INTRODUCCIÓN

Hoy en día la informática desempeña un papel importante en las actividades de las instituciones, más aún si las instituciones son de tipo financieras donde la dependencia de la información es alta, ya que les resultaría muy difícil funcionar sin los recursos informáticos, este es el caso de la Cooperativa de Ahorro y Crédito (COAC) Alianza del Valle, que depende casi en su totalidad de la información para poder realizar sus actividades y poder dar un buen servicio a sus socios.

En caso de un desastre, que ocasione la interrupción de los servicios Informáticos por largo tiempo puede ocasionar pérdidas financieras y lo más importante la imagen de la Institución disminuiría en forma significativa, sobre todo si está implicada la responsabilidad del área informática. Lo más grave es que se puede perder la credibilidad del público y como consecuencia, la Institución puede terminar en un fracaso total.

Por este motivo la información se ha convertido en un patrimonio primordial a cual se deben aplicar medidas de seguridad para protegerla y estar preparados para afrontar desastres de diversos tipos como pueden ser: humano o natural a través de un Plan de Contingencia y con la aplicación de Políticas de Seguridad para preservar la información.

La seguridad informática ha tomado gran auge, debido a las cambiantes condiciones y nuevas plataformas tecnológicas disponibles. La posibilidad de interconectarse a través de redes, ha abierto nuevos horizontes ha las empresas para mejorar su productividad y poder explorar más allá de las

fronteras nacionales, lo cual lógicamente ha traído consigo, la aparición de nuevas amenazas para los sistemas de información.

Estos riesgos que se enfrentan han llevado a que muchas empresas desarrollen documentos y directrices que orientan en el uso adecuado de estas destrezas tecnológicas y recomendaciones para obtener el mayor provecho de estas ventajas, y evitar el uso indebido de las mismas, lo cual puede ocasionar serios problemas a los bienes, servicios y operaciones de la empresa.

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

ANTECEDENTES

Alianza del Valle nace el 26 de mayo de 1970, la finalidad de la Cooperativa se orienta a satisfacer las necesidades económicas y sociales de los sectores productivos que no tienen acceso al Sistema Financiero tradicional apoyando con su gestión a la pequeña, mediana empresa y microempresa así como también ayudando a la solución de vivienda, administrando sus recursos de acuerdo a normas de prudencia y solvencia financiera. Proyectando una imagen de confiabilidad a través de servicios financieros ágiles y oportunos con un enfoque social.

Alianza del Valle, actualmente realiza sus operaciones en los cantones: Quito, Mejía y Rumiñahui de la provincia del Pichincha, su matriz se ubica en el barrio Chaupitena en la parroquia Amaguaña; mantiene una sucursal en la zona norte de la ciudad de Quito, el Inca, y en la parte sur operan las oficinas de Chillogallo, Conocoto, Amaguaña, La Ecuatoriana, Guamaní, en el cantón Mejía operan las agencias de Aloag y Machachi, y la agencia Sangolquí en el cantón Rumiñahui, todas las oficinas se hallan interconectadas con la matriz, dando una mayor facilidad al socio para que realice sus transacciones en cualquiera de las sucursales.

A Enero del 2005, la Cooperativa cuenta con 29.854 socios, actualmente es parte de MEGARED, que es un convenio entre las Cooperativas: El Sagrario, Tulcán, Pablo Muñoz Vega y Alianza del Valle, cuyo objetivo es propender o facilitar la prestación de servicios a los asociados, a través de ventanillas compartidas; y el establecimiento de cajeros automáticos mediante BANRED.

SITUACIÓN ACTUAL

Debido a que la COAC. Alianza del Valle maneja la información de más de 29.854 socios según las estadísticas a Enero del 2005 en sus 9 sucursales que se hallan interconectadas a la matriz, es de vital importancia que el área de sistemas vele por la seguridad de la información y que ésta este disponible cuando se lo requiera.

Una política de seguridad informática es una forma de comunicarse con los usuarios, ya que las mismas establecen un canal formal de actuación del personal, en relación con los recursos y servicios informáticos de la organización.

En la actualidad el departamento de sistemas no tiene delineadas sus políticas de seguridad para la información que allí se maneja esto es un punto muy crítico en la organización más aun si se trabaja con movimientos económicos como lo hace la COAC. Alianza del Valle.

Además dicho departamento según se pudo apreciar actualmente no está preparado para recuperarse y continuar con sus operaciones en un tiempo razonable frente a un desastre de cualquier tipo que pueda ocurrir, ya que no cuentan con un plan de continuidad o contingencia, ocasionando de esta manera que las sucursales paralicen sus operaciones y dejen de atender a los socios.

JUSTIFICACIÓN

Dentro de la estructura de la cooperativa se encuentra el Departamento de Sistemas en el cual se maneja toda la información de los socios y sus respectivas cuentas, siendo así este departamento una unidad administrativa que da soporte a las operaciones y procesos organizacionales de la Cooperativa con el procesamiento de datos e información de una manera sistematizada y automática.

La información que se maneja en el departamento de sistemas es calificada como confidencial y privada por esto diseñar las políticas de seguridad para esta información lo mas rápido posibles es muy primordial teniendo en cuenta que no se puede considerar que una política de seguridad es una descripción técnica de mecanismos, ni una expresión legal que involucre sanciones a conductas de los empleados, es más bien una descripción de los que deseamos proteger y él por qué de ello, pues cada política de seguridad es una invitación a cada uno de sus miembros a reconocer la información como uno de

sus principales activos así como, un motor de intercambio y desarrollo en el ámbito de sus negocios. Por tal razón, las políticas de seguridad deben concluir en una posición consciente y vigilante del personal por el uso y limitaciones de los recursos y servicios informáticos.

Por este motivo es de vital importancia que se tenga muy en claro las políticas de seguridad y el plan de continuidad o contingencia para que la información no se pierda, no se altere, esté segura y disponible cuando se lo requiera, para el normal desenvolvimiento de las actividades que se realizan en la Cooperativa.

Con el diseño de la políticas de seguridad y el desarrollo del plan de contingencia para el área de sistemas de COAC. Alianza del Valle, podremos garantizar el funcionamiento correcto y normal de la cooperativa ante cualquier tipo de desastres, dando así una mayor credibilidad y confianza a todos los clientes.

ALCANCE

Las políticas de seguridad de la información, deben ofrecer explicaciones comprensibles sobre por qué deben tomarse ciertas decisiones y explicar la importancia de los recursos. Igualmente, deberán establecer las expectativas de la organización en relación con la seguridad y especificar la autoridad responsable de aplicar los correctivos o sanciones.

Otro punto importante, es que las políticas de seguridad deben redactarse en un lenguaje sencillo y entendible, libre de tecnicismos y términos ambiguos que impidan una comprensión clara de las mismas.

El Plan de Contingencias implica un análisis detallado y minucioso de los posibles riesgos a los cuales pueden estar expuestos los equipos de cómputo y la información contenida en los diversos medios de almacenamiento, por lo que

se hará el análisis de los riesgos, cómo reducir su posibilidad de ocurrencia y los procedimientos a seguir en caso que se presentara el problema.

Pese a todas las medidas de seguridad puede ocurrir un desastre, por tanto es necesario que el Plan de Contingencias incluya un Plan de Recuperación de Desastres, el cual tendrá como objetivo, restaurar el Servicio de Cómputo en forma rápida, eficiente y con el menor costo y pérdidas posibles.

Si bien es cierto que se puede presentar diferentes niveles de daños, también se hace necesario presuponer que el daño ha sido total, con la finalidad de tener bien definidas las políticas de seguridad de la información y un Plan de Contingencias lo más completo posible.

Para llevar a cabo la elaboración de las políticas de seguridad de la información se seguirá las siguientes actividades:

- Evaluación a fondo de las vulnerabilidades, amenazas y riesgos.
- Recopilación de material de apoyo
- Definir un marco de referencia
- Redactar la documentación

A continuación se muestran las principales actividades requeridas para el desarrollo del Plan de Contingencia:

- Análisis de Riesgos
- Actividades previas al desastre
- Actividades durante el desastre
- Actividades después del desastre
- Distribución y mantenimiento del plan

Resaltamos que la implementación de las alternativas de solución planteados tanto en la políticas como en el plan dependerá de los directivos de la Cooperativa.

OBJETIVOS

- **OBJETIVO GENERAL**

Diseñar las políticas de seguridad de la información y Desarrollar el Plan de Contingencia para el Área de Sistemas de la Cooperativa de Ahorro y Crédito Alianza del Valle.

- **OBJETIVOS ESPECÍFICOS**

1. Analizar y realizar un estudio de la situación actual de las instalaciones informáticas de la COAC. Alianza del Valle.
2. Identificar, analizar los riesgos y sus respectivos impactos que podrían ocasionar la paralización de las operaciones del área de sistemas de la COAC. Alianza del Valle
3. Diseñar políticas de seguridad de información siguiendo los lineamientos propuestos por COBIT y por la metodología a utilizarse en este plan.
4. Desarrollar el Plan de Contingencias.

CAPITULO I

MARCO TEÓRICO

1.1. SEGURIDAD INFORMÁTICA

"EL objetivo de la Seguridad Informática será mantener la Integridad, Disponibilidad, Privacidad (sus aspectos fundamentales), Control y Autenticidad de la información manejada por computadora."[1]

Para comenzar el análisis de la Seguridad Informática se deberá conocer las características de lo que se pretende proteger: la información.

Así, definimos Dato como "la unidad con la que se compone cierta información"[2]

La Información "es una agregación de datos que tiene un significado especifico mas allá de cada uno de estos"[2], y tendrá un sentido particular según como y quien la procese.

1.1.1. Definición de Seguridad Informática

No existe una definición estricta de lo que se entiende por seguridad informática, puesto que ésta abarca múltiples y muy diversas áreas relacionadas con los Sistemas de Información. Áreas que van desde la protección física del ordenador como componentes hardware, de su entorno, hasta la protección de la información que contiene o de las redes que lo comunican con el exterior. Tampoco es el único objetivo de la seguridad. Son muy diversos los tipos de amenazas contra los que debemos protegernos. Desde amenazas físicas, como los cortes eléctricos, hasta errores no intencionados de los usuarios, pasando por los virus informáticos o el robo,

[1] ALDEGANI, Gustavo. Miguel. Seguridad Informática MP ediciones. Argentina. 1997 Página 22.

[2] CALVO, Rafael Fernández. Glosario Básico Ingles-Español para usuarios de internet 1994-2000

destrucción o modificación de la información. No obstante sí hay tres aspectos fundamentales que definen la seguridad informática:

La confidencialidad, la integridad y la disponibilidad. Dependiendo del tipo de sistema informático con el que tratemos (militar, comercial, bancario,...) el orden de importancia de estos tres factores es diferente, e incluso entran en juego otros elementos como la autenticidad o el no repudio. El enfoque de la política de seguridad y de los mecanismos utilizados para su implementación está influido por el más importante de los tres aspectos. Estos aspectos también pueden entenderse como metas u objetivos.

1.1.2. Confidencialidad

Se entiende por confidencialidad el servicio de seguridad, o condición, que asegura que la información no pueda estar disponible o ser descubierta para personas, entidades o procesos no autorizados. La confidencialidad, a veces denominada secreto o privacidad, se refiere a la capacidad del sistema para evitar que personas no autorizadas puedan acceder a la información almacenada en él. En áreas de seguridad gubernamentales el secreto asegura que los usuarios pueden acceder a la información que les está permitida en base a su grado o nivel de autoridad, normalmente impuestas por disposiciones legales o administrativas. En entornos de negocios, la confidencialidad asegura la protección en base a disposiciones legales o criterios estratégicos de información privada, tal como datos de las nóminas de los empleados, documentos internos sobre estrategias, nuevos productos o campañas, etc. Este aspecto de la seguridad es particularmente importante cuando hablamos de organismos públicos, y más concretamente aquellos relacionados con la defensa. En estos entornos los otros dos aspectos de la seguridad son menos

críticos. Algunos de los mecanismos utilizados para salvaguardar la confidencialidad de los datos son:

El uso de técnicas de control de acceso a los sistemas. El cifrado de la información confidencial o de las comunicaciones.

1.1.3. Integridad

Se entiende por integridad el servicio de seguridad que garantiza que la información es modificada, incluyendo su creación y borrado, sólo por el personal autorizado. Suelen integrarse varios conceptos análogos en este segundo aspecto de la seguridad: precisión, integridad, autenticidad.

El concepto de integridad significa que el sistema no debe modificar o corromper la información que almacene, o permitir que alguien no autorizado lo haga. Esta propiedad permite asegurar que no se ha falseado la información. Por ejemplo, que los datos recibidos o recuperados son exactamente los que fueron enviados o almacenados, sin que se haya producido ninguna modificación, adición o borrado. De hecho la integridad no sólo se refiere a modificaciones intencionadas, sino también a cambios accidentales o no intencionados. En el ámbito de las redes y las comunicaciones, un aspecto o variante de la integridad es la autenticidad. Se trata de proporcionar los medios para verificar que el origen de los datos es el correcto, quién los envió y cuándo fueron enviados y recibidos. En el entorno financiero o bancario, este aspecto de la seguridad es el más importante. En los bancos, cuando se realizan transferencias de fondos u otros tipos de transacciones, normalmente es más importante mantener la integridad y precisión de los datos que evitar que sean interceptados o conocidos (mantener la confidencialidad). En el campo de la criptografía hay diversos métodos para mantener asegurar la autenticidad de los mensajes y la precisión de los datos recibidos. Se usan para ello códigos y

firmas añadidos a los mensajes en origen y recalculadas comprobadas en el destino. Este método puede asegurar no sólo la integridad de los datos (lo enviado es igual a lo recibido), sino la autenticidad de la misma (quién lo envía es quien dice que es)

1.1.4. Disponibilidad

Se entiende por disponibilidad el grado en que un dato está en el lugar, momento y forma en que es requerido por el usuario autorizado. La situación que se produce cuando se puede acceder a un Sistema de Información en un espacio de tiempo considerado aceptable. Un sistema seguro debe mantener la información disponible para los usuarios. Disponibilidad significa que el sistema, tanto hardware como software, se mantienen funcionando eficientemente y que es capaz de recuperarse rápidamente en caso de fallo. Lo opuesto a disponibilidad, y uno de los posibles métodos de ataque a un sistema informático, se denomina denegación de servicio. Una denegación de servicio significa que los usuarios no puede obtener del sistema los recursos deseados: El ordenador puede estar estropeado o haber una caída del Sistema Operativo. No hay suficiente memoria para ejecutar los programas. Los discos, cintas o impresoras no están disponibles o están llenos. No se puede acceder a la información. De hecho, muchos ataques, no buscaban borrar, robar, o modificar la información, sino bloquear el sistema creando nuevos procesos que saturaban recursos.

Existen otros aspectos o características de la seguridad que pueden en su mayor parte incluirse o asimilarse a uno de los tres aspectos fundamentales, pero que es importante concretar en sí mismos.

1.1.5. Autenticidad

Esta propiedad permite asegurar el origen de la información. La identidad del emisor puede ser validada, de modo que se puede demostrar que es quien dice ser. De este modo se evita que un usuario envíe una información haciéndose pasar por otro.

1.1.6. Imposibilidad de rechazo

Esta propiedad permite asegurar que cualquier entidad que envía o recibe información, no puede alegar ante terceros que no la envió o la recibió. Esta propiedad y la anterior son especialmente importantes en el entorno bancario y en el uso del comercio digital.

1.1.7. Consistencia

Asegurar que el sistema se comporta como se supone que debe hacerlo con los usuarios autorizados. Si el software o el hardware de repente comienzan a comportarse de un modo radicalmente diferente al esperado, puede ser un desastre. Esta propiedad es amenazada por ejemplo por el uso de los Caballos de Troya. Programas que no hacen lo que se supone que deben hacer, o que además se dedican a otras tareas.

1.1.8. Aislamiento

Regula el acceso al sistema, impidiendo que personas no autorizadas entren en él. Este aspecto está relacionado directamente con la confidencialidad, aunque se centra más en el acceso al sistema que a la información que contiene.

1.2. OBJETIVOS DE CONTROL (COBIT)

Qué es COBIT (Control Objectives for Information and related Technology)

COBIT es un modelo de control dirigido a las necesidades de la Información y sus tecnologías relacionadas.

COBIT complementa a los modelos más generales como COSO (EEUU), CoCo (Canadá) o Cadbury (Inglaterra).

Provee guías detalladas sobre objetivos de control para los procesos de gestión de tecnología de información

1.2.1. La misión de COBIT

"Investigar, desarrollar, publicar y promover un conjunto de objetivos de control en tecnología de información con autoridad, actualizados, de carácter internacional y aceptado generalmente para el uso cotidiano de gerentes de empresas y auditores"[3]

1.2.2. La visión de COBIT

Ser la herramienta más avanzada para la gobernabilidad, control y auditoría de información que ayude a comprender y administrar los riesgos asociados con la información y sus tecnologías relacionadas.

1.2.3. El Marco COBIT

El marco Cobit se sustenta en que el Control de la TI se aborda considerando la información que se necesita para dar soporte a los objetivos de negocio y considerando a dicha información como resultado de la aplicación combinada

[3] COBIT, Directrices de Auditoria, 2da Edición Pág. 4

de los recursos relacionados con la TI que es preciso administrar por medio de los procesos de TI

Para satisfacer los objetivos del negocio, la información necesita concordar con ciertos criterios:

- Requisitos de Calidad:

  Calidad, Costo y Entrega (mayor calidad, a menor costo y menor plazo)

- Requisitos Fiduciarios: (Informe COSO).

  Eficacia y eficiencia de las operaciones.

  Confiabilidad de la información.

  Cumplimiento de las leyes y reglamentaciones

- Requisitos de Seguridad:

  Confidencialidad

  Integridad

  Disponibilidad

El marco referencial consta de objetivos de control de TI de alto nivel y de una estructura general para su clasificación y presentación.

Comenzando por la base, encontramos las actividades y tareas necesarias para alcanzar un resultado medible. Las actividades cuentan con un concepto de ciclo de vida, mientras que las tareas son consideradas más discretas.

Los procesos se definen entonces en un nivel superior como una serie de actividades o tareas conjuntas con “cortes” naturales (de control). Al nivel más alto, los procesos son agrupados de manera natural en dominios. Su agrupamiento natural es confirmado frecuentemente como dominios de

responsabilidad en una estructura organizacional, y está en línea con el ciclo administrativo o ciclo de vida aplicable a los procesos de TI.

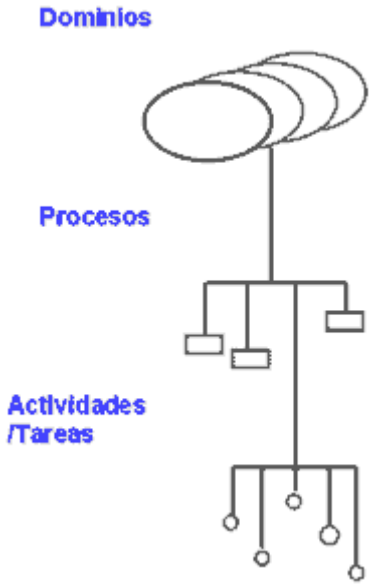

Gráfico 1.1: Procesos de TI

Por lo tanto, el marco referencial conceptual puede ser enfocado desde tres puntos estratégicos: (1) recursos de TI, (2) requerimientos de negocio para la información y (3) procesos de TI.

