansize
maxcontentfiltersize = 256
# Max content ram cache scan size
# This is only used if you use a content scanner plugin such as AV
# This is the max size of file that DG will download and cache
# in RAM.  After this limit is reached it will cache to disk
# This value must be less than or equal to maxcontentfilecachescansize.
# The size is in Kibibytes - eg 10240 = 10Mb
# use 0 to set it to maxcontentfilecachescansize
# This option may be ignored by the configured download manager.
maxcontentramcachescansize = 2000
# Max content file cache scan size
# This is only used if you use a content scanner plugin such as AV
# This is the max size file that DG will download
# so that it can be scanned or virus checked.
# This value must be greater or equal to maxcontentramcachescansize.
# The size is in Kibibytes - eg 10240 = 10Mb
maxcontentfilecachescansize = 20000
# Proxy timeout
# Set timeout between the Proxy and DansGuardian
# Min 20 - Max 30
proxytimeout = 20


# File cache dir
# Where DG will download files to be scanned if too large for the
# RAM cache.
filecachedir = '/tmp'
# Delete file cache after user completes download
# When a file gets save to temp it stays there until it is deleted.
# You can choose to have the file deleted when the user makes a sucessful
# download.  This will mean if they click on the link to download from
# the temp store a second time it will give a 404 error.
# You should configure something to delete old files in temp to stop it filling up.
# on|off (defaults to on)
deletedownloadedtempfiles = on
# Initial Trickle delay
# This is the number of seconds a browser connection is left waiting
# before first being sent *something* to keep it alive.  The
# *something* depends on the download manager chosen.
# Do not choose a value too low or normal web pages will be affected.
# A value between 20 and 110 would be sensible
# This may be ignored by the configured download manager.
initialtrickledelay = 20
# Trickle delay
# This is the number of seconds a browser connection is left waiting
# before being sent more *something* to keep it alive.  The
# *something* depends on the download manager chosen.
# This may be ignored by the configured download manager.
trickledelay = 10



# Download Managers
# These handle downloads of files to be filtered and scanned.
# They differ in the method they deal with large downloads.
# Files usually need to be downloaded 100% before they can be
# filtered and scanned before being sent on to the browser.
# Normally the browser can just wait, but with content scanning,
# for example to AV, the browser may timeout or the user may get
# confused so the download manager has to do some sort of
# 'keep alive'.
#
# There are various methods possible but not all are included.
# The author does not have the time to write them all so I have
# included a plugin systam.  Also, not all methods work with all
# browsers and clients.  Specifically some fancy methods don't
```

```
# work with software that downloads updates.  To solve this,
# each plugin can support a regular expression for matching
# the client's user-agent string, and lists of the mime types
# and extensions it should manage.
#
# Note that these are the matching methods provided by the base plugin
# code, and individual plugins may override or add to them.
# See the individual plugin conf files for supported options.
#
# The plugins are matched in the order you specify and the last
# one is forced to match as the default, regardless of user agent
# and other matching mechanisms.
#
downloadmanager = '/etc/dansguardian/downloadmanagers/fancy.conf'
#downloadmanager = '/etc/dansguardian/downloadmanagers/trickle.conf'
downloadmanager = '/etc/dansguardian/downloadmanagers/default.conf'
# Content Scanners (Also known as AV scanners)
# These are plugins that scan the content of all files your browser fetches
# for example to AV scan.  The options are limitless.  Eventually all of
# DansGuardian will be plugin based.  You can have more than one content
# scanner. The plugins are run in the order you specify.
# This is one of the few places you can have multiple options of the same name.
#
# Some of the scanner(s) require 3rd party software and libraries eg clamav.
# See the individual plugin conf file for more options (if any).
#
#contentscanner = '/etc/dansguardian/contentscanners/clamdscan.conf'
#!! Not compiled !! contentscanner = '/etc/dansguardian/contentscanners/avastdscan.conf'
#!! Not compiled !! contentscanner = '/etc/dansguardian/contentscanners/kavdscan.conf'
#contentscanner = '/etc/dansguardian/contentscanners/icapscan.conf'
#contentscanner = '/etc/dansguardian/contentscanners/commandlinescan.conf'



# Content scanner timeout
# Some of the content scanners support using a timeout value to stop
# processing (eg AV scanning) the file if it takes too long.
# If supported this will be used.
# The default of 60 seconds is probably reasonable.
contentscannertimeout = 60
# Content scan exceptions
# If 'on' exception sites, urls, users etc will be scanned
# This is probably not desirable behavour as exceptions are
# supposed to be trusted and will increase load.
# Correct use of grey lists are a better idea.
# (on|off) default = off
contentscanexceptions = off
# Auth plugins
# These replace the usernameidmethod* options in previous versions. They
# handle the extraction of client usernames from various sources, such as
# Proxy-Authorisation headers and ident servers, enabling requests to be
# handled according to the settings of the user's filter group.
# Multiple plugins can be specified, and will be used per port in the order
# filterports are listed.
#
# If you do not use multiple filter groups, you need not specify this option.
#
#authplugin = '/etc/dansguardian/authplugins/proxy-basic.conf'
#authplugin = '/etc/dansguardian/authplugins/proxy-digest.conf'
#authplugin = '/etc/dansguardian/authplugins/proxy-ntlm.conf'
#authplugin = '/etc/dansguardian/authplugins/ident.conf'
#authplugin = '/etc/dansguardian/authplugins/ip.conf'
# Re-check replaced URLs
# As a matter of course, URLs undergo regular expression search/replace (urlregexplist)
# *after* checking the exception site/URL/regexpURL lists, but *before* checking against
# the banned site/URL lists, allowing certain requests that would be matched against the
# latter in their original state to effectively be converted into grey requests.
# With this option enabled, the exception site/URL/regexpURL lists are also re-checked
# after replacement, making it possible for URL replacement to trigger exceptions based
# on them.
# Defaults to off.
```

```
recheckreplacedurls = off
# Misc settings
# if on it adds an X-Forwarded-For: <clientip> to the HTTP request
# header.  This may help solve some problem sites that need to know the
# source ip. on | off
forwardedfor = off
# if on it uses the X-Forwarded-For: <clientip> to determine the client
# IP. This is for when you have squid between the clients and DansGuardian.
# Warning - headers are easily spoofed. on | off
usexforwardedfor = off
# if on it logs some debug info regarding fork()ing and accept()ing which
# can usually be ignored.  These are logged by syslog.  It is safe to leave
# it on or off
logconnectionhandlingerrors = on
# Fork pool options
# If on, this causes DG to write to the log file whenever child processes are
# created or destroyed (other than by crashes). This information can help in
# understanding and tuning the following parameters, but is not generally
# useful in production.
logchildprocesshandling = off
# sets the maximum number of processes to spawn to handle the incoming
# connections.  Max value usually 250 depending on OS.
# On large sites you might want to try 180.
maxchildren = 120
# sets the minimum number of processes to spawn to handle the incoming connections.
# On large sites you might want to try 32.
minchildren = 8
# sets the minimum number of processes to be kept ready to handle connections.
# On large sites you might want to try 8.
minsparechildren = 4
# sets the minimum number of processes to spawn when it runs out
# On large sites you might want to try 10.
preforkchildren = 6
# sets the maximum number of processes to have doing nothing.
# When this many are spare it will cull some of them.
# On large sites you might want to try 64.
maxsparechildren = 32


# sets the maximum age of a child process before it croaks it.
# This is the number of connections they handle before exiting.
# On large sites you might want to try 10000.
maxagechildren = 500
# Sets the maximum number client IP addresses allowed to connect at once.
# Use this to set a hard limit on the number of users allowed to concurrently
# browse the web. Set to 0 for no limit, and to disable the IP cache process.
maxips = 0
# Process options
# (Change these only if you really know what you are doing).
# These options allow you to run multiple instances of DansGuardian on a single machine.
# Remember to edit the log file path above also if that is your intention.

# IPC filename
#
# Defines IPC server directory and filename used to communicate with the log process.
ipcfilename = '/tmp/.dguardianipc'

# URL list IPC filename
#
# Defines URL list IPC server directory and filename used to communicate with the URL
# cache process.
urlipcfilename = '/tmp/.dguardianurlipc'

# IP list IPC filename
#
# Defines IP list IPC server directory and filename, for communicating with the client
# IP cache process.
ipipcfilename = '/tmp/.dguardianipipc'

# PID filename
#
```

```
# Defines process id directory and filename.
#pidfilename = '/var/run//dansguardian.pid'
# Disable daemoning
# If enabled the process will not fork into the background.
# It is not usually advantageous to do this.
# on|off (defaults to off)
nodaemon = off
# Disable logging process
# on|off (defaults to off)
nologger = off
# Enable logging of "ADs" category blocks
# on|off (defaults to off)
logadblocks = off
# Enable logging of client User-Agent
# Some browsers will cause a *lot* of extra information on each line!
# on|off (defaults to off)
loguseragent = off
# Daemon runas user and group
# This is the user that DansGuardian runs as.  Normally the user/group nobody.
# Uncomment to use.  Defaults to the user set at compile time.
# Temp files created during virus scanning are given owner and group read
# permissions; to use content scanners based on external processes, such as
# clamdscan, the two processes must run with either the same group or user ID.
#daemonuser = 'dansguardian'
#daemongroup = 'vscan'
# Soft restart
# When on this disables the forced killing off all processes in the process group.
# This is not to be confused with the -g run time option - they are not related.
# on|off (defaults to off)
softrestart = off
# Mail program
# Path (sendmail-compatible) email program, with options.
# Not used if usesmtp is disabled (filtergroup specific).
mailer = '/usr/sbin/sendmail -t'
#SSL certificate checking path
#Path to CA certificates used to validate the certificates of https sites.
#sslcertificatepath = '/etc/ssl/certs/'
#SSL man in the middle
#CA certificate path
#Path to the CA certificate to use as a signing certificate for
#generated certificates.
#cacertificatepath = '/home/stephen/dginstall/ca.pem'
#CA private key path
#path to the private key that matches the public key in the CA certificate.
#caprivatekeypath = '/home/stephen/dginstall/ca.key'

#Cert private key path
#The public / private key pair used by all generated certificates
#certprivatekeypath = '/home/stephen/dginstall/cert.key'
#Generated cert path
#The location where generated certificates will be saved for future use.
#(must be writable by the dg user)
#generatedcertpath = '/home/stephen/dginstall/generatedcerts/'
#Generated link path = ''
#The location where symlinks to certificates will be created.
#(must be writable by the dg user)
#generatedlinkpath = '/home/stephen/dginstall/generatedlinks/'
```

Dansguardian1.conf