Gráfico 1.2: Marco referencial

Los puntos de vista diferentes permiten al marco referencial ser accedido eficientemente. Por ejemplo, los gerentes de la empresa pueden interesarse en un enfoque de calidad, seguridad o fiduciario (traducido por el marco referencial en siete requerimientos de información específicos).

Un Gerente de TI puede desear considerar recursos de TI por los cuales es responsable. Propietarios de procesos, especialistas de TI y usuarios pueden tener un interés en procesos particulares. Los auditores podrán desear enfocar el marco referencial desde un punto de vista de cobertura de control.

Estos tres puntos estratégicos son descritos en el Cubo COBIT:

Gráfico 1.3: Cubo COBIT

Con lo anterior como marco de referencia cuatro grandes dominios son identificados: planeación y organización, adquisición e implementación, entrega & soporte y monitoreo.

Las definiciones para los dominios mencionados son las siguientes:

1.2.3.1. Planeación & Organización

Este dominio cubre la estrategia y las tácticas y se refiere a la identificación de la forma en que la tecnología de información puede contribuir de la mejor manera al logro de los objetivos del negocio. Además, la consecución de la visión estratégica necesita ser planeada, comunicada y administrada desde diferentes perspectivas. Finalmente, deberán establecerse una organización y una infraestructura tecnológica apropiadas.

1.2.3.2. Adquisición & Implementación

Para llevar a cabo la estrategia de TI, las soluciones de TI deben ser identificadas, desarrolladas o adquiridas, así como implementadas e integradas dentro del proceso del negocio. Además, este dominio cubre los cambios y el mantenimiento realizados a sistemas existentes.

1.2.3.3. Entrega & Soporte

En este dominio se hace referencia a la entrega de los servicios requeridos, que abarca desde las operaciones tradicionales hasta el entrenamiento, pasando por seguridad y aspectos de continuidad. Con el fin de proveer servicios, deberán establecerse los procesos de soporte necesarios. Este dominio incluye el procesamiento de los datos por sistemas de aplicación, frecuentemente clasificados como controles de aplicación.

1.2.3.4. Monitoreo

Todos los procesos necesitan ser evaluados regularmente a través del tiempo para verificar su calidad y suficiencia en cuanto a los requerimientos de control.

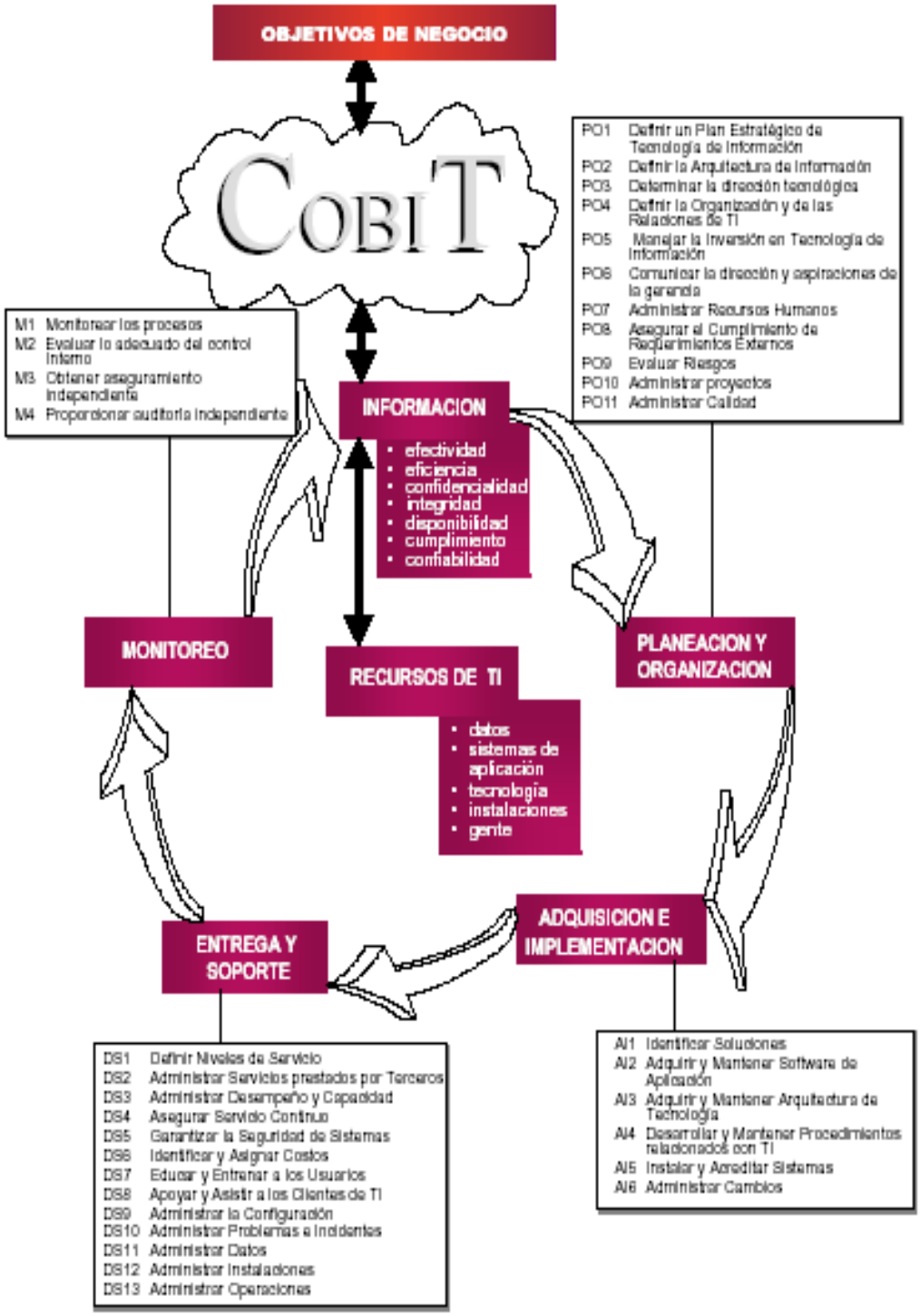

Gráfico 1.4: Dominios y Procesos de COBIT[4]

[4] COBIT, Directrices de Auditoria, 2da Edición Pág. 8

1.3. AMENAZAS CONTRA LA SEGURIDAD

Se entiende por amenaza una condición del entorno del sistema de información (persona, máquina, suceso o idea) que, dada una oportunidad, podría dar lugar a que se produjese una violación de la seguridad (confidencialidad, integridad, disponibilidad o uso legítimo). La política de seguridad y el análisis de riesgos habrán identificado las amenazas que han de ser contrarrestadas, dependiendo del diseñador del sistema de seguridad especificar los servicios y mecanismos de seguridad necesarios.

Las amenazas a la seguridad en una red pueden caracterizarse modelando el sistema como un flujo de información desde una fuente, como por ejemplo un fichero o una región de la memoria principal, a un destino, como por ejemplo otro fichero o un usuario. Un ataque no es más que la realización de una amenaza.

Las cuatro categorías generales de amenazas o ataques son las siguientes

1.3.1. Interrupción

Un recurso del sistema es destruido o se vuelve no disponible. Este es un ataque contra la disponibilidad. Ejemplos de este ataque son la destrucción de un elemento hardware, como un disco duro, cortar una línea de comunicación o deshabilitar el sistema de gestión de ficheros.

1.3.2. Intercepción

Una entidad no autorizada consigue acceso a un recurso. Este es un ataque contra la confidencialidad. La entidad no autorizada podría ser una persona, un programa o un ordenador. Ejemplos de este ataque son pinchar una línea para hacerse con datos que circulen por la red y la copia ilícita de ficheros o programas (intercepción de datos), o bien la lectura de las cabeceras de

paquetes para desvelar la identidad de uno o más de los usuarios implicados en la comunicación observada ilegalmente (intercepción de identidad).

1.3.3. Modificación

Una entidad no autorizada no sólo consigue acceder a un recurso, sino que es capaz de manipularlo. Este es un ataque contra la integridad. Ejemplos de este ataque son el cambio de valores en un archivo de datos, alterar un programa para que funcione de forma diferente y modificar el contenido de mensajes que están siendo transferidos por la red.

1.3.4. Fabricación

Una entidad no autorizada inserta objetos falsificados en el sistema. Este es un ataque contra la autenticidad. Ejemplos de este ataque son la inserción de mensajes espurios en una red o añadir registros a un archivo.

Estos ataques se pueden asimismo clasificar de forma útil en términos de ataques pasivos y ataques activos.

1.3.5. Ataques pasivos

En los ataques pasivos el atacante no altera la comunicación, sino que únicamente la escucha o monitoriza, para obtener información que está siendo transmitida. Sus objetivos son la intercepción de datos y el análisis de tráfico, una técnica más sutil para obtener información de la comunicación, que puede consistir en:

- Obtención del origen y destinatario de la comunicación, leyendo las cabeceras de los paquetes monitorizados.
- Control del volumen de tráfico intercambiado entre las entidades monitorizadas, obteniendo así información acerca de actividad o inactividad inusuales.

- Control de las horas habituales de intercambio de datos entre las entidades de la comunicación, para extraer información acerca de los períodos de actividad.

Los ataques pasivos son muy difíciles de detectar, ya que no provocan ninguna alteración de los datos. Sin embargo, es posible evitar su éxito mediante el cifrado de la información.

1.3.6. Ataques activos

Estos ataques implican algún tipo de modificación del flujo de datos transmitido o la creación de un falso flujo de datos, pudiendo subdividirse en cuatro categorías:

1.3.6.1. Suplantación de identidad

El intruso se hace pasar por una entidad diferente. Normalmente incluye alguna de las otras formas de ataque activo. Por ejemplo, secuencias de autenticación pueden ser capturadas y repetidas, permitiendo a una entidad no autorizada acceder a una serie de recursos privilegiados suplantando a la entidad que posee esos privilegios, como al robar la contraseña de acceso a una cuenta.

1.3.6.2. Reactuación

Uno o varios mensajes legítimos son capturados y repetidos para producir un efecto no deseado, como por ejemplo ingresar dinero repetidas veces en una cuenta dada.

1.3.6.3. Modificación de mensajes

Una porción del mensaje legítimo es alterada, o los mensajes son retardados o reordenados, para producir un efecto no autorizado. Por ejemplo, el mensaje “Ingresa un millón de pesetas en la cuenta A” podría ser modificado para decir “Ingresa un millón de pesetas en la cuenta B”.

1.3.6.4. Degradación fraudulenta del servicio

Impide o inhibe el uso normal o la gestión de recursos informáticos y de comunicaciones. Por ejemplo, el intruso podría suprimir todos los mensajes dirigidos a una determinada entidad o se podría interrumpir el servicio de una red inundándola con mensajes espurios. Entre estos ataques se encuentran los de denegación de servicio, consistentes en paralizar temporalmente el servicio de un servidor de correo, Web, FTP, etc.

1.4. DELITOS INFORMÁTICOS

El delito informático implica actividades criminales que en un primer momento los países han tratado de encuadrar en figuras típicas de carácter tradicional, tales como robos o hurto, fraudes, falsificaciones, perjuicios, estafa, sabotaje, etcétera. Sin embargo, debe destacarse que el uso de las técnicas informáticas ha creado nuevas posibilidades del uso indebido de las computadoras lo que ha propiciado a su vez la necesidad de regulación por parte del derecho.

A nivel internacional se considera que no existe una definición propia del delito informático, sin embargo muchos han sido los esfuerzos de expertos que se han ocupado del tema, y aún cuando no existe una definición con carácter universal, se han formulado conceptos funcionales atendiendo a realidades nacionales concretas.

"No es labor fácil dar un concepto sobre delitos informáticos, en razón de que su misma denominación alude a una situación muy especial, ya que para hablar de "delitos" en el sentido de acciones típicas, es decir tipificadas o contempladas en textos jurídicos penales, se requiere que la expresión "delitos informáticos" esté consignada en los códigos penales, lo cual en nuestro país, al igual que en otros muchos no ha sido objeto de tipificación aún"[5]

Para Carlos Sarzana, en su obra 'Criminalità e tecnología', los crímenes por computadora comprenden "cualquier comportamiento criminógeno en el cual la computadora ha estado involucrada como material o como objeto de la acción criminógena, o como mero símbolo".

Nidia Callegari define al delito informático como "aquel que se da con la ayuda de la informática o de técnicas anexas".

[5]Télles Valdez, Julio. Derecho Informático. 2º Edición. MC Graw Hill. México. Pág. 103-104

Rafael Fernández Calvo define al delito informático como "la realización de una acción que, reuniendo las características que delimitan el concepto de delito, se ha llevado a cabo utilizando un elemento informático o telemático contra los derechos y libertades de los ciudadanos.

María de la Luz Lima dice que el delito electrónico "en un sentido amplio es cualquier conducta criminógena o criminal que en su realización hace uso de la tecnología electrónica ya sea como método, medio o fin y que, en un sentido estricto, el delito informático, es cualquier acto ilícito penal en el que las computadoras, sus técnicas y funciones desempeñan un papel ya sea como método, medio o fin"[6]

Julio Téllez Valdes conceptualiza al delito informático en forma típica y atípica, entendiendo por la primera a " las conductas típicas, antijurídicas y culpables en que se tienen a las computadoras como instrumento o fin" y por las segundas "actitudes ilícitas en que se tienen a las computadoras como instrumento o fin".

Por otra parte, debe mencionarse que se han formulado diferentes denominaciones para indicar las conductas ilícitas en las que se usa la computadora, tales como "delitos informáticos", "delitos electrónicos", "delitos relacionados con las computadoras", "crímenes por computadora". "delincuencia relacionada con el ordenador".

En este orden de ideas, en el presente trabajo se entenderán como "delitos informáticos" todas aquellas conductas ilícitas susceptibles de ser sancionadas por el derecho penal, que hacen uso indebido de cualquier medio informático.

Clasificación.- Julio Téllez Valdes clasifica a los delitos informáticos en base a dos criterios: como instrumento o medio, o como fin u objetivo.

[6] LIMA de la LUZ, Maria. Criminalia Nº 1-6 Año L. Delitos Electrónicos. Ediciones. Porrua.

Como instrumento o medio: Se tienen a las conductas criminógenas que se valen de las computadoras como método, medio, o símbolo en la comisión del ilícito.

Como fin u objetivo: En esta categoría se enmarcan las conductas criminógenas que van dirigidas en contra de la computadora, accesorios o programas como entidad física.

María de la Luz Lima, presenta una clasificación, de lo que ella llama "delitos electrónicos", diciendo que existen tres categorías, a saber:

- Los que utilizan la tecnología electrónica como método,
- Los que utilizan la tecnología electrónica como medio y
- Los que utilizan la tecnología electrónica como fin.

Como método- conductas criminógenas en donde los individuos utilizan métodos electrónicos para llegar a un resultado ilícito.

Como medio.- conductas criminógenas en donde para realizar un delito utilizan una computadora como medio o símbolo.

Como fin.- conductas criminógenas dirigidas contra la entidad física del objeto o máquina electrónica o su material con objeto de dañarla.

1.4.1. Tipos de delitos informáticos

Tipos de delitos informáticos:

1.4.1.1. Fraudes cometidos mediante manipulación de computadoras.

1.4.1.1.1. Manipulación de los datos de entrada

Este tipo de fraude informático conocido también como sustracción de datos, representa el delito informático más común ya que es fácil de cometer y difícil de descubrir. Este delito no requiere de conocimientos técnicos de informática y puede realizarlo cualquier persona que tenga acceso a las funciones normales de procesamiento de datos en la fase de adquisición de los mismos.

1.4.1.1.2. La manipulación de programas

Es muy difícil de descubrir y a menudo pasa inadvertida debido a que el delincuente debe tener conocimientos técnicos concretos de informática. Este delito consiste en modificar los programas existentes en el sistema de computadoras o en insertar nuevos programas o nuevas rutinas. Un método común utilizado por las personas que tienen conocimientos especializados en programación informática es el denominado Caballo de Troya, que consiste en insertar instrucciones de computadora de forma encubierta en un programa informático para que pueda realizar una función no autorizada al mismo tiempo que su función normal.

1.4.1.1.3. Manipulación de los datos de salida

Se efectúa fijando un objetivo al funcionamiento del sistema informático. El ejemplo más común es el fraude de que se hace objeto a los cajeros automáticos mediante la falsificación de instrucciones para la computadora en la fase de adquisición de datos. Tradicionalmente esos fraudes se hacían a base de tarjetas bancarias robadas, sin embargo, en la actualidad se usan ampliamente equipo y programas de computadora especializados para codificar información electrónica falsificada en las bandas magnéticas de las tarjetas bancarias y de las tarjetas de crédito.

1.4.1.1.4. Fraude efectuado por manipulación informática

Aprovecha las repeticiones automáticas de los procesos de cómputo. Es una técnica especializada que se denomina "técnica del salchichón" en la que "rodajas muy finas" apenas perceptibles, de transacciones financieras, se van sacando repetidamente de una cuenta y se transfieren a otra.

1.4.2. Falsificaciones informáticas.

1.4.2.1. Como objeto

Cuando se alteran datos de los documentos almacenados en forma computarizada.

1.4.2.2. Como instrumentos

Las computadoras pueden utilizarse también para efectuar falsificaciones de documentos de uso comercial. Cuando empezó a disponerse de fotocopiadoras computarizadas en color a base de rayos láser surgió una nueva generación de falsificaciones o alteraciones fraudulentas. Estas fotocopiadoras pueden hacer copias de alta resolución, pueden modificar documentos e incluso pueden crear documentos falsos sin tener que recurrir a un original, y los documentos que producen son de tal calidad que sólo un experto puede diferenciarlos de los documentos auténticos.

1.4.3. Daños o modificaciones de programas o datos computarizados.

1.4.3.1. Sabotaje informático

Es el acto de borrar, suprimir o modificar sin autorización funciones o datos de computadora con intención de obstaculizar el funcionamiento normal del sistema. Las técnicas que permiten cometer sabotajes informáticos son:

1.4.3.2. Virus

Es una serie de claves programáticas que pueden adherirse a los programas legítimos y propagarse a otros programas informáticos. Un virus puede ingresar en un sistema por conducto de una pieza legítima de soporte lógico que ha quedado infectada, así como utilizando el método del Caballo de Troya.

1.4.3.3. Gusanos

Se fabrica de forma análoga al virus con miras a infiltrarlo en programas legítimos de procesamiento de datos o para modificar o destruir los datos, pero es diferente del virus porque no puede regenerarse. En términos médicos podría decirse que un gusano es un tumor benigno, mientras que el virus es un tumor maligno. Ahora bien, las consecuencias del ataque de un gusano pueden ser tan graves como las del ataque de un virus: por ejemplo, un programa gusano que subsiguientemente se destruirá puede dar instrucciones a un sistema informático de un banco para que transfiera continuamente dinero a una cuenta ilícita.

1.4.3.4. Bomba lógica o cronológica

Exige conocimientos especializados ya que requiere la programación de la destrucción o modificación de datos en un momento dado del futuro. Ahora bien, al revés de los virus o los gusanos, las bombas lógicas son difíciles de detectar antes de que exploten; por eso, de todos los dispositivos informáticos criminales, las bombas lógicas son las que poseen el máximo potencial de daño. Su detonación puede programarse para que cause el máximo de daño y para que tenga lugar mucho tiempo después de que se haya marchado el delincuente. La bomba lógica puede utilizarse también como instrumento de extorsión y se puede pedir un rescate a cambio de dar a conocer el lugar en donde se halla la bomba.

1.4.3.5. Acceso no autorizado a servicios y sistemas informáticos

Por motivos diversos: desde la simple curiosidad, como en el caso de muchos piratas informáticos (hackers) hasta el sabotaje o espionaje informático.

1.4.3.6. Piratas informáticos o hackers

El acceso se efectúa a menudo desde un lugar exterior, situado en la red de telecomunicaciones, recurriendo a uno de los diversos medios que se mencionan a continuación. El delincuente puede aprovechar la falta de rigor de las medidas de seguridad para obtener acceso o puede descubrir deficiencias en las medidas vigentes de seguridad o en los procedimientos del sistema. A menudo, los piratas informáticos se hacen pasar por usuarios legítimos del sistema; esto suele suceder con frecuencia en los sistemas en los que los usuarios pueden emplear contraseñas comunes o contraseñas de mantenimiento que están en el propio sistema.

1.4.3.7. Reproducción no autorizada de programas informáticos de protección legal

Esta puede entrañar una pérdida económica sustancial para los propietarios legítimos. Algunas jurisdicciones han tipificado como delito esta clase de actividad y la han sometido a sanciones penales. El problema ha alcanzado dimensiones transnacionales con el tráfico de esas reproducciones no autorizadas a través de las redes de telecomunicaciones modernas. Al respecto, consideramos, que la reproducción no autorizada de programas informáticos no es un delito informático debido a que el bien jurídico a tutelar es la propiedad intelectual.

1.5. POLÍTICAS DE SEGURIDAD INFORMÁTICA

La seguridad informática ha tomado gran auge, debido a las cambiantes condiciones y nuevas plataformas tecnológicas disponibles. La posibilidad de interconectarse a través de redes, ha abierto nuevos horizontes a las empresas para mejorar su productividad y poder explorar más allá de las fronteras nacionales, lo cual lógicamente ha traído consigo, la aparición de nuevas amenazas para los sistemas de información.

Estos riesgos que se enfrentan han llevado a que muchas organizaciones desarrollen documentos y directrices que orientan en el uso adecuado de estas destrezas tecnológicas y recomendaciones para obtener el mayor provecho de estas ventajas, y evitar el uso indebido de las mismas, lo cual puede ocasionar serios problemas a los bienes, servicios y operaciones de la empresa.

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

“Una política de seguridad es un conjunto de requisitos definidos por los responsables de un sistema, que indica en términos generales que está y no

está permitido en el área de seguridad durante la operación general del sistema"[7]

La RFC (Request for Comment) 1244 define Política de Seguridad como: "una declaración de intenciones de alto nivel que cubre la seguridad de los sistemas informáticos y que proporciona las bases para definir y delimitar responsabilidades para las diversas actuaciones técnicas y organizativas que se requerirán."[8]

Una política de seguridad informática es una forma de comunicarse con los usuarios, ya que las mismas establecen un canal formal de actuación del personal, en relación con los recursos y servicios informáticos de la organización.

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

[7] HUERTA, Antonio Villalón. Seguridad de Unix y Redes. (Versión 1.2) Capitulo 16-Página 259
[8] RFC 1244: Site Security Handbook. J. Reinolds. – P. Holbrook.

1.5.1. Metodología para la elaboración de políticas de seguridad

Esta metodología es potencialmente útil para el desarrollo, implementación, mantenimiento y eliminación de un conjunto completo de políticas – tanto de seguridad como en otras áreas.

Es frecuente que las personas involucradas con seguridad informática tengan una visión estrecha de lo que significa desarrollar las políticas de seguridad, pues no basta con escribirlas y pretender ponerlas en práctica. En ocasiones se incluye la asignación de responsables, se realizan actividades para dar a conocerlas y, quizá, se supervise su cumplimiento; pero esto tampoco basta. Muchas políticas de seguridad informática fallan ya que se desconoce lo que implica realmente desarrollarlas. Es importante resaltar que una política de seguridad tiene un ciclo de vida completo mientras esta vigente. Este ciclo de vida incluye un esfuerzo de investigación, la labor de escribirla, lograr que las directivas de la organización la acepten, conseguir que sea aprobada, lograr que sea diseminada a través de la empresa, concienciar a los usuarios de la importancia de la política, conseguir que la acaten, hacerle seguimiento, garantizar que esté actualizada y, finalmente, suprimirla cuando haya perdido vigencia. Si no se tiene en cuenta este ciclo de vida se corre el riesgo de desarrollar políticas que sean poco tenidas en cuenta, incompletas, redundantes, sin apoyo por parte de los usuarios y las directivas, superfluas o irrelevantes.

1.5.2. POR QUÉ TENER POLÍTICAS ESCRITAS

Existen varias razones por las cuales es recomendable tener políticas escritas en una organización como la Coac. Alianza del Valle. La siguiente es una lista de algunas de estas razones.

- Para cumplir con regulaciones legales o técnicas
- Como guía para el comportamiento profesional y personal
- Permite unificar la forma de trabajo de personas en diferentes lugares o momentos que tengan responsabilidades y tareas similares
- Permiten recoger comentarios y observaciones que buscan atender situaciones anormales en el trabajo
- Permite encontrar las mejores prácticas en el trabajo
- Permiten asociar la filosofía de una organización (lo abstracto) al trabajo (lo concreto)

1.5.3. Fases en el desarrollo de una política

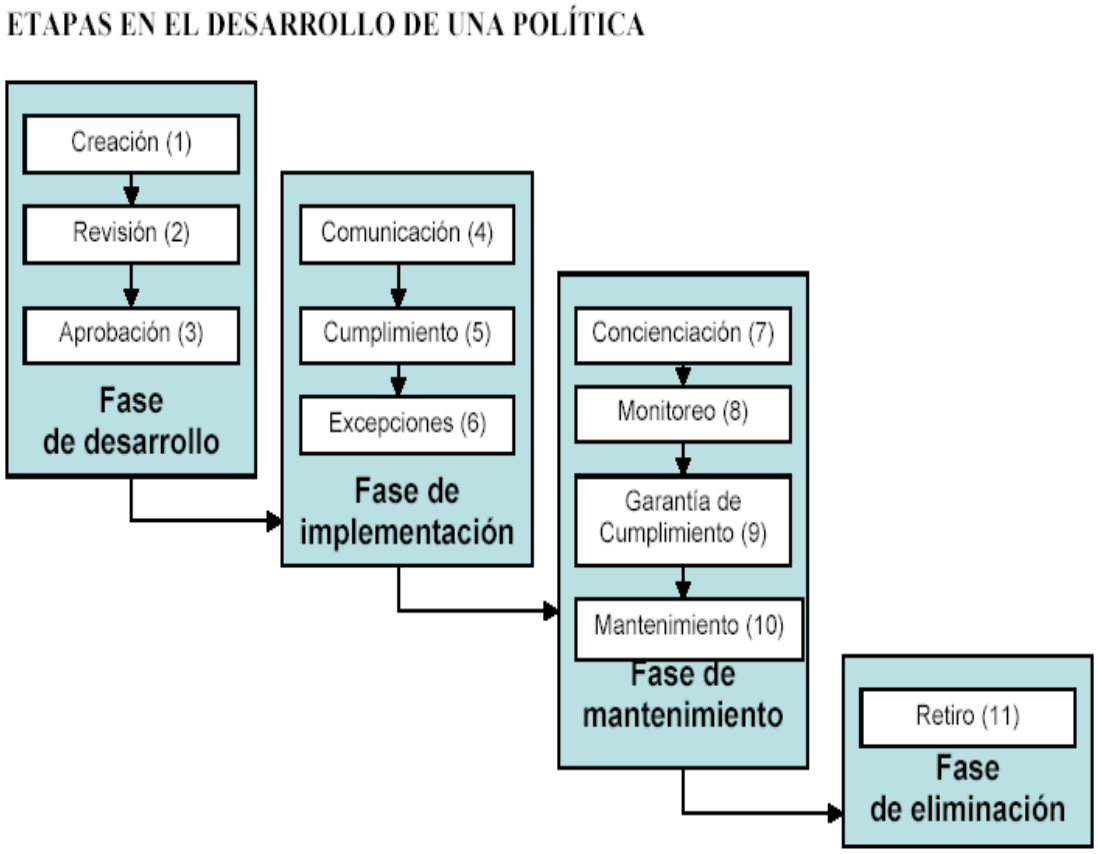

Gráfico 1.5: Fases en el Desarrollo de una Política[9]

[9] Guía para la elaboración de Políticas de Seguridad 2003 Pág. 3, Universidad Nacional de Colombia

Hay 11 etapas que deben realizarse a través de “la vida” de una política. Estas 11 etapas pueden ser agrupadas en 4 fases.

1.5.3.1. Fase de desarrollo

Durante esta fase la política es creada, revisada y aprobada.

1.5.3.1.1. Creación

El primer paso en la fase de desarrollo de una política es la planificación, la investigación y la redacción de la política o, tomado todo junto, la creación. La creación de una política implica identificar por qué se necesita la política (por ejemplo, requerimientos legales, regulaciones técnicas, contractuales u operacionales); determinar el alcance y la aplicabilidad de la política, los roles y las responsabilidades inherentes a la aplicación de la política y garantizar la factibilidad de su implementación. La creación de una política también incluye la investigación para determinar los requerimientos organizacionales para desarrollar las políticas (es decir, que autoridades deben aprobarla, con quién se debe coordinar el desarrollo y estándares del formato de redacción), y la investigación de las mejores prácticas en la industria para su aplicabilidad a las necesidades organizacionales actuales. De esta etapa se tendrá como resultado la documentación de la política de acuerdo con los procedimientos y estándares de la cooperativa, al igual que la coordinación con entidades internas y externas que la política afectará, para obtener información y su aceptación. En general, la creación de una política es la función más fácil de entender en el ciclo de vida de desarrollo de una política.

1.5.3.1.2. Revisión

La revisión de la política es la segunda etapa en la fase de desarrollo del ciclo de vida. Una vez la documentación de la política ha sido creada y la coordinación inicial ha sido iniciada, esta debe ser remitida a un grupo (o un

individuo) independiente para su evaluación antes de su aprobación final. Hay varios beneficios de la revisión independiente: una política más viable a través del escrutinio de individuos que tienen una perspectiva diferente o más vasta que la persona que redactó la política; apoyo más amplio para la política a través de un incremento en el número de involucrados; aumento de credibilidad en la política gracias a la información recibida de diferentes especialistas del grupo de revisión. Propio de esta etapa es la presentación de la política a los revisores, ya sea de manera formal o informal, exponiendo cualquier punto que puede ser importante para la revisión, explicando su objetivo, el contexto y los beneficios potenciales de la política y justificando por qué es necesaria. Como parte de esta función, se espera que el creador de la política recopile los comentarios y las recomendaciones para realizar cambios en la política y efectuar todos los ajustes y las revisiones necesarias para obtener una versión final de la política lista para la aprobación por las directivas.

1.5.3.1.3. Aprobación

El paso final en la fase de desarrollo de la política es la aprobación. El objetivo de esta etapa es obtener el apoyo de la administración de la cooperativa, a través de la firma de una persona ubicada en una posición de autoridad.

La aprobación permite iniciar la implementación de la política. Requiere que el proponente de la política haga una selección adecuada de la autoridad de aprobación, que coordine con dicho funcionario, presente las recomendaciones emitidas durante la etapa de revisión y haga el esfuerzo para que sea aceptada por la administración. Puede ocurrir que por incertidumbre de la autoridad de aprobación sea necesaria una aprobación temporal.

1.5.3.2. Fase de implementación

En esta fase la política es comunicada y acatada (o no cumplida por alguna excepción).

1.5.3.2.1. Comunicación

Una vez la política ha sido aprobada formalmente, se pasa a la fase de implementación. La comunicación de la política es la primera etapa que se realiza en esta fase. La política debe ser inicialmente difundida a los empleados de la cooperativa o a quienes sean afectados directamente por la política (contratistas, proveedores, usuarios de cierto servicio, etc.). Esta etapa implica determinar el alcance y el método inicial de distribución de la política (es posible que deban tenerse en cuenta factores como la ubicación geográfica, el idioma, la cultura y línea de mando que será utilizada para comunicar la política). Debe planificarse esta etapa con el fin de determinar los recursos necesarios y el enfoque que debe ser seguido para mejorar la visibilidad de la política.

1.5.3.2.2. Cumplimiento

La etapa de cumplimiento incluye actividades relacionadas con la ejecución de la política. Implica trabajar con otras personas de la cooperativa, Presidente, Directorio y los jefes de agencia para interpretar cuál es la mejor manera de implementar la política en diversas situaciones y oficinas; asegurando que la política es entendida por aquellos que requieren implementarla, monitorearla, hacerle seguimiento, reportar regularmente su cumplimiento y medir el impacto inmediato de la política en las actividades operativas. Dentro de estas actividades está la elaboración de informes a la administración del estado de la implementación de la política.

1.5.3.2.3. Excepciones

Debido a problemas de coordinación, falta de personal y otros requerimientos operacionales, no todas las políticas pueden ser cumplidas de la manera que se pensó al comienzo. Por esto, cuando los casos lo ameriten, es probable que se requieran excepciones a la política para permitir a ciertas oficinas o personas el no cumplimiento de la política.

Debe establecerse un proceso para garantizar que las solicitudes de excepciones son registradas, seguidas, evaluadas, enviadas para aprobación o desaprobación, documentadas y vigiladas a través del periodo de tiempo establecido para la excepción. El proceso también debe permitir excepciones permanentes a la política al igual que la no aplicación temporal por circunstancias de corta duración.

1.5.3.3. Fase de mantenimiento

Los usuarios deben ser concientes de la importancia de la política, su cumplimiento debe ser monitoreado, se debe garantizar su cumplimiento y se le debe dar mantenimiento (actualizarla).

1.5.3.3.1. Concienciación

La etapa de concienciación de la fase de mantenimiento comprende los esfuerzos continuos realizados para garantizar que las personas están concientes de la política y buscan facilitar su cumplimiento. Esto es hecho al definir las necesidades de concienciación de los diversos grupos de audiencia dentro de la organización (directivos, jefes de agencias, usuarios, etc.); en relación con la adherencia a la política, determinar los métodos de concienciación más efectivos para cada grupo de audiencia (es decir, reuniones informativas, cursos de entrenamiento, mensajes de correo, etcétera); y desarrollo y difusión de material de concienciación (presentaciones,

afiches, circulares, etc.). La etapa de concienciación también incluye esfuerzos para integrar el cumplimiento de la política y retroalimentación sobre el control realizado para su cumplimiento. La tarea final es medir la concienciación de los miembros de la cooperativa con la política y ajustar los esfuerzos de acuerdo con los resultados de las actividades medidas.

1.5.3.3.2. Monitoreo

Durante la fase de mantenimiento, la etapa de monitoreo es realizada para seguir y reportar la efectividad de los esfuerzos en el cumplimiento de la política. Esta información se obtiene de la observación de los jefes de agencia, empleados y los cargos de supervisión, mediante auditorias formales, evaluaciones, inspecciones, revisiones y análisis de los reportes de contravenciones y de las actividades realizadas en respuesta a los incidentes.

Esta etapa incluye actividades continuas para monitorear el cumplimiento o no de la política a través de métodos formales e informales y el reporte de las deficiencias encontradas a las autoridades apropiadas.

1.5.3.3.3. Garantía de cumplimiento

La etapa de garantía de cumplimiento de las políticas incluye las respuestas de la administración a actos u omisiones que tengan como resultado contravenciones de la política con el fin de prevenir que sigan ocurriendo. Esto significa que una vez una contravención sea identificada, la acción correctiva debe ser determinada y aplicada a los procesos (revisión del proceso y mejoramiento), a la tecnología (actualización) y a las personas (acción disciplinaria) involucrados en la contravención con el fin de reducir la probabilidad de que vuelva a ocurrir. Se recomienda incluir información sobre las acciones correctivas adelantadas para garantizar el cumplimiento en la etapa de concienciación.

1.5.3.3.4. Mantenimiento

La etapa de mantenimiento esta relacionada con el proceso de garantizar la vigencia y la integridad de la política. Esto incluye hacer seguimiento a las tendencias de cambios (cambios en la tecnología, en los procesos, en las personas, en la organización, en el enfoque del negocio, etcétera) que puede afectar la política; recomendando y coordinando modificaciones resultado de estos cambios, documentándolos en la política y registrando las actividades de cambio. Esta etapa también garantiza la disponibilidad continuada de la política para todas las partes afectadas por ella, al igual que el mantenimiento de la integridad de la política a través de un control de versiones efectivo. Cuando se requieran cambios a la política, las etapas realizadas antes deben ser re-visitadas, en particular las etapas de revisión, aprobación, comunicación y garantía de cumplimiento.

1.5.3.4. Fase de eliminación

La política se retira cuando no se requiera más.

1.5.3.4.1. Retiro

Después que la política ha cumplido con su finalidad y no es necesaria (por ejemplo, la empresa cambió la tecnología a la cual aplicaba o se creó una nueva política que la reemplazó) entonces debe ser retirada. La etapa de retiro corresponde a la fase de eliminación del ciclo de vida de la política, y es la etapa final del ciclo. Esta función implica retirar una política superflua del inventario de políticas activas para evitar confusión, archivarla para futuras referencias y documentar la información sobre la decisión de retirar la política (es decir, la justificación, quién autorizó, la fecha, etcétera).

Estas cuatro fases del ciclo de vida reúnen 11 etapas diferentes que deben seguirse durante el ciclo de vida de una política específica. No importa como se agrupen, tampoco importa si estas etapas son abreviadas por necesidades de inmediatez, pero cada etapa debe ser realizada. Si en la fase de desarrollo la cooperativa intenta crear una política sin una revisión independiente, se tendrán políticas que no estarán bien concebidas ni serán bien recibidas por los empleados. En otras circunstancias, y por falta de visión, puede desearse omitir la etapa de excepciones de la fase de implementación, pensando equivocadamente que no existirán circunstancias para su no cumplimiento. También se podría descuidar la etapa de mantenimiento, olvidando la importancia de mantener la integridad y la vigencia de las políticas. Muchas veces se encuentran políticas inoficiosas en los documentos de importantes organizaciones, indicando que la etapa de retiro no está siendo realizada.

No sólo se requiere que las once etapas sean realizadas, algunas de ellas deben ser ejecutadas de manera cíclica, en particular mantenimiento, concienciación, monitoreo, y garantía de cumplimiento.