```
# DansGuardian filter group config file for version 2.12.0.0
# Filter group mode
# This option determines whether members of this group have their web access
# unfiltered, filtered, or banned. This mechanism replaces the "banneduserlist"
# and "exceptionuserlist" files from previous versions.
#
# 0 = banned
# 1 = filtered
# 2 = unfiltered (exception)
#
# Only filter groups with a mode of 1 need to define phrase, URL, site, extension,
# mimetype and PICS lists; in other modes, these options are ignored to conserve
# memory.
```

```
#
# Defaults to 0 if unspecified.
# Unauthenticated users are treated as being in the first filter group.
groupmode = 1
# Filter group name
# Used to fill in the -FILTERGROUP- placeholder in the HTML template file, and to
# name the group in the access logs
# Defaults to empty string
#groupname = ''
# Content filtering files location
bannedphraselist = '/etc/dansguardian/lists/bannedphraselist'
weightedphraselist = '/etc/dansguardian/lists/weightedphraselist'
exceptionphraselist = '/etc/dansguardian/lists/exceptionphraselist'
bannedsitelist = '/etc/dansguardian/lists/bannedsitelist'
greysitelist = '/etc/dansguardian/lists/greysitelist'
exceptionsitelist = '/etc/dansguardian/lists/exceptionsitelist'
bannedurllist = '/etc/dansguardian/lists/bannedurllist'
greyurllist = '/etc/dansguardian/lists/greyurllist'
exceptionurllist = '/etc/dansguardian/lists/exceptionurllist'
exceptionregexpurllist = '/etc/dansguardian/lists/exceptionregexpurllist'
bannedregexpurllist = '/etc/dansguardian/lists/bannedregexpurllist'
picsfile = '/etc/dansguardian/lists/pics'
contentregexplist = '/etc/dansguardian/lists/contentregexplist'
urlregexplist = '/etc/dansguardian/lists/urlregexplist'

# Filetype filtering
#
# Blanket download blocking
# If enabled, all files will be blocked, unless they match the
# exceptionextensionlist or exceptionmimetypelist.
# These lists do not override virus scanning.
# Exception lists defined above override all types of filtering, including
# the blanket download block.
# Defaults to disabled.
# (on | off)
#
blockdownloads = off
exceptionextensionlist = '/etc/dansguardian/lists/exceptionextensionlist'
exceptionmimetypelist = '/etc/dansguardian/lists/exceptionmimetypelist'
#
# Use the following lists to block specific kinds of file downloads.
# The two exception lists above can be used to override these.
#
bannedextensionlist = '/etc/dansguardian/lists/bannedextensionlist'
bannedmimetypelist = '/etc/dansguardian/lists/bannedmimetypelist'
#
# In either file filtering mode, the following list can be used to override
# MIME type & extension blocks for particular domains & URLs (trusted download sites).
#
exceptionfilesitelist = '/etc/dansguardian/lists/exceptionfilesitelist'
exceptionfileurllist = '/etc/dansguardian/lists/exceptionfileurllist'

# Categorise without blocking:
# Supply categorised lists here and the category string shall be logged against
# matching requests, but matching these lists does not perform any filtering
# action.
#logsitelist = '/etc/dansguardian/lists/logsitelist'
#logurllist = '/etc/dansguardian/lists/logurllist'
#logregexpurllist = '/etc/dansguardian/lists/logregexpurllist'

# Outgoing HTTP header rules:
# Optional lists for blocking based on, and modification of, outgoing HTTP
# request headers.  Format for headerregexplist is one modification rule per
# line, similar to content/URL modifications.  Format for
# bannedregexpheaderlist is one regular expression per line, with matching
# headers causing a request to be blocked.
# Headers are matched/replaced on a line-by-line basis, not as a contiguous
# block.
# Use for example, to remove cookies or prevent certain user-agents.
headerregexplist = '/etc/dansguardian/lists/headerregexplist'
bannedregexpheaderlist = '/etc/dansguardian/lists/bannedregexpheaderlist'
```

```
# Weighted phrase mode
# Optional; overrides the weightedphrasemode option in dansguardian.conf
# for this particular group.  See documentation for supported values in
# that file.
#weightedphrasemode = 0

# Naughtiness limit
# This the limit over which the page will be blocked.  Each weighted phrase is given
# a value either positive or negative and the values added up.  Phrases to do with
# good subjects will have negative values, and bad subjects will have positive
# values.  See the weightedphraselist file for examples.
# As a guide:
# 50 is for young children,  100 for old children,  160 for young adults.
naughtynesslimit = 50

# Search term blocking
# Search terms can be extracted from search URLs and filtered using the
# bannedphraselist, weightedphraselist and exceptionphraselist, with a separate
# threshold for blocking than that used for normal page content.
# To do this, the first two options below must be enabled.
#
# Search engine regular expression list
# List of regular expressions for matching search engine URLs.  It is assumed
# that the search terms themselves will be contained within the first submatch
# of each expression.
#searchengineregexplist = '/etc/dansguardian/lists/searchengineregexplist'
#
# Search term limit
# The limit over which requests will be blocked for containing search terms
# which match the weightedphraselist.  This should usually be lower than the
# 'naughtynesslimit' value above, because the amount of text being filtered
# is only a few words, rather than a whole page.
# This option must be uncommented if searchengineregexplist is uncommented.
# A value of 0 here indicates that search terms should be extracted,
# for logging/reporting purposes, but no filtering should be performed
# on the resulting text.
#searchtermlimit = 30
#
# Search term lists
# If the three lines below are uncommented, search term blocking will use
# the banned, weighted & exception phrases from these lists, instead of using
# the same phrase lists as for page content.  This is optional but recommended,
# as weights for individual phrases in the "normal" lists may not be
# appropriate for blocking when those phrases appear in a much smaller block
# of text.
# Please note that all or none of the below should be uncommented, not a
# mixture.
#bannedsearchtermlist = '/etc/dansguardian/lists/bannedsearchtermlist'
#weightedsearchtermlist = '/etc/dansguardian/lists/weightedsearchtermlist'
#exceptionsearchtermlist = '/etc/dansguardian/lists/exceptionsearchtermlist'

# Category display threshold
# This option only applies to pages blocked by weighted phrase filtering.
# Defines the minimum score that must be accumulated within a particular
# category in order for it to show up on the block pages' category list.
# All categories under which the page scores positively will be logged; those
# that were not displayed to the user appear in brackets.
#
# -1 = display only the highest scoring category
# 0 = display all categories (default)
# > 0 = minimum score for a category to be displayed
categorydisplaythreshold = 0

# Embedded URL weighting
# When set to something greater than zero, this option causes URLs embedded within a
# page's HTML (from links, image tags, etc.) to be extracted and checked against the
# bannedsitelist and bannedurllist. Each link to a banned page causes the amount set
# here to be added to the page's weighting.
# The behaviour of this option with regards to multiple occurrences of a site/URL is
# affected by the weightedphrasemode setting.
```

```
#
# NB: Currently, this feature uses regular expressions that require the PCRE library.
# As such, it is only available if you compiled DansGuardian with '--enable-pcre=yes'.
# You can check compile-time options by running 'dansguardian -v'.
#
# Set to 0 to disable.
# Defaults to 0.
# WARNING: This option is highly CPU intensive!
embeddedurlweight = 0

# Enable PICS rating support
#
# Defaults to disabled
# (on | off)
enablepics = off

# Temporary Denied Page Bypass
# This provides a link on the denied page to bypass the ban for a few minutes.  To be
# secure it uses a random hashed secret generated at daemon startup.  You define the
# number of seconds the bypass will function for before the deny will appear again.
# To allow the link on the denied page to appear you will need to edit the template.html
# or dansguardian.pl file for your language.
# 300 = enable for 5 minutes
# 0 = disable ( defaults to 0 )
# -1 = enable but you require a separate program/CGI to generate a valid link
bypass = 0

# Temporary Denied Page Bypass Secret Key
# Rather than generating a random key you can specify one.  It must be more than 8 chars.
# '' = generate a random one (recommended and default)
# 'Mary had a little lamb.' = an example
# '76b42abc1cd0fdcaf6e943dcbc93b826' = an example
bypasskey = ''

# Infection/Scan Error Bypass
# Similar to the 'bypass' setting, but specifically for bypassing files scanned and found
# to be infected, or files that trigger scanner errors - for example, archive types with
# recognised but unsupported compression schemes, or corrupt archives.
# The option specifies the number of seconds for which the bypass link will be valid.
# 300 = enable for 5 minutes
# 0 = disable (default)
# -1 = enable, but require a separate program/CGI to generate a valid link
infectionbypass = 0

# Infection/Scan Error Bypass Secret Key
# Same as the 'bypasskey' option, but used for infection bypass mode.
infectionbypasskey = ''

# Infection/Scan Error Bypass on Scan Errors Only
# Enable this option to allow infectionbypass links only when virus scanning fails,
# not when a file is found to contain a virus.
# on = enable (default and highly recommended)
# off = disable
infectionbypasserrorsonly = on

# Disable content scanning
# If you enable this option you will disable content scanning for this group.
# Content scanning primarily is AV scanning (if enabled) but could include
# other types.
# (on|off) default = off.
disablecontentscan = off

# Enable Deep URL Analysis
# When enabled, DG looks for URLs within URLs, checking against the bannedsitelist and
# bannedurllist. This can be used, for example, to block images originating from banned
# sites from appearing in Google Images search results, as the original URLs are
# embedded in the thumbnail GET requests.
# (on|off) default = off
deepurlanalysis = off

# reportinglevel
```

```
#
# -1 = log, but do not block - Stealth mode
#  0 = just say 'Access Denied'
#  1 = report why but not what denied phrase
#  2 = report fully
#  3 = use HTML template file (accessdeniedaddress ignored) - recommended
#
# If defined, this overrides the global setting in dansguardian.conf for
# members of this filter group.
#
#reportinglevel = 3

# accessdeniedaddress is the address of your web server to which the cgi
# dansguardian reporting script was copied. Only used in reporting levels
# 1 and 2.
#
# This webserver must be either:
#  1. Non-proxied. Either a machine on the local network, or listed as an
#     exception in your browser's proxy configuration.
#  2. Added to the exceptionsitelist. Option 1 is preferable; this option is
#     only for users using both transparent proxying and a non-local server
#     to host this script.
#
# If defined, this overrides the global setting in dansguardian.conf for
# members of this filter group.
#
#accessdeniedaddress = 'http://YOURSERVER.YOURDOMAIN/cgi-bin/dansguardian.pl'