1.5.4. Algunas prácticas recomendadas para escribir una política

Sin importar que una política se enuncie formal o informalmente, esta debe incluir 12 tópicos:

- La declaración de la política (cuál es la posición de la administración o qué es lo que se desea regular)
- Nombre y cargo de quien autoriza o aprueba la política
- Nombre de la dependencia, del grupo o de la persona que es el autor o el proponente de la política
- Debe especificarse quién debe acatar la política (es decir, a quién está dirigida) y quién es el responsable de garantizar su cumplimiento

- Indicadores para saber si se cumple o no la política
- Referencias a otras políticas y regulaciones en las cuales se soporta o con las cuales tiene relación
- Enunciar el proceso para solicitar excepciones
- Describir los pasos para solicitar cambios o actualizaciones a la política
- Explicar qué acciones se seguirán en caso de contravenir la política
- Fecha a partir de la cual tiene vigencia la política
- Fecha cuando se revisará la conveniencia y la obsolescencia de la política
- Incluir la dirección de correo electrónico, la página web y el teléfono de la persona o personas que se pueden contactar en caso de preguntas o sugerencias

Otras prácticas que se recomiendan seguir son:

- Uso de lenguaje sencillo (evitar lenguaje técnico hasta donde sea posible)
- Escribir la política como si fuese a utilizarse siempre
- Debe escribirse de tal forma que pueda leerlo cualquier miembro de la cooperativa
- Se debe evitar describir técnicas o métodos particulares que definan una sola forma de hacer las cosas cuando se requiera, hacer referencia explicita y clara a otras dependencias de la organización
- Utilizar la guía para la presentación de documentos escritos de la cooperativa

1.5.5. Aspectos importantes para definir responsabilidades en el desarrollo de políticas

En muchas ocasiones se asume que la función seguridad informática –ya sea un grupo o un individuo- sea la encargada de adelantar la gran mayoría de las etapas en el ciclo de vida de una política y que también actúe como el proponente para la mayoría de las políticas relacionadas con la protección de los activos informáticos. Por diseño, la función seguridad informática tiene la responsabilidad a largo plazo y debe ejecutar las tareas diarias para asegurar los activos de información y por tanto, debe ser el dueño y debe ejercer control centralizado sobre las POLÍTICAS, ESTÁNDARES, MEJORES PRÁCTICAS, PROCEDIMIENTOS Y GUÍAS relacionados con seguridad informática.

Pero en ningún caso la función seguridad informática debe ser el proponente de todas las políticas relacionadas con seguridad, ni tampoco debe realizar todas las etapas de desarrollo en el ciclo de vida de la política. Por ejemplo, los dueños de los sistemas de información deben tener la responsabilidad para establecer los requerimientos necesarios para implementar las políticas de la cooperativa para sus propios sistemas. Cuando existan requerimientos de seguridad en cierta dependencia que deben cumplir con políticas de nivel superior, su proponente debe ser la dependencia que tiene interés en garantizar la efectividad de dicha política.

Aunque el proponente o dueño de una política tiene una responsabilidad continúa sobre el ciclo de vida completo de la política, hay varios factores que influyen sobre la determinación y la decisión de quién o qué dependencia tienen responsabilidad directa para realizar etapas específicas del ciclo de vida de la política en una organización. Entre estos factores se incluyen:

Separación de tareas. El principio de separación de tareas debe ser aplicado para determinar la responsabilidad de una etapa en particular para garantizar que los chequeos y ajustes necesarios sean aplicados. Para proveer una perspectiva más amplia y diferente, un directivo, o un grupo que sea independiente del proponente, deben revisar la política y una directiva, superior al proponente, debe encargarse de aprobar la política. O, para disminuir los posibles conflictos de intereses, la función auditoria (o control interno), como oficina independiente dentro de la organización, debe ser encargada del monitoreo del cumplimiento de la política, en tanto que grupos u organizaciones de auditoria externos deben ser invitados a realizar una evaluación independiente del cumplimiento de las políticas para ser consistentes con el principio de separación de tareas.

Eficiencia. Adicionalmente, por razones de eficiencia, dependencias diferentes a la proponente deben tener alguna responsabilidad para la realización de ciertas etapas del ciclo de vida del desarrollo de una política. Por ejemplo, la difusión y la comunicación de la política sería mejor realizada si se encomendara a la dependencia encargada de estas funciones dentro de la organización (por ejemplo, la Secretaría General, las Secretarías de las sucursales). Por otra parte, basados en la eficiencia, los esfuerzos de concienciación serían asignados a la función capacitación de la cooperativa -aún cuando puede ocurrir que el personal de capacitación no esté entrenado específicamente en la labor de la concienciación de la política de seguridad-. En este último caso, sería mejor que la desarrollara la función de seguridad informática.

Alcance del control. Límites en el alcance del control que la dependencia proponente puede ejercer tiene impacto sobre quién debe ser el ponente de

una política específica. Normalmente, el proponente sólo puede jugar un papel limitado en el monitoreo y en la garantía del cumplimiento de la política debido a que él no puede estar en todos lo sitios, en todo momento, donde ésta debe ser implementada. El gerente, jefes de agencia, jefes de departamento, están cerca de las personas (empleados) a quienes afecta la política de seguridad y por tanto están en una mejor posición para monitorear de manera efectiva y garantizar el cumplimiento de la política. Por tanto deben asumir la responsabilidad de estas etapas. Estos funcionarios pueden garantizar que la política está siendo seguida y que las contravenciones se manejan de manera adecuada.

Autoridad. Límites en la autoridad que un individuo o una dependencia ejerce, puede determinar la habilidad para desarrollar exitosamente una etapa del ciclo de vida de una política. La efectividad de una política, a menudo, puede ser juzgada por su visibilidad y el énfasis que la administración de la cooperativa coloque. La efectividad de una política, en muchos casos, depende de la autoridad en la cual la política se soporta. Para que una política tenga un soporte en toda la organización, el directivo que la aprueba debe tener un reconocido grado de autoridad sobre una gran parte de la cooperativa. Normalmente, la función de seguridad informática de la organización no goza del nivel de reconocimiento ideal a través de toda la organización y requiere el soporte de directivas de nivel superior para cumplir con su misión. En consecuencia, la aceptación y el cumplimiento de las políticas de seguridad informática tienen mayor probabilidad de darse cuando la autoridad que la aprueba es de nivel superior.

Conocimiento. La ubicación del proponente en la cooperativa puede inducir a deficiencias en el conocimiento del entorno en el cual la política será

implementada, entorpeciendo su efectividad. El empleo de un comité que realice la evaluación de políticas puede ofrecer un entendimiento más amplio de las operaciones que afectará la política. Un organismo de este tipo puede ayudar a garantizar que la política sea escrita con el fin de promover su aceptación y su implementación exitosa y puede ser útil para prever problemas de implementación y para evaluar efectivamente situaciones donde las excepciones a la política pueden ser justificadas.

Aplicabilidad. Finalmente, la aplicabilidad de la política también afecta la responsabilidad en las etapas de desarrollo del ciclo de vida de la política. ¿Qué áreas de la cooperativa son afectadas por la política? ¿La política aplica a una sola agencia, sólo a los usuarios de una tecnología en particular o a toda la cooperativa? Si la aplicabilidad de una política está limitada a una sola agencia, entonces la jefatura de la agencia debe tener su propia política. Sin embargo, si la política es aplicable a toda la cooperativa, entonces una dependencia de alto nivel debe asumir la responsabilidad en relación con la política.

1.6. PLAN DE CONTINGENCIA

A medida que las empresas se han vuelto cada vez más dependientes de las computadoras y las redes para manejar sus actividades, la disponibilidad de los sistemas informáticos se ha vuelto crucial. Actualmente, la mayoría de las empresas necesitan un nivel alto de disponibilidad y algunas requieren incluso un nivel continuo de disponibilidad, ya que les resultaría extremadamente difícil funcionar sin los recursos informáticos.

Los procedimientos manuales, si es que existen, sólo serían prácticos por un corto periodo. En caso de un desastre, la interrupción prolongada de los servicios de computación puede llevar a pérdidas financieras significativas, sobre todo si está implicada la responsabilidad de la gerencia de informática. Lo más grave es que se puede perder la credibilidad del público o los clientes y, como consecuencia, la empresa puede terminar en un fracaso total. Cabe preguntarse "¿Por se necesita un plan de contingencia para desastres si existe una póliza de seguro para esta eventualidad?" La respuesta es que si bien el seguro puede cubrir los costos materiales de los activos de una organización en caso de una calamidad, no servirá para recuperar el negocio. No ayudará a conservar a los clientes y, en la mayoría de los casos, no proporcionará fondos por adelantado para mantener funcionando el negocio hasta que se haya recuperado.

En un estudio realizado por la Universidad de Minnesota, se ha demostrado que más del 60% de las empresas que sufren un desastre y que no tienen un plan de recuperación ya en funcionamiento, saldrán del negocio en dos o tres años. Mientras vaya en aumento la dependencia de la disponibilidad de los recursos informáticos, este porcentaje seguramente crecerá.

Por lo tanto, la capacidad para recuperarse exitosamente de los efectos de un desastre dentro de un periodo predeterminado debe ser un elemento crucial en un plan estratégico de seguridad para una organización.

Imagínese una situación que interrumpa las operaciones de las computadoras durante una semana o un mes; imagine la pérdida de todos los datos de la empresa, todas las unidades de respaldo del sitio y la destrucción de equipos vitales del sistema ¿Cómo se manejaría semejante catástrofe? Si Ud. se ve en esta situación y lo único que puede hacer es preguntarse "¿Y ahora qué?" ¡ya es demasiado tarde! La única manera efectiva de afrontar un desastre es tener una solución completa y totalmente probada para recuperarse de los efectos del mismo.

¿Qué es un desastre? Se puede considerar como un desastre la interrupción prolongada de los recursos informáticos y de comunicación de una organización, que no puede remediarse dentro de un periodo predeterminado aceptable y que necesita el uso de un sitio o equipo alterno para su recuperación.

Ejemplos obvios son los grandes incendios, las inundaciones, los terremotos, las explosiones, los actos de sabotaje, etcétera. Estadísticas recientes sobre los tipos más comunes de desastres que ocurren muestran que el terrorismo y los incendios son las causas más comunes en muchos países.

La alta gerencia tiene que decidir el periodo predeterminado que lleva una interrupción de servicio de la situación de "problema" a la de "desastre". La mayoría de las organizaciones logran esto llevando a cabo un análisis de impacto en el negocio para determinar el máximo tiempo de interrupción permisible en funciones vitales de sus actividades.

La reanudación de las actividades ante una calamidad puede ser una de las situaciones más difíciles con las que una organización deba enfrentarse. Tras un desastre, es probable que no haya posibilidades de regresar al lugar de trabajo o que no se disponga de ninguna de los recursos acostumbrados. Incluso, es posible que no se pueda contar con todo el personal. La preparación es la clave del éxito para enfrentar los problemas.
No existe ninguna manera costeable para protegerse completamente contra todo tipo de riesgos, particularmente amenazas naturales a gran escala que pueden arrasar zonas extensas. Como consecuencia, siempre se tiene que tolerar algún riesgo residual. La decisión sobre el alcance del desastre para el que habrá de prepararse debe tomarse en los más altos niveles de la empresa. Por ejemplo, la mayor parte de las empresas implementan una estrategia que proteja contra desastres locales, pero pocas cubren desastres a nivel nacional o incluso internacional. Asimismo, las organizaciones que cuentan dos o más sitios, pueden tener una estrategia de recuperación que funcione en caso de que un sitio sea destruido o dañado, pero no si varios sitios son destruidos o dañados al mismo tiempo.

Un plan de contingencia es el proceso de determinar qué hacer si una catástrofe se abate sobre la empresa y es necesario recuperar la red y los sistemas.

Desdichadamente, un plan de contingencia es como el ejercicio y la dieta: más fácil pensar en ello que hacerlo. Con la cantidad de trabajo que la mayoría de los gerentes tienen, el plan de contingencia tiende a dejarse para una ocasión posterior.

1.6.1. Metodología para elaborar un plan de contingencia

El diseñar e implementar un plan de contingencia para recuperación de desastres no es una tarea fácil; puede implicar esfuerzos y gastos considerables, sobre todo si se está partiendo de cero. Una solución comprende las siguientes actividades:

- Debe ser diseñada y elaborada de acuerdo con las necesidades de la empresa.
- Puede requerir la construcción o adaptación de un sitio para los equipos computacionales.
- Requerirá del desarrollo y prueba de muchos procedimientos nuevos, y éstos deben ser compatibles con las operaciones existentes. Se hará participar a personal de muchos departamentos diferentes, el cual debe trabajar en conjunto cuando se desarrolle e implemente la solución.
- Implicará un compromiso entre costo, velocidad de recuperación, medida de la recuperación y alcance de los desastres cubiertos.

Como con cualquier proyecto de diseño, un método estructurado ayuda a asegurar de que se toman en cuenta todos estos factores y de que se les trata adecuadamente.

A continuación se muestran las principales actividades requeridas para la planificación e implementación de un plan de recuperación de desastres.

- Análisis de Riesgos
- Actividades previas al desastre
    - Medidas de Precaución (Plan de prevención)
    - Establecimiento del Plan de Acción
    - Formación de Equipos Operativos
    - Formación de Equipos de Evaluación

- Actividades durante el desastre
    - Plan de Emergencias
    - Formación de Equipos
    - Entrenamiento
- Actividades después del desastre
    - Evaluación de daños
    - Ejecución de Actividades
    - Evaluación de Resultados

1.6.2. Análisis de Riesgos

"En un entorno informático existen una serie de recursos (humanos, técnicos, de infraestructura...) que están expuestos a diferentes tipos de riesgos: los 'normales', aquellos comunes a cualquier entorno, y los excepcionales, originados por situaciones concretas que afectan o pueden afectar a parte de una organización o a toda la misma, como la inestabilidad política en un país o una región sensible a terremotos"[10]

Para tratar de minimizar los efectos de un problema de seguridad se realiza lo que denominamos un **análisis de riesgos**, término que hace referencia al proceso necesario para responder a tres cuestiones básicas sobre nuestra seguridad:

- ¿Qué queremos proteger?
- ¿Qué puede ir mal?
- ¿Cuál es la probabilidad de que suceda?

1.6.2.1. ¿Qué queremos proteger?

Para responder a esta pregunta se necesita incorporar todos los componentes del sistema susceptibles de ser dañados, dando lugar a la pérdida de

[10] José Plans, Practicas de Auditoria Informatica, Eyrolles, 1983

conectividad, computadoras o datos. Un diagrama de la arquitectura de todos los componentes del sistema facilitará la realización de un inventario de los elementos que pueden necesitar ser restituidos tras un desastre. No hay que olvidar que también el software necesita ser reemplazado, y que todos los productos software relevantes han de ser identificados. Esto incluye cosas como las utilidades del sistema de archivos empleados para facilitar las operaciones de red.

Un inventario completo de una red muestra de manera clara la complejidad de ésta. Cualquiera que realice inventarios de componentes para redes, comprende los problemas en el seguimiento del hardware y software utilizado por los usuarios finales.

Una omisión en el inventario fácilmente puede dar lugar a una recuperación fallida tras un desastre. El sistema de aplicación puede no encontrarse preparado para su uso si alguno de sus componentes no está disponible; en tal caso, es aconsejable estar constantemente a la expectativa de los nuevos elementos que pueden haberse olvidado. Por ejemplo, una aplicación para acceso remoto no funcionaría si los cables no están disponibles para conectar los módem.

Uno de los aspectos menos agradables a tener en cuenta, y que a menudo se pasa por alto, es que las personas esenciales se vean afectadas por el desastre y sea necesario recurrir a otras para realizar sus labores. Una formación diversificada en los sistemas dentro de la organización puede ayudar a reducir el impacto de la indisponibilidad de uno de los colaboradores. Al menos, los manuales de las aplicaciones más importantes para la empresa deberían encontrarse disponibles en un sitio externo.

1.6.2.2. ¿Qué puede ir mal?

Lo más difícil en el plan de contingencia es responder a la pregunta, ¿qué posiblemente pueda ir mal? La respuesta a tal cuestión varía desde lo evidente hasta lo casi increíble.

Las clases más obvias de desastres son los desastres naturales que conllevan tormentas de todo tipo o los acontecimientos geológicos como terremotos o volcanes. En cada localidad existe la posibilidad de tener mal tiempo.

Las inundaciones pueden acaecer en casi cualquier lugar donde el drenaje existente no sea capaz de absorber el volumen de lluvia o fango. Relacionado con las inundaciones se encuentra el perjuicio producido por el agua.

Cada año los incendios en los edificios provocan importantes daños a los sistemas informáticos debido al agua, cuando los sistemas automáticos de irrigación (sprinklers) se activan para apagar el fuego.

Los propios incendios constituyen uno de los peores desastres posibles. El calor, el humo y el agua que rodea a los incendios son tremendamente perjudiciales para los sistemas informáticos. Los dispositivos de almacenamiento se deterioran fácilmente debido a las altas temperaturas y el humo. La eliminación de los residuos tóxicos tras el incendio de una oficina puede llevar meses, incluso años. Esto implica que puede no ser posible disponer de lo sistemas y datos hasta bastante tiempo después del incendio. Existen compañías especializadas en preparar operaciones específicas de limpieza de instalaciones víctimas del incendio, que darán su aprobación para enviar especialistas con trajes protectores al edificio incendiado, recuperar el equipo de procesamiento de datos e intentar restaurar la información de los discos.

Deben considerarse mecanismos alternativos de acceso a la red en el caso de que, por alguna razón, sea imposible acceder al edificio, incluso aunque el edificio puede estar en pie y operacional. Ejemplos de sucesos que pueden impedir e acceso al interior del edificio son los accidentes químicos e industriales, así como los motines y disturbios callejeros.

El fuego no tiene por qué darse necesariamente en la propia instalación para que el problema sea devastador. Un incendio destruyó la oficina central dc Ameritech, en Hinsdale, Illinois, dejando a numerosos clientes sin servicio telefónico durante meses mientras la compañía reparaba la edificación dañada. Obviamente, las comunicaciones que empleaban las líneas telefónicas que habían sido enrutadas a través de esta instalación, se vieron seriamente afectadas.

Desgraciadamente, los ataques terroristas y otros actos deliberados de destrucción cometidos por personas pueden devastar sistemas e instalaciones. Este incluye actos violentos (por ejemplo, descargar armas sobre los equipos informáticos). Menos excitante, pero igual de perjudicial para la organización, es la pérdida de equipos debido al robo. Existen también ataques a los datos contra los que hay que estar prevenidos, en los que la gente destruye intencionadamente datos mediante su borrado o inutilizándolos. Los virus se encuentran en este campo.

Los errores humanos son una de las causas más probables de la pérdida o deterioro de los datos. Si un error de este tipo provoca la pérdida de un sistema en la red, tiene el mismo efecto que cualquier otro tipo de desastre, y como tal debe ser tratado.

1.6.2.3. ¿Cuál es la probabilidad de que suceda?