# HTML Template override
# If defined, this specifies a custom HTML template file for members of this
# filter group, overriding the global setting in dansguardian.conf. This is
# only used in reporting level 3.
#
# The default template file path is <languagedir>/<language>/template.html
# e.g. /usr/share/dansguardian/languages/ukenglish/template.html when using 'ukenglish'
# language.
#
# This option generates a file path of the form:
# <languagedir>/<language>/<htmltemplate>
# e.g. /usr/share/dansguardian/languages/ukenglish/custom.html
#
#htmltemplate = 'custom.html'

# Email reporting - original patch by J. Gauthier

# Use SMTP
# If on, will enable system wide events to be reported by email.
# need to configure mail program (see 'mailer' in global config)
# and email recipients
# default usesmtp = off
usesmtp = off

# mailfrom
# who the email would come from
# example: mailfrom = 'dansguardian@mycompany.com'
mailfrom = ''

# avadmin
# who the virus emails go to (if notify av is on)
# example: avadmin = 'admin@mycompany.com'
avadmin = ''

# contentdmin
# who the content emails go to (when thresholds are exceeded)
# and contentnotify is on
# example: contentadmin = 'admin@mycompany.com'
contentadmin = ''

# avsubject
# Subject of the email sent when a virus is caught.
# only applicable if notifyav is on
```

```
# default avsubject = 'dansguardian virus block'
avsubject = 'dansguardian virus block'

# content
# Subject of the email sent when violation thresholds are exceeded
# default contentsubject = 'dansguardian violation'
contentsubject = 'dansguardian violation'

# notifyAV
# This will send a notification, if usesmtp/notifyav is on, any time an
# infection is found.
# Important: If this option is off, viruses will still be recorded like a
# content infraction.
notifyav = off

# notifycontent
# This will send a notification, if usesmtp is on, based on thresholds
# below
notifycontent = off

# thresholdbyuser
# results are only predictable with user authenticated configs
# if enabled the violation/threshold count is kept track of by the user
thresholdbyuser = off

#violations
# number of violations before notification
# setting to 0 will never trigger a notification
violations = 0

#threshold
# this is in seconds. If 'violations' occur in 'threshold' seconds, then
# a notification is made.
# if this is set to 0, then whenever the set number of violations are made a
# notifaction will be sent.
threshold = 0

#SSL certificate checking
# Check that ssl certificates for servers on https connections are valid
# and signed by a ca in the configured path
sslcertcheck = off