Si se tuviera una cantidad ilimitada de recursos y fuera posible protegerse contra todas las calamidades, esta pregunta carecería de interés. Sin embargo, no se dispone de recursos infinitos; de hecho, los recursos son bastante escasos. Por lo tanto, se deben seleccionar los tipos de desastres contra los que uno intentará protegerse. Obviamente, estos preciados recursos se querrán gastar en aquellos desastres que tengan la mayor probabilidad de afectar a la organización.

Por ejemplo, se podría intentar proteger los sistemas de la improbable ocurrencia de la caída sobre el edifico de un meteorito procedente del espacio exterior. Esto no sería tan valioso como proteger los sistemas de las inundaciones.

Responder a la pregunta: ¿cuál es la probabilidad de que suceda? también requiere de ciertas consideraciones presupuestarias. Ello puede ayudar a asumir distintos escenarios de presupuesto para comprender cuáles son los costos de compromiso para diferentes niveles de protección y preparación. Finalmente, se puede estar expuesto a ciertas amenazas cuya protección no está al alcance del presupuesto, pero, al menos, se es consciente de su existencia y, por lo tanto, es posible mejorar el plan en un futuro.

En la práctica *existen dos aproximaciones para responder a estas cuestiones*, una cuantitativa y otra cualitativa. *La primera* de ellas es con diferencia la menos usada, ya que en muchos casos implica cálculos complejos o datos difíciles de estimar. Se basa en dos parámetros fundamentales: la probabilidad de que un suceso ocurra y una estimación del coste o las pérdidas en caso de que así sea; el producto de ambos términos es lo que se denomina **coste**

anual estimado (EAC, *Estimated Annual Cost*), y aunque teóricamente es posible conocer el riesgo de cualquier evento (el EAC) y tomar decisiones en función de estos datos, en la práctica la inexactitud en la estimación o en el cálculo de parámetros hace difícil y poco realista esta aproximación.

El segundo método de análisis de riesgos es el cualitativo, de uso muy difundido en la actualidad especialmente entre las nuevas `consultoras' de seguridad (aquellas más especializadas en seguridad lógica, cortafuegos, *tests* de penetración y similares). Es mucho más sencillo e intuitivo que el anterior, ya que ahora no entran en juego probabilidades exactas sino simplemente una estimación de pérdidas potenciales. Para ello se interrelacionan cuatro elementos principales: las amenazas, por definición siempre presentes en cualquier sistema, las vulnerabilidades, que potencian el efecto de las amenazas, el impacto asociado a una amenaza, que indica los daños sobre un activo por la materialización de dicha amenaza, y los controles o salvaguardas, contramedidas para minimizar las vulnerabilidades (controles preventivos) o el impacto (controles curativos). Con estos cuatro elementos podemos obtener un indicador cualitativo del nivel de riesgo asociado a un activo determinado dentro de la organización, visto como la probabilidad de que una amenaza se materialice sobre un activo y produzca un determinado impacto.

1.6.3. Actividades previas al Desastre

Son todas las actividades de planeamiento, preparación, entrenamiento y ejecución de las actividades de resguardo de la información, que nos aseguren un proceso de Recuperación con el menor costo posible para la Cooperativa.

Podemos detallar las siguientes Actividades Generales:

- Establecimiento del Plan de Acción.
- Formación de Equipos Operativos.
- Formación de Equipos de Evaluación (auditoría de cumplimiento de los procedimientos sobre Seguridad).

1.6.3.1. Medidas de Precaución (Plan de Prevención)

Al implementar un plan de prevención, estamos encaminados a procurar tener las medidas adecuadas para evitar que un desastre informático suceda y de presentarse, sus daños sean mínimos, ya que la continuidad del negocio, es vital para cualquier organización.

1.6.3.2. Establecimiento del Plan de Acción

En esta fase de Planeamiento se debe de establecer los procedimientos relativos a:

1.6.3.2.1. Sistemas e Información

La Institución deberá tener una relación de los Sistemas de Información con los que cuenta, tanto los realizados por el centro de cómputo como los hechos por las áreas usuarias. Debiendo identificar toda información sistematizada o no, que sea necesaria para la buena marcha Institucional.

La relación de Sistemas de Información deberá detallar los siguientes datos:

- Nombre del Sistema.
- Lenguaje o Paquete con el que fue creado el Sistema. Programas que lo conforman (tanto programas fuentes como programas objetos, rutinas, macros, etc.).
- La Dirección (Gerencia, Departamento, etc.) que genera la información base (el «dueño» del Sistema).

- Las unidades o departamentos (internos/externos) que usan la información del Sistema.
- El volumen de los archivos que trabaja el Sistema.
- El volumen de transacciones diarias, semanales y mensuales que maneja el sistema.
- El equipamiento necesario para un manejo óptimo del Sistema.
- La(s) fecha(s) en las que la información es necesitada con carácter de urgencia.
- El nivel de importancia estratégica que tiene la información de este Sistema para la Institución (medido en horas o días que la Institución puede funcionar adecuadamente, sin disponer de la información del Sistema). Equipamiento mínimo necesario para que el Sistema pueda seguir funcionando (considerar su utilización en tres turnos de trabajo, para que el equipamiento sea el mínimo posible).
- Actividades a realizar para volver a contar con el Sistema de Información (actividades de Restore).

Con toda esta información se deberá de realizar una lista priorizada (un ranking) de los Sistemas de Información necesarios para que la Institución pueda recuperar su operatividad perdida en el desastre (contingencia).

1.6.3.2.2. Equipos de Cómputo

Aparte de las Normas de Seguridad, hay que tener en cuenta:

- Inventario actualizado de los equipos de manejo de información (computadoras, impresoras, etc.), especificando su contenido (software

que usa, principales archivos que contiene), su ubicación y nivel de uso Institucional.

- Pólizas de Seguros Comerciales. Como parte de la protección de los Activos Institucionales, pero haciendo la salvedad en el contrato, que en casos de siniestros, la restitución del Computador siniestrado se podrá hacer por otro de mayor potencia (por actualización tecnológica), siempre y cuando esté dentro de los montos asegurados.
- Señalización o etiquetado de los Computadores de acuerdo a la importancia de su contenido, para ser priorizados en caso de evacuación. Por ejemplo etiquetar (colocar un sticker) de color rojo a los Servidores, color amarillo a las PC's con Información importante o estratégica y color verde a las PC's de contenidos normales.
- Tener siempre actualizada una relación de PC's requeridas como mínimo para cada Sistema permanente de la Institución (que por sus funciones constituyen el eje central de los Servicios Informáticos de la Institución), las funciones que realizaría y su posible uso en dos o tres turnos de trabajo, para cubrir las funciones básicas y prioritarias de cada uno de estos Sistemas.

1.6.3.2.3. Obtención y Almacenamiento de los Respaldos de Información

Se deberá establecer los procedimientos para la obtención de copias de Seguridad de todos los elementos de software necesarios para asegurar la correcta ejecución de los Sistemas o aplicativos de la Institución. Para lo cual se debe contar con:

- Backups del Sistema Operativo (en caso de tener varios Sistemas Operativos o versiones, se contará con una copia de cada uno de ellos).

- Backups del Software Base (Paquetes y/o Lenguajes de Programación con los cuales han sido desarrollados o interactúan nuestros Aplicativos Institucionales).
- Backups del Software Aplicativo (Considerando tanto los programas fuentes, como los programas objetos correspondientes, y cualquier otro software o procedimiento que también trabaje con la data, para producir los resultados con los cuales trabaja el usuario final). Se debe considerar también las copias de los listados fuentes de los programas definitivos, para casos de problemas.
- Backups de los Datos (Bases de Datos, Indices, tablas de validación, passwords, y todo archivo necesario para la correcta ejecución del Software Aplicativo de nuestra Institución).
- Backups del Hardware. Se puede implementar bajo dos modalidades :
- Modalidad Externa. Mediante convenio con otra Institución que tenga equipos similares o mayores y que brinden la seguridad de poder procesar nuestra Información, y ser puestos a nuestra disposición, al ocurrir una contingencia y mientras se busca una solución definitiva al siniestro producido. Este tipo de convenios debe tener tanto las consideraciones de equipamiento como de ambientes y facilidades de trabajo que cada institución se compromete a brindar, y debe de ser actualizado cada vez que se efectúen cambios importantes de sistemas que afecten a cualquiera de las instituciones.
- Modalidad Interna. Si tenemos más de un local, en ambos debemos tener señalados los equipos, que por sus características técnicas y capacidades, son susceptibles de ser usados como equipos de emergencia del otro local, debiéndose poner por escrito (igual que en el

caso externo), todas las actividades a realizar y los compromisos asumidos.

- En ambos casos se deberá probar y asegurar que los procesos de restauración de Información posibiliten el funcionamiento adecuado de los Sistemas. En algunos casos puede ser necesario volver a recompilar nuestro software aplicativo bajo plataformas diferentes a la original, por lo que es imprescindible contar con los programas fuentes, al mismo grado de actualización que los programas objeto.

1.6.3.3. Formación de Equipos Operativos

En cada unidad operativa de la Institución, que almacene información y sirva para la operatividad Institucional, se deberá designar un responsable de la seguridad de la Información de su unidad. Pudiendo ser el jefe de dicha Área Operativa.

Sus labores serán:

- Ponerse en contacto con los propietarios de las aplicaciones y trabajar con ellos.
- Proporcionar soporte técnico para las copias de respaldo de las aplicaciones.
- Planificar y establecer los requerimientos de los sistemas operativos en cuanto a archivos, bibliotecas, utilitarios, etc., para los principales sistemas y subsistemas.
- Supervisar procedimientos de respaldo y restauración.
- Supervisar la carga de archivos de datos de las aplicaciones, y la creación de los respaldos incrementales.
- Coordinar líneas, terminales, modem, otros aditamentos para comunicaciones.

- Establecer procedimientos de seguridad en los sitios de recuperación.
- Organizar la prueba de hardware y software.
- Ejecutar trabajos de recuperación.
- Cargar y probar archivos del sistema operativo y otros sistemas almacenados en el local alternante.
- Realizar procedimientos de control de inventario y seguridad del almacenamiento en el local alternante.
- Establecer y llevar a cabo procedimientos para restaurar el lugar de recuperación.
- Participar en las pruebas y simulacros de desastres.

1.6.3.4. Formación de Equipos de Evaluación

Esta función debe ser realizada de preferencia por personal de Inspectoría, de no ser posible, la realizará el personal del área de Informática, debiendo establecerse claramente sus funciones, responsabilidades y objetivos:

- Revisar que las Normas y procedimientos con respecto a Backups y seguridad de equipos y data se cumpla.
- Supervisar la realización periódica de los backups, por parte de los equipos operativos, comprobando físicamente su realización, adecuado registro y almacenamiento.
- Revisar la correlación entre la relación de Sistemas e Informaciones necesarios para la buena marcha de la Institución (detallados en «a»), y los backups realizados.
- Informar de los cumplimientos e incumplimientos de las Normas, para las acciones de corrección respectivas.

1.6.4. Actividades durante el desastre

Una vez presentada la Contingencia o Siniestro, se deberá ejecutar las siguientes actividades, planificadas previamente:

1.6.4.1. Plan de Emergencias

En este plan se establecen las acciones se deben realizar cuando se presente un Siniestro, así como la difusión de las mismas.

Es conveniente prever los posibles escenarios de ocurrencia del Siniestro:

- Durante el día.
- Durante la Noche o madrugada.

Este plan deberá incluir la participación y actividades a realizar por todas y cada una de las personas que se pueden encontrar presentes en el área donde ocurre el siniestro, debiendo detallar:

- Vías de salida o escape.
- Plan de Evacuación del Personal.
- Plan de puesta a buen recaudo de los activos (incluyendo los activos de Información) de la Institución (si las circunstancias del siniestro lo posibilitan)
- Ubicación y señalización de los elementos contra el siniestro (extinguidores, cobertores contra agua, etc.)
- Secuencia de llamadas en caso de siniestro, tener a la mano: elementos de iluminación (linternas), lista de teléfonos de Bomberos / Ambulancia, Jefatura de Seguridad y de su personal (equipos de seguridad) nombrados para estos casos.

1.6.4.2. Formación de Equipos

Establecer claramente cada equipo (nombres, puestos, ubicación, etc.) con funciones claramente definidas a ejecutar durante el siniestro.

Si bien la premisa básica es la protección de la Integridad del personal, en caso de que el siniestro lo permita (por estar en un inicio o estar en una área cercana, etc.), deberá de existir dos equipos de personas que actúen directamente durante el siniestro, un equipo para combatir el siniestro y otro para el salvamento de los recursos Informáticos, de acuerdo a los lineamientos o clasificación de prioridades, para salvar los equipos señalados en el Plan de Acción.

1.6.4.3. Entrenamiento

Establecer un programa de prácticas periódicas de todo el personal en la lucha contra los diferentes tipos de siniestros, de acuerdo a los roles que se le hayan asignado en los planes de evacuación del personal o equipos, para minimizar costos se puede aprovechar fechas de recarga de extinguidores, charlas de los proveedores, etc.

Un aspecto importante es que el personal tome conciencia de que los siniestros (incendios, inundaciones, terremotos, apagones, etc.) pueden realmente ocurrir, y tomen con seriedad y responsabilidad estos entrenamientos, para estos efectos es conveniente que participen los elementos directivos, dando el ejemplo de la importancia que la alta dirección otorga a la Seguridad Institucional.

1.6.5. Actividades después del desastre

Después de ocurrido el Siniestro o Desastre es necesario realizar las actividades que se detallan, las cuales deben estar especificadas en el Plan de Acción.

1.6.5.1. Evaluación de Daños

Inmediatamente después que el siniestro ha concluido, se deberá evaluar la magnitud del daño que se ha producido, que sistemas se están afectando, que equipos han quedado no operativos, cuales se pueden recuperar, y en cuanto tiempo, etc.

Adicionalmente se deberá lanzar un pre-aviso a la Institución con la cual tenemos el convenio de respaldo, para ir avanzando en las labores de preparación de entrega de los equipos por dicha Institución.

1.6.5.2. Priorización de Actividades del Plan de Acción

Toda vez que el Plan de acción es general y contempla una pérdida total, la evaluación de daños reales y su comparación contra el Plan, nos dará la lista de las actividades que debemos realizar, siempre priorizándola en vista a las actividades estratégicas y urgentes de nuestra Institución.

Es importante evaluar la dedicación del personal a actividades que puedan no haberse afectado, para ver su asignamiento temporal a las actividades afectadas, en apoyo al personal de los sistemas afectados y soporte técnico.

1.6.5.3. Ejecución de Actividades

La ejecución de actividades implica la creación de equipos de trabajo para realizar las actividades previamente planificadas en el Plan de acción. Cada uno de estos equipos deberá contar con un coordinador que deberá reportar diariamente el avance de los trabajos de recuperación y, en caso de producirse algún problema, reportarlo de inmediato a la jefatura a cargo del Plan de Contingencias.

Los trabajos de recuperación tendrán dos etapas, la primera la restauración del servicio usando los recursos de la Institución o local de respaldo, y la segunda etapa es volver a contar con los recursos en las cantidades y lugares propios del Sistema de Información, debiendo ser esta última etapa lo suficientemente

rápida y eficiente para no perjudicar el buen servicio de nuestro Sistema e imagen Institucional, como para no perjudicar la operatividad de la Institución o local de respaldo.

1.6.5.4. Evaluación de Resultados

Una vez concluidas las labores de Recuperación del (los) Sistema(s) que fueron afectado (s) por el siniestro, debemos de evaluar objetivamente, todas las actividades realizadas, que tan bien se hicieron, que tiempo tomaron, que circunstancias modificaron (aceleraron o entorpecieron) las actividades del plan de acción, como se comportaron los equipos de trabajo, etc.

De la Evaluación de resultados y del siniestro en si, deberían de salir dos tipos de recomendaciones, una la retroalimentación del plan de Contingencias y otra una lista de recomendaciones para minimizar los riesgos y pérdida que ocasionaron el siniestro.

1.6.5.5. Retroalimentación del Plan de Acción

Con la evaluación de resultados, debemos de optimizar el plan de acción original, mejorando las actividades que tuvieron algún tipo de dificultad y reforzando los elementos que funcionaron adecuadamente.

1.6.6. Pruebas del plan

Una vez redactado el plan, hay que probarlo. Hay que estar seguro de que el plan va a funcionar. Para ello, se debe ser escéptico sobre el propio trabajo, de manera que pueda uno probarse a sí mismo que funciona. Psicológicamente, esto no es fácil porque con toda probabilidad se ha invertido una gran cantidad de tiempo y energía personal en este proceso, aunque lo mejor sería, si es posible, situarse de manera imparcial ante la confiabilidad del plan. Por consiguiente, han de realizarse las pruebas para encontrar problemas, no para

verificar que el plan funciona. Si existen errores en la información, tómese nota de ellos y corríjase el plan.

1.6.6.1. Comprobación del plan por partes

No se puede tumbar el sistema algún día para ver si se es capaz de recuperarlo. Existen muchas y mejores formas de verificar un plan de contingencia sin causar mayores interrupciones en el trabajo de la organización. Algunas de las cosas en las que habitualmente no se piensa a la hora de comprobar pueden ahorrar mucho tiempo posteriormente. Por ejemplo, llamar a los números telefónicos de los colaboradores incluidos en las listas telefónicas del plan para confirmar si son actuales; llamar a los vendedores y comprobar si disponen de existencias de productos, ya que puede que hayan modificado su política de inventario. Algún día, viajar hasta la instalación alterna para saber dónde está y cómo reconocer el edificio.

Por supuesto, también es necesario verificar los procedimientos que se emplearán para recuperar los datos. Compruébese el software para la realización de las copias de seguridad para confirmar si pueden recuperarse las aplicaciones de mayor prioridad de la manera esperada. Una vez recuperada la información, verifíquese si el usuario puede acceder a ella. Esto requiere de algunas estaciones de trabajo conectadas a la red para simular auténticos usuarios finales con cuentas en los servidores originales. En este punto, puede ser necesario actualizar el plan para incluir información sobre el establecimiento de cuentas de usuario. Compruébese cada una de las operaciones del plan individualmente y examínese entonces si, como resultado, se tiene un sistema de red en funcionamiento. No está de más verificar el plan

con otras personas de la organización que se encuentren tan familiarizadas con los productos o procedimientos empleados.

Revísese cada día la parte del plan relacionada con las operaciones de copias de seguridad verificando la finalización correcta de las mismas. Además, supervise esto asegurándose de que algunas personas de la organización saben realizar copias de seguridad adecuadamente, y comprobar su finalización.

1.6.7. Distribución y mantenimiento del plan

Por último, cuando se disponga de un plan definitivo ya verificado, es necesario distribuirlo a las personas que necesitan tenerlo. Inténtese controlar las versiones del plan, de manera que no exista confusión con múltiples versiones. Así mismo, es necesario asegurar la disponibilidad de copias extra del plan para su depósito en la instalación exterior en cualquier otro lugar además del lugar de trabajo. Manténgase una lista de todas las personas y ubicaciones que tienen una copia del plan. Cuando se actualice el plan, sustituya todas las copias y recoja las versiones previas.

El mantenimiento del plan es un proceso sencillo. Se comienza con una revisión del plan existente y se examina en su totalidad, realizando cambios a cualquier información que pueda haber variado. En ese instante, se debe volver a evaluar los sistemas de aplicación y determinar cuáles son los más importantes para la organización. Las modificaciones a esta parte del plan causarán modificaciones consecutivas a los procedimientos de recuperación. Sin embargo, esto no debería verse como un problema porque probablemente la sección de procedimientos tenga que actualizarse de todas formas debido a otros cambios. Si se han realizado modificaciones al sistema de copias de

seguridad, hay que cerciorarse de incluir la información sobre el funcionamiento del nuevo o actualizado sistema.

Este proceso llevará tiempo, pero posee algunos valiosos beneficios que se percibirán aunque nunca tengan que utilizarse. Más gente conocerá la red. Esto proporcionará a la organización una base técnica más amplia para mantener correctamente la red. También facilitará el crecimiento de una perspectiva global sobre la red dentro del núcleo de administradores de sistemas de información y puede ayudar a identificar las futuras o actuales áreas conflictivas. Uno de los aspectos más difíciles en cualquier labor distribuida, como es la gestión y administración de LAN, es dar a conocer la situación actual. El mantenimiento y verificación de un plan de migración ayudará a que se produzca dicha comunicación dentro de la organización.

CAPITULO II

DISEÑO DE LAS POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

2.1. Análisis de Riesgos y Amenazas contra la Seguridad

2.1.1. Situación Actual

La Cooperativa actualmente realiza sus operaciones en los cantones: Quito, Mejía y Rumiñahui de la provincia del Pichincha, su matriz se ubica en el barrio Chaupitena en la parroquia Amaguaña donde funciona el departamento de Sistemas; mantiene una sucursal en la zona norte de la ciudad de Quito, el Inca, y el parte sur operan las oficinas de Chillogallo, Conocoto, Amaguaña, La Ecuatoriana, Guamaní, en el cantón Mejía operan las agencias de Aloag y Machachi, y la agencia Sangolquí en el cantón Rumiñahui.

2.1.2. Infraestructura Física

Tabla 2.1: Descripción de la infraestructura física

Componente	Situación Actual
Infraestructura de la Cooperativa	• Cuenta con una sola planta, donde se halla distribuidos los diferentes departamentos que conforman la Cooperativa. • Su estructura es de hormigón • Todos los departamentos están alfombrados, a excepción del cuarto de Servidores.
Acceso a las instalaciones	• Existen 2 accesos a las instalaciones las cuales se

	encuentran custodiadas por personal de seguridad. • El ingreso es libre para cualquier persona. • El departamento de Sistemas no tiene ningún tipo de seguridad.
Planos Arquitectónicos	• El edificio cuenta con los planos de la edificación y su estructuración completa.
Instalaciones Eléctricas	• Las tomas eléctricas del edificio cumplen con las especificaciones técnicas adecuadas para un buen funcionamiento. • Posee una planta de energía eléctrica que suple al normal fluido eléctrico proporcionado por parte de la empresa eléctrica de ser necesario. • Posee una red de UPS centralizada para los diferentes departamentos.
Detectores de humo y alarmas	• No cuenta con sistemas detectores de humo • Si cuenta con un sistema de alarmas, el cual se encuentra conectado con la Policía Nacional.

Extintores de incendio	• No todos los departamentos cuentan con su extintor de incendio
Cableado estructurado	• Cuenta con un cableado estructurado categoría 5, el cual no se encuentra certificado, ni existen planos de estos.
Acceso al Cuarto de Servidores	• El acceso es restringido • Se cuenta con una puerta de vidrio y una cerradura convencional.
Seguridades del Cuarto de Servidores	• No cuenta con ningún tipo de seguridad.
Sistema de enfriamiento para el Cuarto de Servidores	• Cuenta con un sistema de aire acondicionado en el cuarto de servidores exclusivo para este fin, el cual se activa de forma automática.
Central Telefónica	• Posee una central telefónica
Salidas de emergencia	• El edificio no cuenta con salidas de emergencia.

2.1.3. Inventario Hardware

A continuación se detallan los equipos informáticos pertenecientes a la Cooperativa, tanto en la matriz como en las sucursales.

Tabla 2.2: Inventario de Hw que posee la Cooperativa

MATRIZ

DEPTO.	PROCESADOR	RAM	HARD DISK	IMPRESORA
Gerencia	AMD (Portátil)		40 GB	HP Desk Jet
Secretaria	Intel P3 16 Hz	255 MB	37 GB	Epson
Sistemas				
	Intel (Portátil)	448 MB	37.2 GB	No
	Intel P4 1.8 GHz	248 MB	37.2 GB	No
	Intel P4 1.8 GHz	120 MB	32.2 GB	No
	Intel P3 1.8 GHz	120 MB	37 GB	No
Cuarto de Servidores				
	Servidor Sun Full Power (Ultra Spak 250)	768 MB	5 HD de 36 GB	No
	HP Net Server LC 3 (AT/AT Compatible Pentium II)	130 MB	9.6 GB	No
Contabilidad				
	Intel P4 1.8 GHz	120 MB	37.2 GB	Canon
	AMD 266 MHz	120 MB	37.4 GB	Epson G716
	Intel Celeron (TM) -366 MHz	112 MB	12 GB	No
	Intel Celeron de 333 MHz	160 MB	23 GB	Epson LQ 2070
Cartera	Pentium Pro 266 MHz	88 MB	4 GB	No
Tesorería	Intel (R) Pentuim III 1.80GHz	120 MB	37 GB	Compaq FX-880
Auditoría Interna	Pentium (R) 200 MHz	128 MB	5.6 GB	Canon BJC-1000
Dto. Legal	Pentium-s CPU 120MHz	47 MB	2 GB	No
Secretaría Consejo Administración	Pentium I 166 MHz	48 MB	4.28 GB	Epson LX-300
Consejo Administración	Celeron (TM)-MMX CPU 366 MHz	31 MB	19.5 GB	No
Consejo Vigilancia	Genuine Intel x 86	256 MB	39 GB	No

SUCURSAL MAYOR

DEPTO.	PROCESADOR	RAM	HARD DISK	IMPRESORA
Cartera				
	Intel ® Pentuim 4 1.80 GHz	120 MB	37 GB	HP
	Authentic AMD	128 MB	448 GB	No
Servicio al Cliente				
	Authentic AMD	128 MB	448 GB	No
	Pentium Pro de 300 MHz	128. MB	4.1 GB	Epson LX 300
Cobranzas	Intel Celeron 333 Mhz	80 MB	651.GB	Epson LX 300
Cajas				
	Intel Pentium 4	120 MB	37.2 GB	Epson FX 880
	Pentium Pro 300Mhz			No

AGENCIA EL INCA

DEPTO.	PROCESADOR	RAM	HARD DISK	IMPRESORA
Jefatura	Pentium Pro (R) 333 Mhz	96 MB	4 GB	Hp Desk Jet 695C
Servicio al Cliente	Pentium Pro ® 333 Mhz	160 MB	6.02 GB	Epson
Cartera	Pentium Pro 333 Mhz	128 MB	4 GB	HP 1200
	Intel Celeron de 400 Mhz	96 MB	4 GB	HP 1200
Cobranzas	Intel Pentium Pro 333 Mhz	96 MB	4.1 GB	No
Caja	Intel Celeron de 333 MHZ	96 MB	1 GB	Epson FX-880+
	Intel pentium IV de 1.8 GHz	120 MB	37.2 GB	Epson FX-880+
	Pentium Pro (R) 333 Mhz	96 MB	2 GB	No
Servidores	HP X86 Family 6 Model 5 Stepping 2	130.484 Kb	1.90 GB	No
	Amd Athlon(TM) XP 2400	490.992 Kb	37.2 GB	No

AGENCIA CHILLOGALLO

DEPTO.	PROCESADOR	RAM	HARD DISK	IMPRESORA
Jefatura	Intel P. IV de 1.8 Ghz	128 MB	40 Gb	LEXMARK Z12
Servicio al Cliente	Intel Pentium II de 400 Mhz	128 MB	5.99 GB	Epson LX-300
	Intel Pentium II 400 Mhz	128 MB	7.85 GB	No
Cartera y Crédito	Intel Pentium II de 400 Mhz	128 MB	10 GB	HP 1000
	INTEL PENTIUM II DE 400 Mhz	64 MB	2 GB	EPSON LQ 2180
Cajas	INTEL CELERON DE 333 Mhz	128 MB	4 GB	EPSON FX-880+
	Intel Pentium Pro ® de 333 Mhz	128 MB	4 GB	Epson Fx - 880+
Servidores	Intel Pentium III de 800 Mhz	256 MB	10 GB	No

AGENCIA SANGOLQUÍ

DEPTO.	PROCESADOR	RAM	HARD DISK	IMPRESORA
Jefatura	Intel	261.616 KB	38.2 GB	Canon BJC-250
Servicio al Cliente	Pentium II 450MHz	56 MB	6 GB	Epson FX-880+
	Pentium III 450 MHz	128 MB	9 GB	Epson LX-300 +
	Pentium II 300 Mhz	128 MB	20 GB	HP LASER 1300
	Intel Pentium IV de 2.8	256 MB	40 GB	LEXMARK E210 LASER
	Pentium Pro 200 MHz	32 MB	1.96 GB	No
Cobranzas	celeron (TM) - MMX 333 MHZ	128 MB	3.98 GB	No
Cajas	Pentium III 450 Mhz	128 MB	20 GB	Epson Lx-300+
	celeron (TM) - MMX 333 MHZ	128 MB	4 GB	Epson LX-300+
Servidores	X86 Family 6 model 8 stepping 63 AT/AT	145.716 Kb	10 GB	No
	Intel Pentium IV de 2.8	256 MB	40 GB	No

AGENCIA MACHACHI

DEPTO.	PROCESADOR	RAM	HARD DISK	IMPRESORA
Jefatuta	Pentium III 800 EB Mhz	256 MB	30 GB	Hp Deskjet
Servicio al Cliente	Celeron™ MMX CPU Ethernet Adapter 333Mhz	160 MB	4 GB	Epson Fx-880+
	Intel Pentium III 700 Mhz	128 MB	20 GB	Epson Lx-300+
Crédito	Intel Celeron 300 Mhz	128 MB	1.51 GB	Epson LX-300+
Cajas	Autentic AMD K6 266 Mhz	128 MB	4 GB	Epson Fx-880+
Servidores	HP Intel P III X86 Family 6 Modem 8 stepping 10/AT compatible	256 MB	20 GB	No

AGENCIA ALOAG

DEPTO.	PROCESADOR	RAM	HARD DISK	IMPRESORA
Servicio al Cliente	Intel Pentium III de 866 Mhz	128 MB	30 GB	No
Cajas	Intel Celeron de 333 Mhz	62 MB	2 GB	Epson FX-880+

AGENCIA AMAGUAÑA

DEPTO.	PROCESADOR	RAM	HARD DISK	IMPRESORA
Jefatura	Pentium III de 600 Mhz	120 MB	30 GB	Lexmark Z12
Servicio al Cliente	Autentic AMD K6 de 266 Mhz	64 MB	4 GB	EPSON FX-890
Cobranzas	Autentic AMD K6 de 266 Mhz	64 MB	4 GB	EPSON FX-890
Cajas	Intel Celeron de 400 Mhz	96 MB	4 GB	EPSON FX-880+
	Pc Chips	32 MB	4 GB	No
Servidores	Acer Verition X86 Family 15 Model 1 stepping 2 AT/AT compatible	261,492 Kb	20 GB	No

AGENCIA CONOCOTO

DEPTO.	PROCESADOR	RAM	HARD DISK	IMPRESORA
Jefatura	Celeron™ MMX CPU at 333 MHz	128 MB	4 GB	Epson Lx-300+
Servicio al Cliente	Pentium (R) 4CPU 1.80 GHz	120 MB	40 GB	HP DESK JET
Cajas	Intel Pentium III de 1 Ghz	255 MB	1.96 GB	Epson FX-880

AGENCIA GUAMANI

DEPTO.	PROCESADOR	RAM	HARD DISK	IMPRESORA
Jefatura	INTEL PENTIUM IV DE 1.8 GHZ	128 MB	40 GB	EPSON STYLUS 1500
Servicio al Cliente	INTEL P II de 400 Mhz	128 MB	8 GB	EPSON LX 300+
Cajas	INTEL P II de 400 Mhz	128 MB	20 GB	EPSON LX 300+

AGENCIA ECUATORIANA

DEPTO.	PROCESADOR	RAM	HARD DISK	IMPRESORA
Servicio al Cliente	Intel Pentium IV de 1.8 Ghz	128 MB	40 GB	EPSON LX - 300+
Caja	Intel Celeron de 366 Mhz	128 MB	4 GB	EPSON LX-300+

LABORATORIO COBIS

DEPTO.	PROCESADOR	RAM	HARD DISK	IMPRESORA
Desarrollo	Intel Pentium IV de 1.8 Gz	128 MB	40 GB	Epson Fx 880+

2.1.4. Inventario Software

La Cooperativa para su correcto funcionamiento cuenta con una amplia variedad en software de diferente procedencia, esto es, con licenciamiento, obtención gratuita, aplicaciones desarrolladas y sin autorización, para lo cual se detalla a continuación su procedencia y descripción.

Tabla 2.3: Tipos de Licencias de Sw

Procedencia	Descripción
Libre	Este tipo de software no requiere de licenciamiento alguno para su instalación.
Adquirido o con equipos	Es el software que por su necesidad es adquirido por la Cooperativa o a su vez con la compra de equipos nuevos.
Desarrollado	Software que por la necesidad han sido desarrollados por el Departamento de Sistemas o por otras empresas especialistas en el desarrollo de Sw a la medida.
Sin Autorización	Existen software que mantiene la Cooperativa sin licenciamiento conocido como “pirata”

A continuación detallamos el software que tiene instalado la Cooperativa en sus diferentes equipos de computación.

Tabla 2.4 : Software que tiene la Cooperativa

Software	Tipo	Procedencia
Microsoft Windows 95	Sistema Operativo	Con equipos
Microsoft Windows 98	Sistema Operativo	Con equipos
Microsoft Windows Milenium	Sistema Operativo	Adquirido
Microsoft Windows XP	Sistema Operativo	Con equipos
Microsoft Windows 2000 Server	Sistema Operativo para servidores	Adquirido
Microsoft Windows NT 4.0	Sistema Operativo para servidores	Adquirido
Microsoft Office 97	Procesador de palabras, hojas de cálculos, presentaciones.	Adquirido
Microsoft Office 2000	Procesador de palabras, hojas de cálculos, presentaciones.	Con equipos
Microsoft Project	Organizador de Proyectos	Adquirido
Pcanywhere 10.5	Acceso Remoto	Sin Autorización
Acrobat 6.0	Lectura de archivos pdf	Libre
Mcafee Virus scann 7.1 y 4.51	Deteccion de Virus Informaticos	Adquirido
Framework		

Software Kernel Cobis para NT		Desarrollado
Software Base 325 Segur	Instalador Fornt end de Cobis	Desarrollado
Megared	Sistema Integrado de Caja	Adquirido
ORINOCO OR Manager	Telecomunicaciones	Adquirido
HT SERVER	Control del Internet (Proxy)	Adquirido
Visual Estudio 6.0	Desarrollo de Aplicaciones	Adquirido
Nero	Quemador de Cd's	Libre
Windows Commander	Transferencia de archivos	Libre
Timbuktu Pro	Monitoreo de la Red	
Flash Get	Gestor de descargas	Libre

La Cooperativa adquirió un sistema denominado **COBIS,** el cual esta compuesto por los siguientes módulos:

Tabla 2.5: Módulos de COBIS

Aplicación	Descripción	Procedencia
Admin. Seguridades	Este módulo crea usuarios para el sistema, da accesos, horarios, actualiza feriados, Administra accesos a los diferentes menús de los módulos COBIS	Desarrollado
Riesgo de Mercado	Monitorea la composición de cartera activa y pasiva sujetas a tasa, para determinar el nivel de exposición del riesgo de pérdida que potencialmente podría afectar a la Cooperativa ante variaciones en el mercado.	Desarrollado
Cartera	Maneja todo lo que se refiere al proceso de préstamos, permitiendo tener un control total sobre cada una de las operaciones realizadas.	Desarrollado

Ahorros	Maneja todo lo que es cuentas de ahorros, bloqueos, desbloqueos de cuentas y todo el proceso de Ventanilla (Depósito, retiro, pago de préstamo, etc.)	Desarrollado
MIS	Maneja los datos de los Clientes de la Cooperativa, (direcciones, teléfono, etc.)	Desarrollado
Plazo Fijo Administrativo	Este módulo parametriza las tazas de interés de lo certificados de Inversión	Desarrollado
Plazo Fijo Operativo	Lleva el control y realiza las operaciones de Plazo Fijo e Inversiones.	Desarrollado
FIRMAS	Mantiene una base de datos de firmas de clientes y esta asociado con el módulo de ATX para la verificación en ventanilla (El ingreso de firmas se realiza mediante digitalización por scanner)	Desarrollado
Contabilidad	Lleva el control de la contabilidad de la Cooperativa, realiza comprobantes contables, etc.	Desarrollado
Crédito	Verifica el estado de la cuenta del cliente para un crédito (gestiona el tramite). Ingresa la información del crédito, comentarios del Oficial, Inspector, y los datos solicitados ara el préstamo.	Desarrollado

2.1.5. Información (Base de Datos)

Cada módulo que conforma el sistema de Información denominado COBIS, tiene su propia Base de Datos las que se encuentran en el motor de base de datos llamado SYSBASE.

Los respaldos son realizados diariamente al final de la jornada de trabajo.

Tabla 2.6 : Bases de datos que posee la Cooperativa

Base de Datos	Responsable
Seguridades	Administrador BD
Ahorros	Administrador BD
Cartera	Administrador BD
Crédito	Administrador BD
Plazo Fijo	Administrador BD
Contabilidad	Administrador BD
Firmas	Administrador BD
MIS	Administrador BD
Riesgos de Mercado	Administrador BD
Garantías	Administrador BD
Seguridades	Administrador BD
Ahorros	Administrador BD

2.1.6. Redes LAN

La red local o LAN (Local Area Network) es un sistema de comunicaciones de alta velocidad que conecta microcomputadoras o PC y/o periféricos que se encuentran cercanos, por lo general dentro del mismo edificio.