#SSL man in the middle
# Forge ssl certificates for all sites, decrypt the data then re encrypt it
# using a different private key. Used to filter ssl sites
sslmitm = off
```

ANEXO 8: ENCUESTA NIVEL SATISFACCIÓN DE USO DE SOFTWARE LIBRE

UNIVERSIDAD TÉCNICA PARTICULAR DE LOJA

Encuesta sobre la Implementación de Software Libre

Encuestado: Victor Andrade **Fecha:** 28 / Noviembre / 2016

1.- ¿Conoce usted qué es software libre?

Sí ☑ No ☐

2.- ¿Tiene conocimiento del Sistema Operativo GNU/Linux o experiencia en el uso del mismo?

Ninguno ☐ Poco ☐ Medio ☑ Bastante ☐

3.- ¿De ser afirmativa la segunda pregunta, sabe que distribución GNU/Linux utiliza para sus aplicaciones?

Sí ☐ No ☑

4.- ¿Sabía Usted que el trabajo de desarrollar Software Libre, es apoyado de forma comunitaria (comunidades de informáticos alrededor del mundo sin fines de lucro, para beneficio de los usuarios)?

Sí ☑ No ☐

5.- ¿Ha escuchado hablar sobre las aplicaciones de software Libre Office que son equivalente a las aplicaciones de Office con licencia de Windows?

Ninguno ☐ Poco ☐ Medio ☑ Bastante ☐

6.- ¿La capacitación del uso del software Libre en el plan piloto iniciado en la Cooperativa le ayudo en sus tareas diarias?

Sí ☑ No ☐

7.- ¿Para la aplicación del Plan Piloto se utilizó el sistema operativo Fedora, tenía conocimiento de este sistema de software libre?

Sí ☐ No ☑

8.- ¿Cuál es su nivel de conocimiento, entendimiento en el uso de las aplicaciones Libre Office?

Ninguno ☑ Poco ☐ Medio ☐ Bastante ☐

9.- ¿Cuál es su nivel de conocimiento, entendimiento en el uso del Gestor de Archivos?

Ninguno ☐ Poco ☑ Medio ☐ Bastante ☐

10.- ¿Se adaptó a la interfaz del sistema operativo Fedora y sus aplicativos en relación a lo experimentado en el Sistema operativo Windows?

Sí ☑ No ☐

11.- ¿El uso de software libre le beneficio para la optimización de recursos en la Cooperativa?

Sí ☑ No ☐

12.- ¿En base a la capacitación, desenvolvimiento obtenido recomendaría el uso de software libre a usuarios que utilizan software con licencia?

Sí ☑ No ☐

13.- ¿Cree usted que sería factible aplicar el uso de software libre en todas las estaciones de la Cooperativa?

Sí ☑ No ☐

Encuestado

Encuestador

UNIVERSIDAD TÉCNICA PARTICULAR DE LOJA

Encuesta sobre la Implementación de Software Libre

Encuestado: Joao Velez **Fecha:** 28/Noviembre/2016

1.- ¿Conoce usted qué es software libre?

Sí ☑ No ☐

2.- ¿Tiene conocimiento del Sistema Operativo GNU/Linux o experiencia en el uso del mismo?

Ninguno ☐ Poco ☑ Medio ☐ Bastante ☐

3.- ¿De ser afirmativa la segunda pregunta, sabe que distribución GNU/Linux utiliza para sus aplicaciones?

Sí ☑ No ☐

4.- ¿Sabía Usted que el trabajo de desarrollar Software Libre, es apoyado de forma comunitaria (comunidades de informáticos alrededor del mundo sin fines de lucro, para beneficio de los usuarios)?

Sí ☑ No ☐

5.- ¿Ha escuchado hablar sobre las aplicaciones de software Libre Office que son equivalente a las aplicaciones de Office con licencia de Windows?

Ninguno ☐ Poco ☑ Medio ☐ Bastante ☐

6.- ¿La capacitación del uso del software Libre en el plan piloto iniciado en la Cooperativa le ayudo en sus tareas diarias?

Sí ☑ No ☐

7.- ¿Para la aplicación del Plan Piloto se utilizó el sistema operativo Fedora, tenía conocimiento de este sistema de software libre?

Sí ☑ No ☐

8.- ¿Cuál es su nivel de conocimiento, entendimiento en el uso de las aplicaciones Libre Office?

Ninguno ☐ Poco ☐ Medio ☑ Bastante ☐

9.- ¿Cuál es su nivel de conocimiento, entendimiento en el uso del Gestor de Archivos?

Ninguno ☐ Poco ☑ Medio ☐ Bastante ☐

10.- ¿Se adaptó a la interfaz del sistema operativo Fedora y sus aplicativos en relación a lo experimentado en el Sistema operativo Windows?

Sí ☑ No ☐

11.- ¿El uso de software libre le beneficio para la optimización de recursos en la Cooperativa?

Sí ☑ No ☐

12.- ¿En base a la capacitación, desenvolvimiento obtenido recomendaría el uso de software libre a usuarios que utilizan software con licencia?

Sí ☑ No ☐

13.- ¿Cree usted que sería factible aplicar el uso de software libre en todas las estaciones de la Cooperativa?

Sí ☑ **No** ☐

Encuestado **Encuestador**

UNIVERSIDAD TÉCNICA PARTICULAR DE LOJA

Encuesta sobre la Implementación de Software Libre

Encuestado: Nohemi Zambrano **Fecha:** 28/Noviembre/2016

1.- ¿Conoce usted qué es software libre?

Sí ☑ No ☐

2.- ¿Tiene conocimiento del Sistema Operativo GNU/Linux o experiencia en el uso del mismo?

Ninguno ☐ Poco ☐ Medio ☑ Bastante ☐

3.- ¿De ser afirmativa la segunda pregunta, sabe que distribución GNU/Linux utiliza para sus aplicaciones?

Sí ☑ No ☐

4.- ¿Sabía Usted que el trabajo de desarrollar Software Libre, es apoyado de forma comunitaria (comunidades de informáticos alrededor del mundo sin fines de lucro, para beneficio de los usuarios)?

Sí ☑ No ☐

5.- ¿Ha escuchado hablar sobre las aplicaciones de software Libre Office que son equivalente a las aplicaciones de Office con licencia de Windows?

Ninguno ☐ Poco ☐ Medio ☑ Bastante ☐

6.- ¿La capacitación del uso del software Libre en el plan piloto iniciado en la Cooperativa le ayudo en sus tareas diarias?

Sí ☑ No ☐

7.- ¿Para la aplicación del Plan Piloto se utilizó el sistema operativo Fedora, tenía conocimiento de este sistema de software libre?

Sí ☑ No ☐

8.- ¿Cuál es su nivel de conocimiento, entendimiento en el uso de las aplicaciones Libre Office?

Ninguno ☐ Poco ☐ Medio ☑ Bastante ☐

9.- ¿Cuál es su nivel de conocimiento, entendimiento en el uso del Gestor de Archivos?

Ninguno ☐ Poco ☐ Medio ☑ Bastante ☐

10.- ¿Se adaptó a la interfaz del sistema operativo Fedora y sus aplicativos en relación a lo experimentado en el Sistema operativo Windows?

Sí ☑ No ☐

11.- ¿El uso de software libre le beneficio para la optimización de recursos en la Cooperativa?

Sí ☑ No ☐

12.- ¿En base a la capacitación, desenvolvimiento obtenido recomendaría el uso de software libre a usuarios que utilizan software con licencia?

Sí ☑ No ☐

13.- ¿Cree usted que sería factible aplicar el uso de software libre en todas las estaciones de la Cooperativa?

Sí ☑ **No** ☐

Encuestado **Encuestador**

UNIVERSIDAD TÉCNICA PARTICULAR DE LOJA

Encuesta sobre la Implementación de Software Libre

Encuestado: Mariuxi Pastigua **Fecha:** 28/Noviembre/2016

1.- ¿Conoce usted qué es software libre?

Sí ☐ No ☒

2.- ¿Tiene conocimiento del Sistema Operativo GNU/Linux o experiencia en el uso del mismo?

Ninguno ☒ Poco ☐ Medio ☐ Bastante ☐

3.- ¿De ser afirmativa la segunda pregunta, sabe que distribución GNU/Linux utiliza para sus aplicaciones?

Sí ☐ No ☐

4.- ¿Sabía Usted que el trabajo de desarrollar Software Libre, es apoyado de forma comunitaria (comunidades de informáticos alrededor del mundo sin fines de lucro, para beneficio de los usuarios)?

Sí ☐ No ☒

5.- ¿Ha escuchado hablar sobre las aplicaciones de software Libre Office que son equivalente a las aplicaciones de Office con licencia de Windows?

Ninguno ☐ Poco ☒ Medio ☐ Bastante ☐

6.- ¿La capacitación del uso del software Libre en el plan piloto iniciado en la Cooperativa le ayudo en sus tareas diarias?

Sí ☒ No ☐

7.- ¿Para la aplicación del Plan Piloto se utilizó el sistema operativo Fedora, tenía conocimiento de este sistema de software libre?

Sí ☐ No ☒

8.- ¿Cuál es su nivel de conocimiento, entendimiento en el uso de las aplicaciones Libre Office?

Ninguno ☐ Poco ☒ Medio ☐ Bastante ☐

9.- ¿Cuál es su nivel de conocimiento, entendimiento en el uso del Gestor de Archivos?

Ninguno ☒ Poco ☐ Medio ☐ Bastante ☐

10.- ¿Se adaptó a la interfaz del sistema operativo Fedora y sus aplicativos en relación a lo experimentado en el Sistema operativo Windows?

Sí ☒ No ☐

11.- ¿El uso de software libre le beneficio para la optimización de recursos en la Cooperativa?

Sí ☒ No ☐

12.- ¿En base a la capacitación, desenvolvimiento obtenido recomendaría el uso de software libre a usuarios que utilizan software con licencia?

Sí ☒ No ☐

13.- ¿Cree usted que sería factible aplicar el uso de software libre en todas las estaciones de la Cooperativa?

Sí ☒ No ☐

Encuestado **Encuestador**

UNIVERSIDAD TÉCNICA PARTICULAR DE LOJA

Encuesta sobre la Implementación de Software Libre

Encuestado: Sergio Villalta **Fecha:** 28/Noviembre/2016

1.- ¿Conoce usted qué es software libre?

Sí ☐ No ☑

2.- ¿Tiene conocimiento del Sistema Operativo GNU/Linux o experiencia en el uso del mismo?

Ninguno ☑ Poco ☐ Medio ☐ Bastante ☐

3.- ¿De ser afirmativa la segunda pregunta, sabe que distribución GNU/Linux utiliza para sus aplicaciones?

Sí ☐ No ☐

4.- ¿Sabía Usted que el trabajo de desarrollar Software Libre, es apoyado de forma comunitaria (comunidades de informáticos alrededor del mundo sin fines de lucro, para beneficio de los usuarios)?

Sí ☐ No ☑

5.- ¿Ha escuchado hablar sobre las aplicaciones de software Libre Office que son equivalente a las aplicaciones de Office con licencia de Windows?

Ninguno ☐ Poco ☑ Medio ☐ Bastante ☐

6.- ¿La capacitación del uso del software Libre en el plan piloto iniciado en la Cooperativa le ayudo en sus tareas diarias?

Sí ☑ No ☐

7.- ¿Para la aplicación del Plan Piloto se utilizó el sistema operativo Fedora, tenía conocimiento de este sistema de software libre?

Sí ☐ No ☑

8.- ¿Cuál es su nivel de conocimiento, entendimiento en el uso de las aplicaciones Libre Office?

Ninguno ☐ Poco ☑ Medio ☐ Bastante ☐

9.- ¿Cuál es su nivel de conocimiento, entendimiento en el uso del Gestor de Archivos?

Ninguno ☐ Poco ☑ Medio ☐ Bastante ☐

10.- ¿Se adaptó a la interfaz del sistema operativo Fedora y sus aplicativos en relación a lo experimentado en el Sistema operativo Windows?

Sí ☑ No ☐

11.- ¿El uso de software libre le beneficio para la optimización de recursos en la Cooperativa?

Sí ☑ No ☐

12.- ¿En base a la capacitación, desenvolvimiento obtenido recomendaría el uso de software libre a usuarios que utilizan software con licencia?

Sí ☑ No ☐

13.- ¿Cree usted que sería factible aplicar el uso de software libre en todas las estaciones de la Cooperativa?

Sí ☑ No ☐

Encuestado

Encuestador

UNIVERSIDAD TÉCNICA PARTICULAR DE LOJA

Encuesta sobre la Implementación de Software Libre

Encuestado: Fabian Zambrano Fecha: 28/Noviembre/2016

1.- ¿Conoce usted qué es software libre?
Sí ☑ No ☐

2.- ¿Tiene conocimiento del Sistema Operativo GNU/Linux o experiencia en el uso del mismo?
Ninguno ☐ Poco ☐ Medio ☑ Bastante ☐

3.- ¿De ser afirmativa la segunda pregunta, sabe que distribución GNU/Linux utiliza para sus aplicaciones?
Sí ☑ No ☐

4.- ¿Sabía Usted que el trabajo de desarrollar Software Libre, es apoyado de forma comunitaria (comunidades de informáticos alrededor del mundo sin fines de lucro, para beneficio de los usuarios)?
Sí ☑ No ☐

5.- ¿Ha escuchado hablar sobre las aplicaciones de software Libre Office que son equivalente a las aplicaciones de Office con licencia de Windows?
Ninguno ☐ Poco ☐ Medio ☑ Bastante ☐

6.- ¿La capacitación del uso del software Libre en el plan piloto iniciado en la Cooperativa le ayudo en sus tareas diarias?
Sí ☑ No ☐

7.- ¿Para la aplicación del Plan Piloto se utilizó el sistema operativo Fedora, tenía conocimiento de este sistema de software libre?
Sí ☑ No ☐

8.- ¿Cuál es su nivel de conocimiento, entendimiento en el uso de las aplicaciones Libre Office?
Ninguno ☐ Poco ☐ Medio ☑ Bastante ☐

9.- ¿Cuál es su nivel de conocimiento, entendimiento en el uso del Gestor de Archivos?
Ninguno ☐ Poco ☐ Medio ☑ Bastante ☐