La Cooperativa posee varias redes de área local ubicadas en diferentes cantones de la provincia de Pichincha las cuales se muestran a continuación:

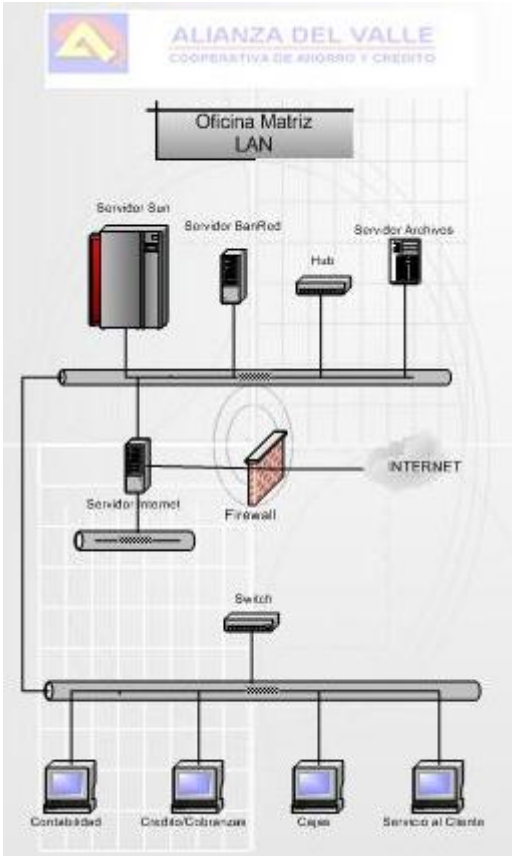

Gráfico 2.1 : LAN Oficina Matriz

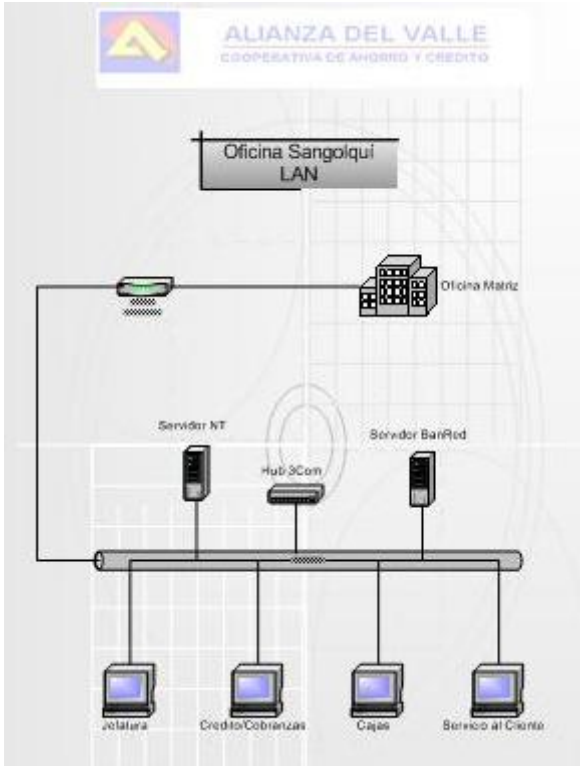

Gráfico 2.3 : LAN Agencia Sangolquí

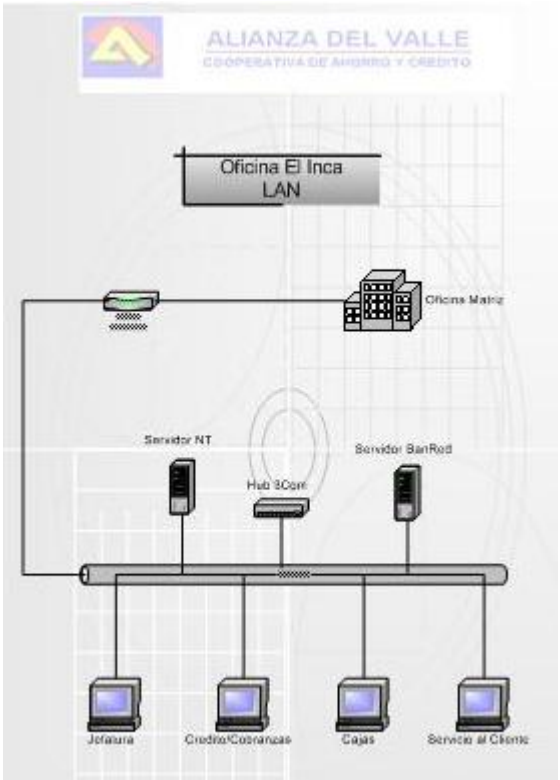

Gráfico 2.2 : LAN Agencia El Inca

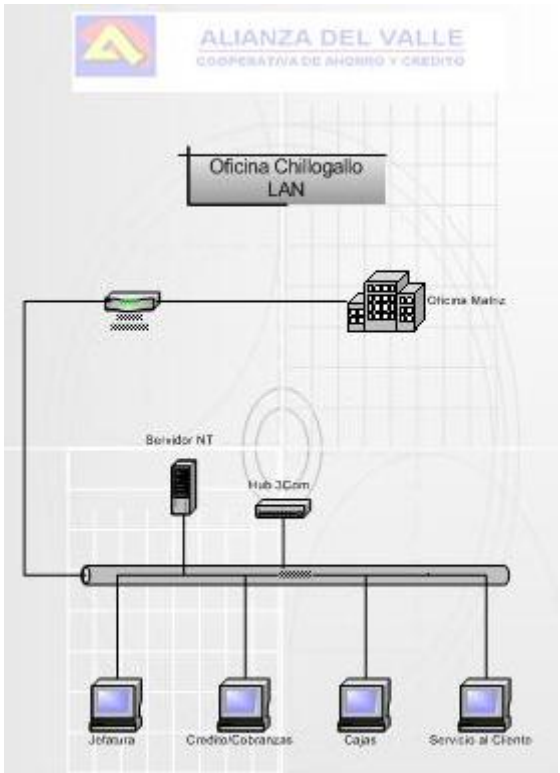

Gráfico 2.4 : LAN Agencia Chillogallo

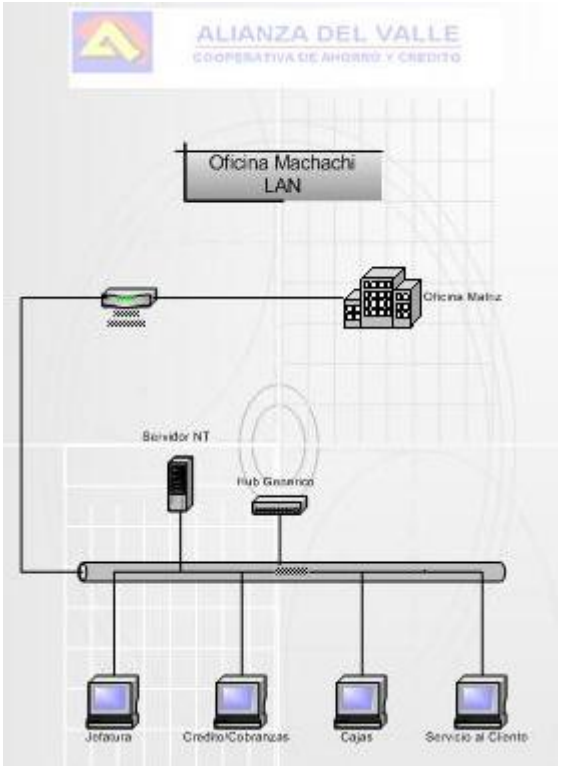

Gráfico 2.5 : LAN Agencia Machachi

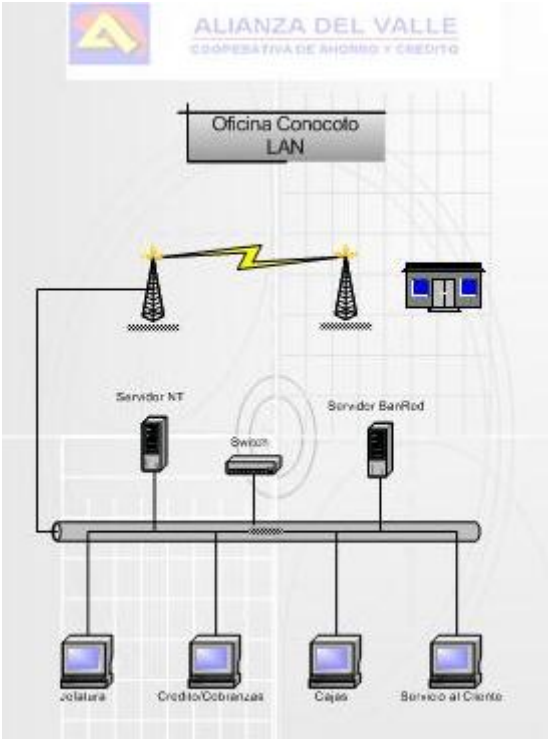

Gráfico 2.7 : LAN Agencia Conocoto

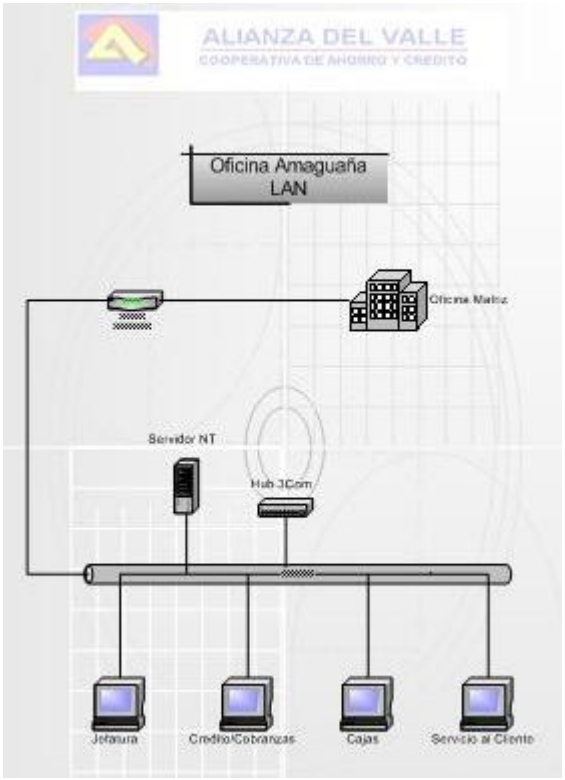

Gráfico 2.6 : LAN Agencia Amaguaña

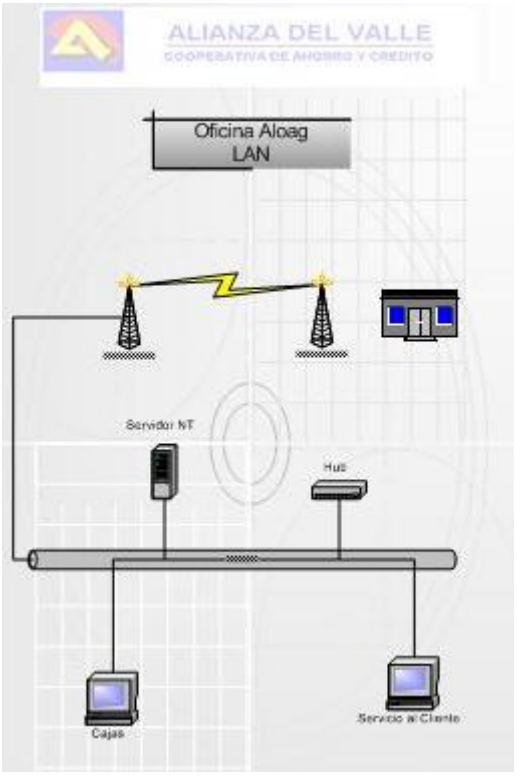

Gráfico 2.8 : LAN Agencia Aloag

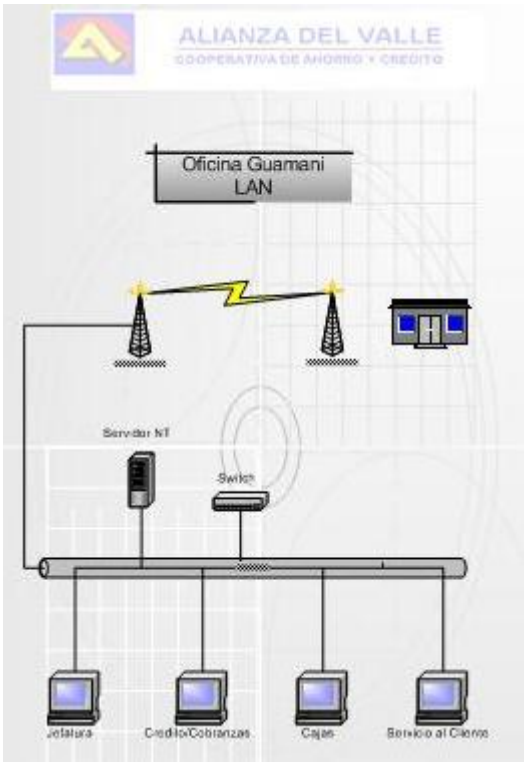

Gráfico 2.9 : LAN Agencia Guamani

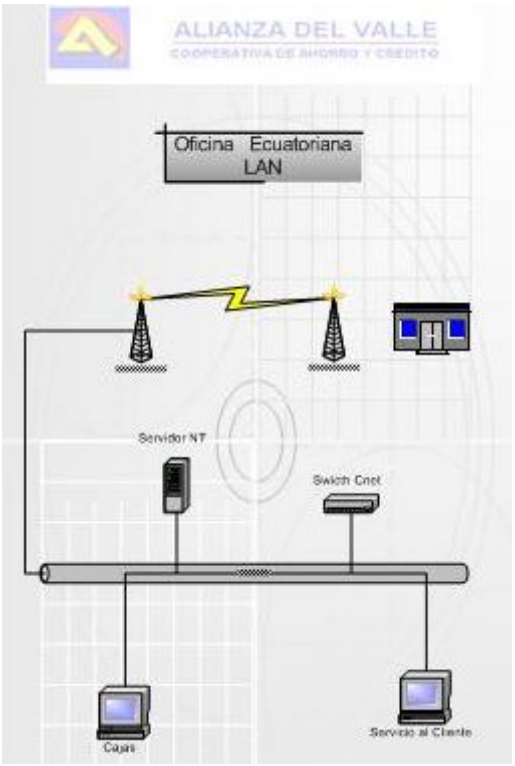

Gráfico 2.11 : LAN Agencia Ecuatoriana

2.1.7. Red Wan

Es un sistema de comunicación de alta velocidad que conecta PC's, entre sí para intercambiar información, similar a la LAN; aunque estos no están limitados geográficamente en tamaño. La WAN utiliza un hardware especial, así como líneas telefónicas proporcionadas por una compañía telefónica.

El hardware para crear una WAN también llega a incluir enlaces de satélites, fibras ópticas, aparatos de rayos infrarrojos y de láser.

Todas las agencias de la Cooperativa se encuentran interconectadas con la Matriz donde se mantiene una base de datos centralizada dando facilidad al socio para que pueda realizar cualquier transacción (retiro y depósito de ahorros, pago de préstamos, etc.) en sus diferentes oficinas, en el siguiente

gráfico se encuentra la representación de la Red WAN de la Cooperativa Alianza del Valle.

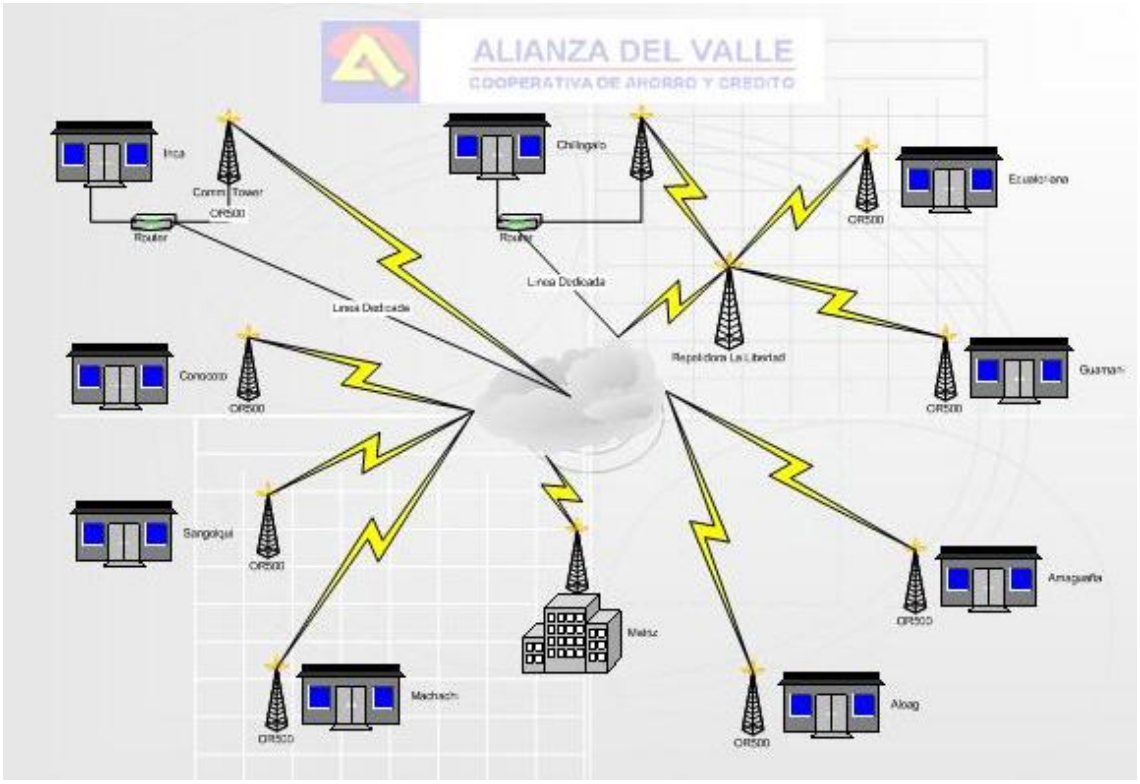

Gráfico 2.12 : Red Wan Cooperativa Alianza del Valle

A continuación se presentan los diferentes equipos de comunicaciones que posee la Cooperativa:

Tabla 2.7: Equipos de Comunicación

Equipo de Comunicación	Marca	Cantidad	Ubicación Agencia
Ruteador	Cisco 800	3	Matriz Inca Chillogallo
Switch de 16 Puertos	Cisco	1	Matriz
Switch de 12 Puertos	3Com	1	Matriz
Switch de 8 Puertos	Cnet	2	Ecuatoriana Conocoto
Hub de 16 Puertos	3Com	2	Machachi Amaguaña
Hub de 8 Puertos	3Com	3	Matriz Aloag Guamaní

Hub de 18 Puertos	3Com	3	Inca Chillogallo Sangolquí
Radio	Orinoco OR500	6	Matriz Sangolquí Machachi Conocoto Amaguaña Aloag
Radio	Rapid wave	4	Guamaní Ecuatoriana Inca Chillogallo
Antena Grilla		10	Matriz Inca Chillogallo Sangolquí Machachi Conocoto Amaguaña Aloag Ecuatoriana Guamaní

2.1.8. Análisis de Riesgos

Una vez que se ha establecido la situación actual en la cual se encuentra la Cooperativa con sus sistemas existentes y los recursos asociados, a continuación definiremos los recursos críticos, se analizarán las vulnerabilidades de los sistemas y sus recursos asociados, que se podrían presentar por diferentes situaciones que hipotéticamente se plantearán y se establecerá su respectiva clasificación de tal manera se logrará ilustrar, calificar y evaluar, cada uno de los distintos escenarios posibles con su respectiva incidencia en los recursos informáticos de la Cooperativa.