10.- ¿Se adaptó a la interfaz del sistema operativo Fedora y sus aplicativos en relación a lo experimentado en el Sistema operativo Windows?
Sí ☑ No ☐

11.- ¿El uso de software libre le beneficio para la optimización de recursos en la Cooperativa?
Sí ☑ No ☐

12.- ¿En base a la capacitación, desenvolvimiento obtenido recomendaría el uso de software libre a usuarios que utilizan software con licencia?
Sí ☑ No ☐

13.- ¿Cree usted que sería factible aplicar el uso de software libre en todas las estaciones de la Cooperativa?

Sí ☑ No ☐

Encuestado **Encuestador**

ANEXO 9: EXPERIENCIAS EN EL USO DE SEGURIDAD EN LA INFORMACIÓN

UNIVERSIDAD TÉCNICA PARTICULAR DE LOJA

Encuesta sobre la Implementación de Políticas de seguridad

Encuestado: Andrea Moran **Fecha:** 29/Noviembre/2016

1.- Conoce sobre políticas de seguridad en la información aplicables a organizaciones e instituciones financieras

Sí ☑ No ☐

2.- La Cooperativa tenía definida e implementadas políticas de seguridad en la información.

Sí ☐ No ☑

3.- Recibió información sobre las políticas de seguridad en la información implementadas en la Cooperativa.

Sí ☑ No ☐

4.- La rol de usuario administrativo esta autentificado en cada estación de trabajo de la Cooperativa.

Sí ☐ No ☑

5.- Es necesario la aplicación de la Carta de Confidencialidad de la información para definir roles de Usuarios.

Sí ☑ No ☐

6.- Cree beneficioso la aplicación del restringir las unidades de almacenamiento externos, como medida implementada para mantener la confidencialidad de la información del cliente y seguridad del sistema informático.

Sí ☑ No ☐

7.- Cree beneficioso la aplicación del acceso restringido a sitios WEB, para evitar posibles infecciones por virus, robo de información, delitos informáticos.

Sí ☑ No ☐

8.- Cree beneficioso la aplicación de la clasificación y etiquetado de la información para la fácil ubicación de la documentación en el momento que sea requerida.

Sí ☑ No ☐

9.- El tiempo de acceso a páginas web actualmente es rápido para sus tareas diarias.

Sí ☐ No ☑

10.- La restricción a páginas de redes sociales contribuye en la productividad del colaborador, medible en tiempo de desarrollo de las tareas.

Sí ☑ No ☐

11.- La compartición de archivos entre las estaciones es más ágil actualmente en la ejecución de las tareas.

Sí ☑ No ☐

12.- El uso de los dispositivos como escáner e impresoras con la nueva distribución de la red es satisfactorio, con relación a la distribución de la red antes de la ejecución del Proyecto.

Sí ☑ No ☐

13.- Los cambios realizados para el manejo de la información en la Cooperativa es.

Positivo ☑ Negativo ☐

Encuestado

Encuestador

UNIVERSIDAD TÉCNICA PARTICULAR DE LOJA

Encuesta sobre la Implementación de Políticas de seguridad

Encuestado: Ana Rodriguez Fecha: 29/Noviembre/2016

1.- Conoce sobre políticas de seguridad en la información aplicables a organizaciones e instituciones financieras

Sí ☐ No ☑

2.- La Cooperativa tenía definida e implementadas políticas de seguridad en la información.

Sí ☐ No ☑

3.- Recibió información sobre las políticas de seguridad en la información implementadas en la Cooperativa.

Sí ☑ No ☐

4.- La rol de usuario administrativo esta autentificado en cada estación de trabajo de la Cooperativa.

Sí ☐ No ☑

5.- Es necesario la aplicación de la Carta de Confidencialidad de la información para definir roles de Usuarios.

Sí ☑ No ☐

6.- Cree beneficioso la aplicación del restringir las unidades de almacenamiento externos, como medida implementada para mantener la confidencialidad de la información del cliente y seguridad del sistema informático.

Sí ☐ No ☑

7.- Cree beneficioso la aplicación del acceso restringido a sitios WEB, para evitar posibles infecciones por virus, robo de información, delitos informáticos.

Sí ☐ No ☑

8.- Cree beneficioso la aplicación de la clasificación y etiquetado de la información para la fácil ubicación de la documentación en el momento que sea requerida.

Sí ☐ No ☑

9.- El tiempo de acceso a páginas web actualmente es rápido para sus tareas diarias.

Sí ☐ No ☑

10.- La restricción a páginas de redes sociales contribuye en la productividad del colaborador, medible en tiempo de desarrollo de las tareas.

Sí ☑ No ☐

11.- La compartición de archivos entre las estaciones es más ágil actualmente en la ejecución de las tareas.

Sí ☐ No ☑

12.- El uso de los dispositivos como escáner e impresoras con la nueva distribución de la red es satisfactorio, con relación a la distribución de la red antes de la ejecución del Proyecto.

Sí ☑ No ☐

13.- Los cambios realizados para el manejo de la información en la Cooperativa es.

Positivo ☑ Negativo ☐

Encuestado **Encuestador**

UNIVERSIDAD TÉCNICA PARTICULAR DE LOJA

Encuesta sobre la Implementación de Políticas de seguridad

Encuestado: Alejandro Montero **Fecha:** 29 / Noviembre / 2016

1.- Conoce sobre políticas de seguridad en la información aplicables a organizaciones e instituciones financieras

Sí ☐ No ☒

2.- La Cooperativa tenía definida e implementadas políticas de seguridad en la información.

Sí ☐ No ☒

3.- Recibió información sobre las políticas de seguridad en la información implementadas en la Cooperativa.

Sí ☒ No ☐

4.- La rol de usuario administrativo esta autentificado en cada estación de trabajo de la Cooperativa.

Sí ☐ No ☒

5.- Es necesario la aplicación de la Carta de Confidencialidad de la información para definir roles de Usuarios.

Sí ☒ No ☐

6.- Cree beneficioso la aplicación del restringir las unidades de almacenamiento externos, como medida implementada para mantener la confidencialidad de la información del cliente y seguridad del sistema informático.

Sí ☒ No ☐

7.- Cree beneficioso la aplicación del acceso restringido a sitios WEB, para evitar posibles infecciones por virus, robo de información, delitos informáticos.

Sí ☒ No ☐

8.- Cree beneficioso la aplicación de la clasificación y etiquetado de la información para la fácil ubicación de la documentación en el momento que sea requerida.

Sí ☒ No ☐

9.- El tiempo de acceso a páginas web actualmente es rápido para sus tareas diarias.

Sí ☒ No ☐

10.- La restricción a páginas de redes sociales contribuye en la productividad del colaborador, medible en tiempo de desarrollo de las tareas.

Sí ☒ No ☐

11.- La compartición de archivos entre las estaciones es más ágil actualmente en la ejecución de las tareas.

Sí ☒ No ☐

12.- El uso de los dispositivos como escáner e impresoras con la nueva distribución de la red es satisfactorio, con relación a la distribución de la red antes de la ejecución del Proyecto.

Sí ☒ No ☐

13.- Los cambios realizados para el manejo de la información en la Cooperativa es.

Positivo ☒ Negativo ☐

Encuestado

Encuestador

UNIVERSIDAD TÉCNICA PARTICULAR DE LOJA

Encuesta sobre la Implementación de Políticas de seguridad

Encuestado: Ruben Dario Fecha: 29 / Noviembre / 2016

1.- Conoce sobre políticas de seguridad en la información aplicables a organizaciones e instituciones financieras

Sí ☑ No ☐

2.- La Cooperativa tenía definida e implementadas políticas de seguridad en la información.

Sí ☑ No ☐

3.- Recibió información sobre las políticas de seguridad en la información implementadas en la Cooperativa.

Sí ☑ No ☐

4.- La rol de usuario administrativo esta autentificado en cada estación de trabajo de la Cooperativa.

Sí ☑ No ☐

5.- Es necesario la aplicación de la Carta de Confidencialidad de la información para definir roles de Usuarios.

Sí ☑ No ☐

6.- Cree beneficioso la aplicación del restringir las unidades de almacenamiento externos, como medida implementada para mantener la confidencialidad de la información del cliente y seguridad del sistema informático.

Sí ☑ No ☐

7.- Cree beneficioso la aplicación del acceso restringido a sitios WEB, para evitar posibles infecciones por virus, robo de información, delitos informáticos.

Sí ☐ No ☑

8.- Cree beneficioso la aplicación de la clasificación y etiquetado de la información para la fácil ubicación de la documentación en el momento que sea requerida.

Sí ☑ No ☐

9.- El tiempo de acceso a páginas web actualmente es rápido para sus tareas diarias.

Sí ☑ No ☐

10.- La restricción a páginas de redes sociales contribuye en la productividad del colaborador, medible en tiempo de desarrollo de las tareas.

Sí ☐ No ☑

11.- La compartición de archivos entre las estaciones es más ágil actualmente en la ejecución de las tareas.

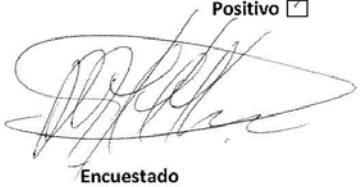
Sí ☑ No ☐

12.- El uso de los dispositivos como escáner e impresoras con la nueva distribución de la red es satisfactorio, con relación a la distribución de la red antes de la ejecución del Proyecto.

Sí ☑ No ☐

13.- Los cambios realizados para el manejo de la información en la Cooperativa es.

Positivo ☑ Negativo ☐



Encuestado **Encuestador**

UNIVERSIDAD TÉCNICA PARTICULAR DE LOJA

Encuesta sobre la Implementación de Políticas de seguridad

Encuestado: Abel Chávez **Fecha:** 29 / Noviembre / 2016

1.- Conoce sobre políticas de seguridad en la información aplicables a organizaciones e instituciones financieras

Sí ☑ No ☐

2.- La Cooperativa tenía definida e implementadas políticas de seguridad en la información.

Sí ☐ No ☑

3.- Recibió información sobre las políticas de seguridad en la información implementadas en la Cooperativa.

Sí ☑ No ☐

4.- La rol de usuario administrativo esta autentificado en cada estación de trabajo de la Cooperativa.

Sí ☐ No ☑

5.- Es necesario la aplicación de la Carta de Confidencialidad de la información para definir roles de Usuarios.

Sí ☐ No ☑

6.- Cree beneficioso la aplicación del restringir las unidades de almacenamiento externos, como medida implementada para mantener la confidencialidad de la información del cliente y seguridad del sistema informático.

Sí ☐ No ☑

7.- Cree beneficioso la aplicación del acceso restringido a sitios WEB, para evitar posibles infecciones por virus, robo de información, delitos informáticos.

Sí ☐ No ☑

8.- Cree beneficioso la aplicación de la clasificación y etiquetado de la información para la fácil ubicación de la documentación en el momento que sea requerida.

Sí ☑ No ☐

9.- El tiempo de acceso a páginas web actualmente es rápido para sus tareas diarias.

Sí ☐ No ☑

10.- La restricción a páginas de redes sociales contribuye en la productividad del colaborador, medible en tiempo de desarrollo de las tareas.

Sí ☐ No ☑

11.- La compartición de archivos entre las estaciones es más ágil actualmente en la ejecución de las tareas.

Sí ☑ No ☐

12.- El uso de los dispositivos como escáner e impresoras con la nueva distribución de la red es satisfactorio, con relación a la distribución de la red antes de la ejecución del Proyecto.

Sí ☑ No ☐

13.- Los cambios realizados para el manejo de la información en la Cooperativa es.

Positivo ☐ Negativo ☑

Encuestado **Encuestador**

Cooperativa de Ahorro y Crédito de la Pequeña Empresa
CACPE Manabí Ltda.

UNIVERSIDAD TÉCNICA PARTICULAR DE LOJA

Encuesta sobre la Implementación de Políticas de seguridad

Encuestado: Leonardo Falconi Fecha: 29/Noviembre/2016

1.- Conoce sobre políticas de seguridad en la información aplicables a organizaciones e instituciones financieras

Sí ☐ No ☑

2.- La Cooperativa tenía definida e implementadas políticas de seguridad en la información.

Sí ☑ No ☐

3.- Recibió información sobre las políticas de seguridad en la información implementadas en la Cooperativa.

Sí ☑ No ☐

4.- La rol de usuario administrativo esta autentificado en cada estación de trabajo de la Cooperativa.

Sí ☐ No ☑

5.- Es necesario la aplicación de la Carta de Confidencialidad de la información para definir roles de Usuarios.

Sí ☑ No ☐

6.- Cree beneficioso la aplicación del restringir las unidades de almacenamiento externos, como medida implementada para mantener la confidencialidad de la información del cliente y seguridad del sistema informático.

Sí ☐ No ☑

7.- Cree beneficioso la aplicación del acceso restringido a sitios WEB, para evitar posibles infecciones por virus, robo de información, delitos informáticos.

Sí ☑ No ☐

8.- Cree beneficioso la aplicación de la clasificación y etiquetado de la información para la fácil ubicación de la documentación en el momento que sea requerida.

Sí ☑ No ☐

9.- El tiempo de acceso a páginas web actualmente es rápido para sus tareas diarias.

Sí ☐ No ☑

10.- La restricción a páginas de redes sociales contribuye en la productividad del colaborador, medible en tiempo de desarrollo de las tareas.

Sí ☑ No ☐

11.- La compartición de archivos entre las estaciones es más ágil actualmente en la ejecución de las tareas.

Sí ☑ **No** ☐

12.- El uso de los dispositivos como escáner e impresoras con la nueva distribución de la red es satisfactorio, con relación a la distribución de la red antes de la ejecución del Proyecto.

Sí ☑ **No** ☐

13.- Los cambios realizados para el manejo de la información en la Cooperativa es.

Positivo ☐ **Negativo** ☑

Encuestado **Encuestador**

Cooperativa de Ahorro y Crédito de la Pequeña Empresa CACPE Manabí Ltda.

UNIVERSIDAD TÉCNICA PARTICULAR DE LOJA

Encuesta sobre la Implementación de Políticas de seguridad

Encuestado: Gabriela Ortega Fecha: 29/Noviembre/2016

1.- Conoce sobre políticas de seguridad en la información aplicables a organizaciones e instituciones financieras

Sí ☑ No ☐

2.- La Cooperativa tenía definida e implementadas políticas de seguridad en la información.

Sí ☐ No ☑

3.- Recibió información sobre las políticas de seguridad en la información implementadas en la Cooperativa.

Sí ☑ No ☐

4.- La rol de usuario administrativo esta autentificado en cada estación de trabajo de la Cooperativa.

Sí ☐ No ☑

5.- Es necesario la aplicación de la Carta de Confidencialidad de la información para definir roles de Usuarios.

Sí ☑ No ☐

6.- Cree beneficioso la aplicación del restringir las unidades de almacenamiento externos, como medida implementada para mantener la confidencialidad de la información del cliente y seguridad del sistema informático.

Sí ☐ No ☑

7.- Cree beneficioso la aplicación del acceso restringido a sitios WEB, para evitar posibles infecciones por virus, robo de información, delitos informáticos.

Sí ☐ No ☑

8.- Cree beneficioso la aplicación de la clasificación y etiquetado de la información para la fácil ubicación de la documentación en el momento que sea requerida.

Sí ☑ No ☐

9.- El tiempo de acceso a páginas web actualmente es rápido para sus tareas diarias.

Sí ☑ No ☐

10.- La restricción a páginas de redes sociales contribuye en la productividad del colaborador, medible en tiempo de desarrollo de las tareas.

Sí ☑ No ☐

11.- La compartición de archivos entre las estaciones es más ágil actualmente en la ejecución de las tareas.

Sí ☑ No ☐

12.- El uso de los dispositivos como escáner e impresoras con la nueva distribución de la red es satisfactorio, con relación a la distribución de la red antes de la ejecución del Proyecto.

Sí ☐ No ☑

13.- Los cambios realizados para el manejo de la información en la Cooperativa es.

Positivo ☑ Negativo ☐

Encuestado **Encuestador**

UNIVERSIDAD TÉCNICA PARTICULAR DE LOJA

Encuesta sobre la Implementación de Políticas de seguridad

Encuestado: Johana Cantos Fecha: 29 / Noviembre / 2016

1.- Conoce sobre políticas de seguridad en la información aplicables a organizaciones e instituciones financieras

Sí ☑ No ☐

2.- La Cooperativa tenía definida e implementadas políticas de seguridad en la información.

Sí ☐ No ☑

3.- Recibió información sobre las políticas de seguridad en la información implementadas en la Cooperativa.

Sí ☑ No ☐

4.- La rol de usuario administrativo esta autentificado en cada estación de trabajo de la Cooperativa.

Sí ☑ No ☐

5.- Es necesario la aplicación de la Carta de Confidencialidad de la información para definir roles de Usuarios.

Sí ☑ No ☐

6.- Cree beneficioso la aplicación del restringir las unidades de almacenamiento externos, como medida implementada para mantener la confidencialidad de la información del cliente y seguridad del sistema informático.

Sí ☑ No ☐

7.- Cree beneficioso la aplicación del acceso restringido a sitios WEB, para evitar posibles infecciones por virus, robo de información, delitos informáticos.

Sí ☑ No ☐

8.- Cree beneficioso la aplicación de la clasificación y etiquetado de la información para la fácil ubicación de la documentación en el momento que sea requerida.

Sí ☑ No ☐

9.- El tiempo de acceso a páginas web actualmente es rápido para sus tareas diarias.

Sí ☑ No ☐

10.- La restricción a páginas de redes sociales contribuye en la productividad del colaborador, medible en tiempo de desarrollo de las tareas.

Sí ☑ No ☐

11.- La compartición de archivos entre las estaciones es más ágil actualmente en la ejecución de las tareas.

Sí ☑ No ☐

12.- El uso de los dispositivos como escáner e impresoras con la nueva distribución de la red es satisfactorio, con relación a la distribución de la red antes de la ejecución del Proyecto.

Sí ☑ No ☐

13.- Los cambios realizados para el manejo de la información en la Cooperativa es.

Positivo ☑ Negativo ☐

Encuestado **Encuestador**

UNIVERSIDAD TÉCNICA PARTICULAR DE LOJA

Encuesta sobre la Implementación de Políticas de seguridad

Encuestado: Efren Gómez **Fecha:** 29 / Noviembre / 2016

1.- Conoce sobre políticas de seguridad en la información aplicables a organizaciones e instituciones financieras

Sí ☑ No ☐

2.- La Cooperativa tenía definida e implementadas políticas de seguridad en la información.

Sí ☐ No ☑

3.- Recibió información sobre las políticas de seguridad en la información implementadas en la Cooperativa.

Sí ☐ No ☑

4.- La rol de usuario administrativo esta autentificado en cada estación de trabajo de la Cooperativa.

Sí ☑ No ☐

5.- Es necesario la aplicación de la Carta de Confidencialidad de la información para definir roles de Usuarios.

Sí ☑ No ☐

6.- Cree beneficioso la aplicación del restringir las unidades de almacenamiento externos, como medida implementada para mantener la confidencialidad de la información del cliente y seguridad del sistema informático.

Sí ☐ No ☑

7.- Cree beneficioso la aplicación del acceso restringido a sitios WEB, para evitar posibles infecciones por virus, robo de información, delitos informáticos.

Sí ☐ No ☑

8.- Cree beneficioso la aplicación de la clasificación y etiquetado de la información para la fácil ubicación de la documentación en el momento que sea requerida.

Sí ☑ No ☐

9.- El tiempo de acceso a páginas web actualmente es rápido para sus tareas diarias.

Sí ☑ No ☐

10.- La restricción a páginas de redes sociales contribuye en la productividad del colaborador, medible en tiempo de desarrollo de las tareas.

Sí ☑ No ☐

11.- La compartición de archivos entre las estaciones es más ágil actualmente en la ejecución de las tareas.

Sí ☑ **No** ☐

12.- El uso de los dispositivos como escáner e impresoras con la nueva distribución de la red es satisfactorio, con relación a la distribución de la red antes de la ejecución del Proyecto.

Sí ☑ **No** ☐

13.- Los cambios realizados para el manejo de la información en la Cooperativa es.

Positivo ☑ **Negativo** ☐

Encuestado **Encuestador**

Cooperativa de Ahorro y Crédito de la Pequeña Empresa CACPE Manabí Ltda.

UNIVERSIDAD TÉCNICA PARTICULAR DE LOJA

Encuesta sobre la Implementación de Políticas de seguridad

Encuestado: Victor Andrade **Fecha:** 29 / Noviembre / 2016

1.- Conoce sobre políticas de seguridad en la información aplicables a organizaciones e instituciones financieras

Sí ☑ No ☐

2.- La Cooperativa tenía definida e implementadas políticas de seguridad en la información.

Sí ☐ No ☑

3.- Recibió información sobre las políticas de seguridad en la información implementadas en la Cooperativa.

Sí ☑ No ☐

4.- La rol de usuario administrativo esta autentificado en cada estación de trabajo de la Cooperativa.

Sí ☐ No ☑

5.- Es necesario la aplicación de la Carta de Confidencialidad de la información para definir roles de Usuarios.

Sí ☐ No ☑

6.- Cree beneficioso la aplicación del restringir las unidades de almacenamiento externos, como medida implementada para mantener la confidencialidad de la información del cliente y seguridad del sistema informático.

Sí ☑ No ☐

7.- Cree beneficioso la aplicación del acceso restringido a sitios WEB, para evitar posibles infecciones por virus, robo de información, delitos informáticos.

Sí ☑ No ☐

8.- Cree beneficioso la aplicación de la clasificación y etiquetado de la información para la fácil ubicación de la documentación en el momento que sea requerida.

Sí ☑ No ☐

9.- El tiempo de acceso a páginas web actualmente es rápido para sus tareas diarias.

Sí ☑ No ☐

10.- La restricción a páginas de redes sociales contribuye en la productividad del colaborador, medible en tiempo de desarrollo de las tareas.

Sí ☑ No ☐

11.- La compartición de archivos entre las estaciones es más ágil actualmente en la ejecución de las tareas.

Sí ☑ **No** ☐

12.- El uso de los dispositivos como escáner e impresoras con la nueva distribución de la red es satisfactorio, con relación a la distribución de la red antes de la ejecución del Proyecto.

Sí ☑ **No** ☐

13.- Los cambios realizados para el manejo de la información en la Cooperativa es.

Positivo ☑ **Negativo** ☐

Encuestado **Encuestador**

UNIVERSIDAD TÉCNICA PARTICULAR DE LOJA

Encuesta sobre la Implementación de Políticas de seguridad

Encuestado: Nohemí Zambrano Fecha: 29/ Noviembre/2016

1.- Conoce sobre políticas de seguridad en la información aplicables a organizaciones e instituciones financieras

Sí ☑ No ☐

2.- La Cooperativa tenía definida e implementadas políticas de seguridad en la información.

Sí ☑ No ☐

3.- Recibió información sobre las políticas de seguridad en la información implementadas en la Cooperativa.

Sí ☑ No ☐

4.- La rol de usuario administrativo esta autentificado en cada estación de trabajo de la Cooperativa.

Sí ☑ No ☐

5.- Es necesario la aplicación de la Carta de Confidencialidad de la información para definir roles de Usuarios.

Sí ☑ No ☐

6.- Cree beneficioso la aplicación del restringir las unidades de almacenamiento externos, como medida implementada para mantener la confidencialidad de la información del cliente y seguridad del sistema informático.

Sí ☑ No ☐

7.- Cree beneficioso la aplicación del acceso restringido a sitios WEB, para evitar posibles infecciones por virus, robo de información, delitos informáticos.

Sí ☑ No ☐

8.- Cree beneficioso la aplicación de la clasificación y etiquetado de la información para la fácil ubicación de la documentación en el momento que sea requerida.

Sí ☑ No ☐

9.- El tiempo de acceso a páginas web actualmente es rápido para sus tareas diarias.

Sí ☑ No ☐

10.- La restricción a páginas de redes sociales contribuye en la productividad del colaborador, medible en tiempo de desarrollo de las tareas.

Sí ☑ No ☐

11.- La compartición de archivos entre las estaciones es más ágil actualmente en la ejecución de las tareas.

Sí ☑ No ☐

12.- El uso de los dispositivos como escáner e impresoras con la nueva distribución de la red es satisfactorio, con relación a la distribución de la red antes de la ejecución del Proyecto.

Sí ☐ No ☑

13.- Los cambios realizados para el manejo de la información en la Cooperativa es.

Positivo ☑ Negativo ☐

Encuestado **Encuestador**

Cooperativa de Ahorro y Crédito de la Pequeña Empresa CACPE Manabí Ltda.

UNIVERSIDAD TÉCNICA PARTICULAR DE LOJA

Encuesta sobre la Implementación de Políticas de seguridad

Encuestado: Joao Velez **Fecha:** 28/Noviembre/2014

1.- Conoce sobre políticas de seguridad en la información aplicables a organizaciones e instituciones financieras

Sí ☑ No ☐

2.- La Cooperativa tenía definida e implementadas políticas de seguridad en la información.

Sí ☐ No ☑

3.- Recibió información sobre las políticas de seguridad en la información implementadas en la Cooperativa.

Sí ☑ No ☐

4.- La rol de usuario administrativo esta autentificado en cada estación de trabajo de la Cooperativa.

Sí ☐ No ☑

5.- Es necesario la aplicación de la Carta de Confidencialidad de la información para definir roles de Usuarios.

Sí ☑ No ☐

6.- Cree beneficioso la aplicación del restringir las unidades de almacenamiento externos, como medida implementada para mantener la confidencialidad de la información del cliente y seguridad del sistema informático.

Sí ☑ No ☐

7.- Cree beneficioso la aplicación del acceso restringido a sitios WEB, para evitar posibles infecciones por virus, robo de información, delitos informáticos.

Sí ☑ No ☐

8.- Cree beneficioso la aplicación de la clasificación y etiquetado de la información para la fácil ubicación de la documentación en el momento que sea requerida.

Sí ☑ No ☐

9.- El tiempo de acceso a páginas web actualmente es rápido para sus tareas diarias.

Sí ☑ No ☐

10.- La restricción a páginas de redes sociales contribuye en la productividad del colaborador, medible en tiempo de desarrollo de las tareas.

Sí ☐ No ☑

11.- La compartición de archivos entre las estaciones es más ágil actualmente en la ejecución de las tareas.

Sí ☑ No ☐

12.- El uso de los dispositivos como escáner e impresoras con la nueva distribución de la red es satisfactorio, con relación a la distribución de la red antes de la ejecución del Proyecto.

Sí ☑ No ☐

13.- Los cambios realizados para el manejo de la información en la Cooperativa es.

Positivo ☑ Negativo ☐

Encuestado **Encuestador**

UNIVERSIDAD TÉCNICA PARTICULAR DE LOJA

Encuesta sobre la Implementación de Políticas de seguridad

Encuestado: Mariuxi Posligua **Fecha:** 29 / Noviembre / 2016

1.- Conoce sobre políticas de seguridad en la información aplicables a organizaciones e instituciones financieras

Sí ☑ No ☐

2.- La Cooperativa tenía definida e implementadas políticas de seguridad en la información.

Sí ☑ No ☐

3.- Recibió información sobre las políticas de seguridad en la información implementadas en la Cooperativa.

Sí ☐ No ☑

4.- La rol de usuario administrativo esta autentificado en cada estación de trabajo de la Cooperativa.

Sí ☑ No ☐

5.- Es necesario la aplicación de la Carta de Confidencialidad de la información para definir roles de Usuarios.

Sí ☐ No ☑

6.- Cree beneficioso la aplicación del restringir las unidades de almacenamiento externos, como medida implementada para mantener la confidencialidad de la información del cliente y seguridad del sistema informático.

Sí ☐ No ☑

7.- Cree beneficioso la aplicación del acceso restringido a sitios WEB, para evitar posibles infecciones por virus, robo de información, delitos informáticos.

Sí ☑ No ☐

8.- Cree beneficioso la aplicación de la clasificación y etiquetado de la información para la fácil ubicación de la documentación en el momento que sea requerida.

Sí ☑ No ☐

9.- El tiempo de acceso a páginas web actualmente es rápido para sus tareas diarias.

Sí ☑ No ☐

10.- La restricción a páginas de redes sociales contribuye en la productividad del colaborador, medible en tiempo de desarrollo de las tareas.

Sí ☑ No ☐

11.- La compartición de archivos entre las estaciones es más ágil actualmente en la ejecución de las tareas.

Sí ☑ No ☐

12.- El uso de los dispositivos como escáner e impresoras con la nueva distribución de la red es satisfactorio, con relación a la distribución de la red antes de la ejecución del Proyecto.

Sí ☑ No ☐

13.- Los cambios realizados para el manejo de la información en la Cooperativa es.

Positivo ☑ Negativo ☐

Encuestado

Encuestador

UNIVERSIDAD TÉCNICA PARTICULAR DE LOJA

Encuesta sobre la Implementación de Políticas de seguridad

Encuestado: Sergio Villalta **Fecha:** 29/Noviembre/2016

1.- Conoce sobre políticas de seguridad en la información aplicables a organizaciones e instituciones financieras

Sí ☑ No ☐

2.- La Cooperativa tenía definida e implementadas políticas de seguridad en la información.

Sí ☐ No ☑

3.- Recibió información sobre las políticas de seguridad en la información implementadas en la Cooperativa.

Sí ☑ No ☐

4.- La rol de usuario administrativo esta autentificado en cada estación de trabajo de la Cooperativa.

Sí ☑ No ☐

5.- Es necesario la aplicación de la Carta de Confidencialidad de la información para definir roles de Usuarios.

Sí ☑ No ☐

6.- Cree beneficioso la aplicación del restringir las unidades de almacenamiento externos, como medida implementada para mantener la confidencialidad de la información del cliente y seguridad del sistema informático.

Sí ☐ No ☑

7.- Cree beneficioso la aplicación del acceso restringido a sitios WEB, para evitar posibles infecciones por virus, robo de información, delitos informáticos.

Sí ☐ No ☑

8.- Cree beneficioso la aplicación de la clasificación y etiquetado de la información para la fácil ubicación de la documentación en el momento que sea requerida.

Sí ☑ No ☐

9.- El tiempo de acceso a páginas web actualmente es rápido para sus tareas diarias.

Sí ☑ No ☐

10.- La restricción a páginas de redes sociales contribuye en la productividad del colaborador, medible en tiempo de desarrollo de las tareas.

Sí ☑ No ☐

11.- La compartición de archivos entre las estaciones es más ágil actualmente en la ejecución de las tareas.

Sí ☑ No ☐

12.- El uso de los dispositivos como escáner e impresoras con la nueva distribución de la red es satisfactorio, con relación a la distribución de la red antes de la ejecución del Proyecto.

Sí ☑ No ☐

13.- Los cambios realizados para el manejo de la información en la Cooperativa es.

Positivo ☑ Negativo ☐

Encuestado **Encuestador**

Cooperativa de Ahorro y Crédito de la Pequeña Empresa CACPE Manabí Ltda.

UNIVERSIDAD TÉCNICA PARTICULAR DE LOJA

Encuesta sobre la Implementación de Políticas de seguridad

Encuestado: Fabian Zambrano **Fecha:** 29 / Noviembre / 2016

1.- Conoce sobre políticas de seguridad en la información aplicables a organizaciones e instituciones financieras

Sí ☑ No ☐

2.- La Cooperativa tenía definida e implementadas políticas de seguridad en la información.

Sí ☑ No ☐

3.- Recibió información sobre las políticas de seguridad en la información implementadas en la Cooperativa.

Sí ☑ No ☐

4.- La rol de usuario administrativo esta autentificado en cada estación de trabajo de la Cooperativa.

Sí ☑ No ☐

5.- Es necesario la aplicación de la Carta de Confidencialidad de la información para definir roles de Usuarios.

Sí ☐ No ☑

6.- Cree beneficioso la aplicación del restringir las unidades de almacenamiento externos, como medida implementada para mantener la confidencialidad de la información del cliente y seguridad del sistema informático.

Sí ☑ No ☐

7.- Cree beneficioso la aplicación del acceso restringido a sitios WEB, para evitar posibles infecciones por virus, robo de información, delitos informáticos.

Sí ☐ No ☑

8.- Cree beneficioso la aplicación de la clasificación y etiquetado de la información para la fácil ubicación de la documentación en el momento que sea requerida.

Sí ☑ No ☐

9.- El tiempo de acceso a páginas web actualmente es rápido para sus tareas diarias.

Sí ☐ No ☑

10.- La restricción a páginas de redes sociales contribuye en la productividad del colaborador, medible en tiempo de desarrollo de las tareas.

Sí ☑ No ☐

11.- La compartición de archivos entre las estaciones es más ágil actualmente en la ejecución de las tareas.

Sí ☑ **No** ☐

12.- El uso de los dispositivos como escáner e impresoras con la nueva distribución de la red es satisfactorio, con relación a la distribución de la red antes de la ejecución del Proyecto.

Sí ☐ **No** ☑

13.- Los cambios realizados para el manejo de la información en la Cooperativa es.

Positivo ☑ **Negativo** ☐

Encuestado **Encuestador**

ANEXO 10: DECLARACIÓN DE CONFIDENCIALIDAD

Declaración de Confidencialidad

Fecha: 29 de noviembre de 2016

Estimado(a):

Para asegurarnos de que se cumpla con el código de Ética desde el Principio de Confidencialidad y los lineamientos dados en por la Cooperativa de Ahorro y crédito Cacpe Manabí con relación a nuestras responsabilidades profesionales y en especial con la protección de la información que administramos, es esencial mantener la confidencialidad de los asuntos de la compañía, dando cumplimiento a "ser prudentes en el uso y protección de la información adquirida en el transcurso del trabajo y a no utilizar la información para lucro personal o de alguna manera que fuera contraria a la ley en detrimento de los objetivos legítimos y éticos de la organización".

He leído, entendido y cumplo el lineamiento dado sobre confidencialidad, en relación con los asuntos de la Organización.

Firma: _____

Nombre: SERGIO VILLALTA

cedula: 1715719918

Declaración de Confidencialidad

Fecha: 29 de noviembre de 2016

Estimado(a):

Para asegurarnos de que se cumpla con el código de Ética desde el Principio de Confidencialidad y los lineamientos dados en por la Cooperativa de Ahorro y crédito Cacpe Manabí con relación a nuestras responsabilidades profesionales y en especial con la protección de la información que administramos, es esencial mantener la confidencialidad de los asuntos de la compañía, dando cumplimiento a "ser prudentes en el uso y protección de la información adquirida en el transcurso del trabajo y a no utilizar la información para lucro personal o de alguna manera que fuera contraria a la ley en detrimento de los objetivos legítimos y éticos de la organización".

He leído, entendido y cumplo el lineamiento dado sobre confidencialidad, en relación con los asuntos de la Organización.

Firma: _____

Nombre: _____

cedula: 1308414673

Declaración de Confidencialidad

Fecha: 29 de noviembre de 2016

Estimado(a):

Para asegurarnos de que se cumpla con el código de Ética desde el Principio de Confidencialidad y los lineamientos dados en por la Cooperativa de Ahorro y crédito Cacpe Manabí con relación a nuestras responsabilidades profesionales y en especial con la protección de la información que administramos, es esencial mantener la confidencialidad de los asuntos de la compañía, dando cumplimiento a "ser prudentes en el uso y protección de la información adquirida en el transcurso del trabajo y a no utilizar la información para lucro personal o de alguna manera que fuera contraria a la ley en detrimento de los objetivos legítimos y éticos de la organización".

He leído, entendido y cumplo el lineamiento dado sobre confidencialidad, en relación con los asuntos de la Organización.

Firma: _____

Nombre: Mariuxi Posligua Gomez

cedula: 131323413-8

Declaración de Confidencialidad

Fecha: 29 de noviembre de 2016

Estimado(a):

Para asegurarnos de que se cumpla con el código de Ética desde el Principio de Confidencialidad y los lineamientos dados en por la Cooperativa de Ahorro y crédito Cacpe Manabí con relación a nuestras responsabilidades profesionales y en especial con la protección de la información que administramos, es esencial mantener la confidencialidad de los asuntos de la compañía, dando cumplimiento a "ser prudentes en el uso y protección de la información adquirida en el transcurso del trabajo y a no utilizar la información para lucro personal o de alguna manera que fuera contraria a la ley en detrimento de los objetivos legítimos y éticos de la organización".

He leído, entendido y cumplo el lineamiento dado sobre confidencialidad, en relación con los asuntos de la Organización.

Firma: _____

Nombre: Sara Vélez Nava

cedula: 131079426-6

Declaración de Confidencialidad

Fecha: 29 de noviembre de 2016

Estimado(a):

Para asegurarnos de que se cumpla con el código de Ética desde el Principio de Confidencialidad y los lineamientos dados en por la Cooperativa de Ahorro y crédito Cacpe Manabí con relación a nuestras responsabilidades profesionales y en especial con la protección de la información que administramos, es esencial mantener la confidencialidad de los asuntos de la compañía, dando cumplimiento a "ser prudentes en el uso y protección de la información adquirida en el transcurso del trabajo y a no utilizar la información para lucro personal o de alguna manera que fuera contraria a la ley en detrimento de los objetivos legítimos y éticos de la organización".

He leído, entendido y cumplo el lineamiento dado sobre confidencialidad, en relación con los asuntos de la Organización.

Firma:

Nombre: Cristian Antonio Maldonado Granados

cedula: 090678965-8

Declaración de Confidencialidad

Fecha: 29 de noviembre de 2016

Estimado(a):

Para asegurarnos de que se cumpla con el código de Ética desde el Principio de Confidencialidad y los lineamientos dados en por la Cooperativa de Ahorro y crédito Cacpe Manabí con relación a nuestras responsabilidades profesionales y en especial con la protección de la información que administramos, es esencial mantener la confidencialidad de los asuntos de la compañía, dando cumplimiento a "ser prudentes en el uso y protección de la información adquirida en el transcurso del trabajo y a no utilizar la información para lucro personal o de alguna manera que fuera contraria a la ley en detrimento de los objetivos legítimos y éticos de la organización".

He leído, entendido y cumplo el lineamiento dado sobre confidencialidad, en relación con los asuntos de la Organización.

Firma: _____

Nombre: Noheme Elizabeth Zambrano Robolino

cedula: 1304773161-9

Cooperativa de Ahorro y Crédito de la Pequeña Empresa CACPE Manabí Ltda.

Declaración de Confidencialidad

29 de noviembre de 2016

Fecha:

Estimado(a):

Para asegurarnos de que se cumpla con el código de Ética desde el Principio de Confidencialidad y los lineamientos dados en por la Cooperativa de Ahorro y crédito Cacpe Manabí con relación a nuestras responsabilidades profesionales y en especial con la protección de la información que administramos, es esencial mantener la confidencialidad de los asuntos de la compañía, dando cumplimiento a "ser prudentes en el uso y protección de la información adquirida en el transcurso del trabajo y a no utilizar la información para lucro personal o de alguna manera que fuera contraria a la ley en detrimento de los objetivos legítimos y éticos de la organización".

He leído, entendido y cumplo el lineamiento dado sobre confidencialidad, en relación con los asuntos de la Organización.

Firma: _____

Nombre: Johanna Cortez Zambrano

cedula: 1309766358

Declaración de Confidencialidad

Fecha: 29 de noviembre de 2016

Estimado(a):

Para asegurarnos de que se cumpla con el código de Ética desde el Principio de Confidencialidad y los lineamientos dados en por la Cooperativa de Ahorro y crédito Cacpe Manabí con relación a nuestras responsabilidades profesionales y en especial con la protección de la información que administramos, es esencial mantener la confidencialidad de los asuntos de la compañía, dando cumplimiento a "ser prudentes en el uso y protección de la información adquirida en el transcurso del trabajo y a no utilizar la información para lucro personal o de alguna manera que fuera contraria a la ley en detrimento de los objetivos legítimos y éticos de la organización".

He leído, entendido y cumplo el lineamiento dado sobre confidencialidad, en relación con los asuntos de la Organización.

Firma: _____

Nombre: Elsa Emilia Gómez M.

cedula: 1308496353

Cooperativa de Ahorro y Crédito de la Pequeña Empresa CACPE Manabí Ltda.

Declaración de Confidencialidad

Fecha:
29 de noviembre de 2016

Estimado(a):

Para asegurarnos de que se cumpla con el código de Ética desde el Principio de Confidencialidad y los lineamientos dados en por la Cooperativa de Ahorro y crédito Cacpe Manabí con relación a nuestras responsabilidades profesionales y en especial con la protección de la información que administramos, es esencial mantener la confidencialidad de los asuntos de la compañía, dando cumplimiento a "ser prudentes en el uso y protección de la información adquirida en el transcurso del trabajo y a no utilizar la información para lucro personal o de alguna manera que fuera contraria a la ley en detrimento de los objetivos legítimos y éticos de la organización".

He leído, entendido y cumplo el lineamiento dado sobre confidencialidad, en relación con los asuntos de la Organización.

Firma: _____

Nombre: Pedro David Morales J.

cedula: 1302127756

Declaración de Confidencialidad

Fecha:
29 de noviembre de 2016

Estimado(a):

Para asegurarnos de que se cumpla con el código de Ética desde el Principio de Confidencialidad y los lineamientos dados en por la Cooperativa de Ahorro y crédito Cacpe Manabí con relación a nuestras responsabilidades profesionales y en especial con la protección de la información que administramos, es esencial mantener la confidencialidad de los asuntos de la compañía, dando cumplimiento a "ser prudentes en el uso y protección de la información adquirida en el transcurso del trabajo y a no utilizar la información para lucro personal o de alguna manera que fuera contraria a la ley en detrimento de los objetivos legítimos y éticos de la organización".

He leído, entendido y cumplo el lineamiento dado sobre confidencialidad, en relación con los asuntos de la Organización.

Firma: _____

Nombre: Abel Chávez Vera

cedula: 131120879

Declaración de Confidencialidad

Fecha:
29 de noviembre de 2016

Estimado(a):

Para asegurarnos de que se cumpla con el código de Ética desde el Principio de Confidencialidad y los lineamientos dados en por la Cooperativa de Ahorro y crédito Cacpe Manabí con relación a nuestras responsabilidades profesionales y en especial con la protección de la información que administramos, es esencial mantener la confidencialidad de los asuntos de la compañía, dando cumplimiento a "ser prudentes en el uso y protección de la información adquirida en el transcurso del trabajo y a no utilizar la información para lucro personal o de alguna manera que fuera contraria a la ley en detrimento de los objetivos legítimos y éticos de la organización".

He leído, entendido y cumplo el lineamiento dado sobre confidencialidad, en relación con los asuntos de la Organización.

Firma: _____

Nombre: Ana Rodriguez

cedula: 130909529-5

Cooperativa de Ahorro y Crédito de la Pequeña Empresa
CACPE Manabí Ltda.

Declaración de Confidencialidad

Fecha:
29 de noviembre de 2016

Estimado(a):

Para asegurarnos de que se cumpla con el código de Ética desde el Principio de Confidencialidad y los lineamientos dados en por la Cooperativa de Ahorro y crédito Cacpe Manabí con relación a nuestras responsabilidades profesionales y en especial con la protección de la información que administramos, es esencial mantener la confidencialidad de los asuntos de la compañía, dando cumplimiento a "ser prudentes en el uso y protección de la información adquirida en el transcurso del trabajo y a no utilizar la información para lucro personal o de alguna manera que fuera contraria a la ley en detrimento de los objetivos legítimos y éticos de la organización".

He leído, entendido y cumplo el lineamiento dado sobre confidencialidad, en relación con los asuntos de la Organización.

Firma: _____

Nombre: Washington Montero

cedula: 1310780034

Declaración de Confidencialidad

Fecha:

29 de noviembre de 2016

Estimado(a):

Para asegurarnos de que se cumpla con el código de Ética desde el Principio de Confidencialidad y los lineamientos dados en por la Cooperativa de Ahorro y crédito Cacpe Manabí con relación a nuestras responsabilidades profesionales y en especial con la protección de la información que administramos, es esencial mantener la confidencialidad de los asuntos de la compañía, dando cumplimiento a "ser prudentes en el uso y protección de la información adquirida en el transcurso del trabajo y a no utilizar la información para lucro personal o de alguna manera que fuera contraria a la ley en detrimento de los objetivos legítimos y éticos de la organización".

He leído, entendido y cumplo el lineamiento dado sobre confidencialidad, en relación con los asuntos de la Organización.

Firma: _____

Nombre: Andrea Moran

cedula: 1309095830-3

Declaración de Confidencialidad

Fecha: 29 de noviembre de 2016

Estimado(a):

Para asegurarnos de que se cumpla con el código de Ética desde el Principio de Confidencialidad y los lineamientos dados en por la Cooperativa de Ahorro y crédito Cacpe Manabí con relación a nuestras responsabilidades profesionales y en especial con la protección de la información que administramos, es esencial mantener la confidencialidad de los asuntos de la compañía, dando cumplimiento a "ser prudentes en el uso y protección de la información adquirida en el transcurso del trabajo y a no utilizar la información para lucro personal o de alguna manera que fuera contraria a la ley en detrimento de los objetivos legítimos y éticos de la organización".

He leído, entendido y cumplo el lineamiento dado sobre confidencialidad, en relación con los asuntos de la Organización.

Firma: _____

Nombre: LEONARDO FALCONI ROMERO

cedula: 1309549572

Declaración de Confidencialidad

29 de noviembre de 2016

Fecha:

Estimado(a):

Para asegurarnos de que se cumpla con el código de Ética desde el Principio de Confidencialidad y los lineamientos dados en por la Cooperativa de Ahorro y crédito Cacpe Manabí con relación a nuestras responsabilidades profesionales y en especial con la protección de la información que administramos, es esencial mantener la confidencialidad de los asuntos de la compañía, dando cumplimiento a "ser prudentes en el uso y protección de la información adquirida en el transcurso del trabajo y a no utilizar la información para lucro personal o de alguna manera que fuera contraria a la ley en detrimento de los objetivos legítimos y éticos de la organización".

He leído, entendido y cumplo el lineamiento dado sobre confidencialidad, en relación con los asuntos de la Organización.

Firma: _____

Nombre: Gabriela Arteaga

cedula: 1308816133

Cooperativa de Ahorro y Crédito de la Pequeña Empresa CACPE Manabí Ltda.