2.1.9. Infraestructura Física

Conocido una vez las características en cuanto a infraestructura física, se establece las posibles amenazas que van a ser tomadas en cuenta para la calificación respectiva, enumerándolas y clasificándolas de la siguiente manera:

- **Desastres Naturales**
  - Terremotos
  - Erupciones
  - Inundaciones
- **Fallas eléctricas**
  - Apagones
  - Variaciones Eléctricas
  - Incendios
- **Daños de la Información**
  - Daños en equipos Informáticos
  - Desconfiguración
- **Fallas en comunicaciones**
  - Caída de enlaces
  - Falla de equipos
- **Acciones Hostiles**
  - Hackers y Crackers
  - Ingreso a instalaciones (Robo, Asaltos)

A continuación vamos a detallar la calificación y costo que se asignaran a las posibles amenazas que se van a tomar en cuenta para el siguiente análisis.

Tabla 2.8 : Calificación y Costo para la Cooperativa

Calificación	Costo
Alto	Mas de 6001 Dólares
Medio	Mas de 1001 y Menos de 6000 Dólares
Bajo	Menos de 1000 Dólares

Tabla 2.9 : Descripción de Impacto y Costo para la Cooperativa

Impacto en la Cooperativa	Descripción	Costo
Catastrófico	Se paralizarían de forma permanente las funciones de todos los departamentos de la Cooperativa	Alto
Crítico	Afectaría el normal desenvolvimiento de las funciones de los departamentos involucrados de la Cooperativa	Medio
Marginal	Seria imperceptible la falencia de los servicios de la Cooperativa	Medio
Despreciable	No se interrumpe con las funciones encargadas a los diferentes departamentos y áreas de la Cooperativa	Bajo

El método que se utilizó para encontrar la posibilidad de ocurrencia de la amenaza fue el cualitativo, para esto se realizó estimaciones de acuerdo a las experiencias del personal de sistemas, con los cuales se realizaron las sesiones de trabajo pertinentes.

Tabla 2.10 : Análisis de las amenazas con su nivel de impacto, probabilidad de ocurrencia y costo para la Cooperativa

Amenaza	Impacto	Costo	Riesgo
Desastres Naturales	Catastrófico	Alto	Poco Probable
Fallas Eléctricas	Crítico	Medio	Probable
Daños en la Información	Catastrófico	Alto	Poco Probable
Fallas en las Comunicaciones	Catastrófico	Alto	Probable
Acciones Hostiles	Catastrófico	Alto	Probable

Tabla 2.11 : Análisis de las amenazas con su nivel de impacto, probabilidad de ocurrencia y costo en la infraestructura física de la Cooperativa

Componente	Amenaza	Impacto	Costo	Riesgo
Infraestructura de la Cooperativa	**Inundación:** El departamento se halla en la planta baja, según normas no debería estar en dicha planta.	Catastrófico	Alto	Probable
	Incendio: El piso del departamento de Sistemas es alfombrado., lo que aumenta la probabilidad de que ocurra esta amenaza.	Crítico	Medio	Probable
Acceso a las instalaciones	**Robo de equipos o datos:** No existe un control de acceso a las instalaciones	Marginal	Bajo	Poco Probable
Instalaciones Eléctricas	**Suspensión del servicio:** o No existe personal especializado en electricidad	Marginal	Bajo	Poco Probable

	○ Las baterías de los UPS de los servidores no han recibido el mantenimiento respectivo	Catastrófico	Medio	Probable
Detectores de humo y alarmas	**Incendio:** No existen detectores de humo en el edificio	Crítico	Medio	Probable
Extintores de llamas	**Incendio:** ○ No existe el número suficiente de extintores ○ No existe una capacitación al personal de su uso	Marginal	Bajo	Probable
Cableado Estructurado	**Perdida de la comunicación:** ○ Las canaletas están llenas ° No existen planos del cableado	Catastrófico	Alto	Muy Probable
	Suspensión del servicio: ° No existe seguridad en lugar donde se encuentran los equipos de comunicación	Crítico	Alto	Probable
Seguridades del cuarto de servidores	**Robo de equipos:** No existe seguridad en el cuarto de servidores	Catastrófica	Alto	Probable

Salidas de emergencia	**Incendio o Terremoto:** No existen salidas de emergencia exteriores	Crítico	Alto	Probable

2.1.10. Hardware

De la misma manera se procede a establecer las posibles amenazas que se podrían dar para el hardware de la Matriz y todas las agencias de la Cooperativa y por tratarse de equipos de cómputo todos estos están expuestos a las siguientes amenazas:

- Fallas eléctricas
  - Apagones
  - Variaciones de voltaje
  - Incendios
- Fallas en el equipo
  - Daños en circuitos internos
- Uso indebido del hardware por parte de los usuarios
  - Manipulación incorrecta de los equipos
  - Violación de las normas de trabajo (comer en la oficina, fumar, etc.)
- Acciones Hostiles
  - Robo

Una vez descrita las amenazas de una forma clara y comprensible procederemos a detallar los equipos considerados como imprescindibles que de llegar a fallar ocasionarían un impacto catastrófico que paralizarían las operaciones de la cooperativa o de una de sus agencias.

Tabla 2.12 : Equipos imprescindibles de la Cooperativa

Agencia	Modelo	Departamento	Descripción
Matriz	Pentium Pro de 300 MHz	Servicio al Cliente	Servidor de Impresión
	Servidor Sun Full Power (Ultra Spak 250)	Cuatro servidores	Host Principal
	Hp Net Server LC3 (AT/AT compatible Pentium II)	Cuarto servidores	Servidor de archivos
	Servidor Sun Full Power (Ultra Spak 250)	Cuarto servidores	Host de Backup
Inca	Pentium Pro 333 Mhz	Servicio al cliente	Servidor impresión
	Hp X86 family 6 Model 5 Stepping 2	Sistemas	Servidor de Transacciones
	Amd Athlon (TM) XP 2400	Sistemas	Servidor de archivos
Chillogallo	Intel Pentium II de 400 Mhz	Servicio al cliente	Servidor de impresión
	Intel Pentium III de 800 Mhz	Sistemas	Servidor de transacciones
Sangolquí	Intel Pentium IV de 2.8Ghz	Servicio al cliente	Servidor impresión
	X86 Family 6 Model 8 Stepping 63 AT/AT Compatible	Sistemas	Servidor de Transacciones
	Intel Pentium IV de 2.8	Sistemas	Servidor de archivos
Amaguaña	Amd K 6 de 266 Mhz	Servicio al Cliente	Servidor de impresión
	Accer Verition X86 Family 15 Model 1 Stepping 2 AT/AT Compatible	Sistemas	Servidor de Transacciones y Servidor de archivos
Machachi	Celeron MMX CPU ethernet	Servicio al cliente	Servidor de impresión

	adapter 333 Mhz		
	Hp Intel P III X86 Family 6 Model 8 Stepping 10 AT/AT Compatible	Sistemas	Servidor de Transacciones y Servidor de archivos
Conocoto	Pentium IV 1.80 Ghz	Servicio al Cliente	Servidor de impresión
Guamani	Intel Pentium II de 400 Mhz	Servicio al cliente	Servidor de impresión
La Ecuatoriana	Intel Pentium IV 1.8 Ghz	Servicio al cliente	Servidor de impresión
Aloag	Intel Pentium III 866 Mhz	Servicio al cliente	Servidor de impresión

Para ver el cuadro completo del análisis de las amenazas de los equipos de cómputo que posee la Cooperativa ver Anexo A.

2.1.11. Software

A continuación detallamos las principales amenazas a las que se encuentra expuesto el software que posee la Cooperativa:

- Uso Indebido del Software por parte de los usuarios
  - Agregar, modificar y eliminar programas, archivos, librerías propios del sistema.
- Acciones Hostiles
  - Hackers, Crackers
  - Virus, Gusanos, Bombas lógicas.

Con las amenazas antes descritas se procedió a realizar el análisis de las mismas y su impacto en la Cooperativa.

Tabla 2.13 : Posibles amenazas para el software que posee la Cooperativa y su impacto en ella.

Software	Tipo	Procedencia	Amenazas	Impacto	Calificación
Microsoft Windows 95	Sistema Operativo	Con equipos	° Uso indebido Sw por parte de los usuarios ° Acciones Hostiles	Marginal	Prioritario
Microsoft Windows 98	Sistema Operativo	Con equipos	° Uso indebido Sw por parte de los usuarios ° Acciones Hostiles	Marginal	Prioritario
Microsoft Windows Milenium	Sistema Operativo	Adquirido	° Uso indebido Sw por parte de los usuarios ° Acciones Hostiles	Marginal	Prioritario
Microsoft Windows XP	Sistema Operativo	Con equipos	° Uso indebido Sw por parte de los usuarios ° Acciones Hostiles	Marginal	Prioritario
Microsoft Windows 2000 Server	Sistema Operativo para servidores	Adquirido	° Uso indebido Sw por parte de los usuarios ° Acciones Hostiles	Crítico	Prioritario
Microsoft Windows NT 4.0	Sistema Operativo para servidores	Adquirido	° Uso indebido Sw por parte de los usuarios	Crítico	Prioritario

			° Acciones Hostiles		
Microsoft Office 97	Procesador de palabras, hojas de cálculos, presentaciones.	Adquirido	° Uso indebido Sw por parte de los usuarios ° Acciones Hostiles	Marginal	Baja Prioridad
Microsoft Office 2000	Procesador de palabras, hojas de cálculos, presentaciones.	Con equipos	° Uso indebido Sw por parte de los usuarios ° Acciones Hostiles	Marginal	Baja Prioridad
Microsoft Project	Organizador de Proyectos	Adquirido	° Uso indebido Sw por parte de los usuarios ° Acciones Hostiles	Marginal	Baja Prioridad
Pcanywhere 10.5	Acceso Remoto	Sin Autorización	° Uso indebido Sw por parte de los usuarios ° Acciones Hostiles	Marginal	Baja Prioridad
Acrobat 6.0	Lectura de archivos pdf	Libre	° Uso indebido Sw por parte de los usuarios ° Acciones Hostiles	Marginal	Baja Prioridad
Mcafee Virus scann 7.1 y 4.51	Deteccion de Virus Informaticos	Adquirido	° Uso indebido Sw por parte de los usuarios ° Acciones Hostiles	Marginal	Prioritario

Framework			° Uso indebido Sw por parte de los usuarios ° Acciones Hostiles	Marginal	Baja Prioridad
Software Kernel Cobas para NT		Desarrollado	° Uso indebido Sw por parte de los usuarios ° Acciones Hostiles	Crítico	Imprescindible
Software Base 325 Segur	Instalador Fornt end de Cobis	Desarrollado	° Uso indebido Sw por parte de los usuarios ° Acciones Hostiles	Crítico	Imprescindible
Megared	Sistema Integrado de Caja	Adquirido	° Uso indebido Sw por parte de los usuarios ° Acciones Hostiles	Crítico	Prioritario
ORINOCO OR Manager	Telecomunicaciones	Adquirido	° Uso indebido Sw por parte de los usuarios ° Acciones Hostiles	Marginal	Prioritario
HT SERVER	Control del Internet (Proxy)	Adquirido	° Uso indebido Sw por parte de los usuarios ° Acciones Hostiles	Marginal	Prioritario

Visual Estudio 6.0	Desarrollo de Aplicaciones	Adquirido	° Uso indebido Sw por parte de los usuarios ° Acciones Hostiles	Marginal	Baja Prioridad
Nero	Quemador de Cd's	Libre	° Uso indebido Sw por parte de los usuarios ° Acciones Hostiles	Marginal	Baja Prioridad
Windows Commander	Transferencia de archivos	Libre	° Uso indebido Sw por parte de los usuarios ° Acciones Hostiles	Marginal	Baja Prioridad
Timbuktu Pro	Monitoreo de la Red		° Uso indebido Sw por parte de los usuarios ° Acciones Hostiles	Marginal	Baja Prioridad
Flash Get	Gestor de descargas	Libre	° Uso indebido Sw por parte de los usuarios ° Acciones Hostiles	Marginal	Baja Prioridad

A continuación vamos a realizar un Ranking de los Sistemas de Información necesarios para que la Cooperativa pueda recuperar su operatividad perdida en un posible desastre.

Nombre del Sistema: AHORROS

Lenguaje o Paquete en que fue creado el sistema:
VISUAL BASIC 6.0 front-ent, SYBASE back-end (BDD)

Gerencia, Departamento(s) que genera la información:

Cajas, Servicio al Cliente, Cartera, Contabilidad

Las unidades o departamentos (internos/externos) que usan la información del Sistema:

INTERNOS
Contabilidad, Riesgos, Tesorería, Negocios, Marketing, Servicio al Cliente, Cartera, Crédito y cobranzas, auditoria.

EXTERNOS

- CONSEP
- AGD

Volumen de transacciones que maneja el sistema:

Diarias	2,820
Semanales	8,745
Mensuales	38,028

Equipo mínimo necesario para que el Sistema pueda seguir funcionando:

Hardware:

- CPU full 64 bits
- Procesador 250 Mz.
- RAM 1.5 GB
- HD 2 GB

Software:

- S.O. Sun Solaris
- Motor de base de datos SYBASE (SQL Server ASE)
- Kernel Central COBIS

Cuanto tiempo la Cooperativa puede funcionar de una forma adecuada, sin disponer de la información del sistema.

_____0_____Horas _____Días

Actividades a realizar para volver a contar con el Sistema de Información (actividades de Restore).

Hardware: En caso de daños de piezas y partes se mantiene un contrato de mantenimiento del Host Central de 24x7x365 con la empresa COMWARE con el compromiso de préstamo de equipo de iguales características en caso de no resolverse el problemas en forma inmediata con tiempos de respuesta para la solución de 2h00 como máximo.

Software:

- Chequeo de la BDD con DBCC propios de Sybase
- Bajar y subir el Motor Transacción SYBASE

En caso de no reaccionar.

- Subir el servidor de backup
- Levantar el último respaldo de la noche anterior después del cierre de día, de la cinta copia que reposa en archivador-caja fuerte que reposa en el departamento de sistemas.
- Y Colocar en online la BDD

Nombre del Sistema: CARTERA

Lenguaje o Paquete en que fue creado el sistema:
VISUAL BASIC 6.0 front-ent, SYBASE back-end (BDD)

Gerencia, Departamento(s) que genera la información:

Cajas, Cartera, Crédito y cobranzas

Las unidades o departamentos (internos/externos) que usan la información del Sistema:

INTERNAS

Contabilidad, Riesgos, Tesoreria, Negocios, Marketing, Servicio al Cliente,

Cartera, Crédito y cobranzas, auditoria.

EXTERNAS

- SuperIntendencia de bancos y seguros (SIB)
- SRI
- CONSEP

Volumen de transacciones que maneja el sistema:

Diarias	5,608
Semanales	27,673
Mensuales	118,245

Equipo mínimo necesario para que el Sistema pueda seguir funcionando:

Hardware:

- CPU full 64 bits
- Procesador 250 Mz.
- RAM 1.5 GB
- HD 2 GB

Software:

- S.O. Sun Solaris
- Motor de base de datos SYBASE (SQL Server ASE)
- Kernel Central COBIS

Cuanto tiempo la Cooperativa puede funcionar de una forma adecuada, sin disponer de la información del sistema.

_____12_____Horas _____Días

Actividades a realizar para volver a contar con el Sistema de Información (actividades de Restore).

Hardware: En caso de daños de piezas y partes se mantiene un contrato de mantenimiento del Host Central de 24x7x365 con la empresa COMWARE con el compromiso de préstamo de equipo de iguales características en caso de no resolverse el problemas en forma inmediata con tiempos de respuesta para la solución de 2h00 como máximo.

Software:

- Chequeo de la BDD con DBCC propios de Sybase
- Bajar y subir el Motor Transacción SYBASE

En caso de no reaccionar.

- Subir el servidor de backup
- Levantar el último respaldo de la noche anterior después del cierre de día, de la cinta copia (respaldo) que reposa en archivador-caja fuerte que reposa en el departamento de sistemas.
- Y Colocar en online la BDD

Nombre del Sistema: CRÉDITO Y COBRANZAS

Lenguaje o Paquete en que fue creado el sistema:
VISUAL BASIC 6.0 front-ent, SYBASE back-end (BDD)

Gerencia, Departamento(s) que genera la información:

Cartera, Crédito y cobranzas

Las unidades o departamentos (internos/externos) que usan la información del Sistema:

INTERNAS

Contabilidad, Riesgos, Tesorería, Crédito y cobranzas, auditoria.

Volumen de transacciones que maneja el sistema:

Diarias	33
Semanales	137
Mensuales	622

Equipo mínimo necesario para que el Sistema pueda seguir funcionando:

Hardware:

- CPU full 64 bits

- Procesador 250 Mz.
- RAM 1.5 GB
- HD 2 GB

Software:

- S.O. Sun Solaris
- Motor de base de datos SYBASE (SQL Server ASE)
- Kernel Central COBIS

Cuanto tiempo la Cooperativa puede funcionar de una forma adecuada, sin disponer de la información del sistema.

_____Horas _____1_____Días

Actividades a realizar para volver a contar con el Sistema de Información (actividades de Restore).

Hardware: En caso de daños de piezas y partes se mantiene un contrato de mantenimiento del Host Central de 24x7x365 con la empresa COMWARE con el compromiso de prestamo de equipo de iguales caracteristicas en caso de no resolverse el problemas en forma inmediata con tiempos de respuesta para la solicion de 2h00 como maximo.

Software:

- Chequeo de la BDD con DBCC propios de Sybase
- Bajar y subir el Motor Transacción SYBASE

En caso de no reaccionar.

- Subir el servidor de backup
- Levantar el último respaldo de la noche anterior después del cierre de día, de la cinta copia que reposa en archivador-caja fuerte que reposa en el departamento de sistemas.
- Y Colocar en online la BDD

Nombre del Sistema: PLAZO FIJO

Lenguaje o Paquete en que fue creado el sistema:
VISUAL BASIC 6.0 front-ent, SYBASE back-end (BDD)

Gerencia, Departamento(s) que genera la información:

Cajas, Servicio al Cliente, Cartera, Contabilidad

Las unidades o departamentos (internos/externos) que usan la información del Sistema:

INTERNAS

Cajas, Servicio al Cliente, Cartera, Contabilidad, Riesgos, Tesoreria, auditoria.

Volumen de transacciones que maneja el sistema:

Diarias	40
Semanales	157
Mensuales	633

Equipo mínimo necesario para que el Sistema pueda seguir funcionando:

Hardware:

- CPU full 64 bits
- Procesador 250 Mz.
- RAM 1.5 GB
- HD 2 GB

Software:

- S.O. Sun Solaris
- Motor de base de datos SYBASE (SQL Server ASE)
- Kernel Central COBIS

Cuanto tiempo la Cooperativa puede funcionar de una forma adecuada, sin disponer de la información del sistema.

_____Horas _____6_____Días

Actividades a realizar para volver a contar con el Sistema de Información (actividades de Restore).

Hardware: En caso de daños de piezas y partes se mantiene un contrato de mantenimiento del Host Central de 24x7x365 con la empresa COMWARE con el compromiso de prestamo de equipo de iguales caracteristicas en caso de no resolverse el problemas en forma inmediata con tiempos de respuesta para la solicion de 2h00 como maximo.

Software:

- Chequeo de la BDD con DBCC propios de Sybase
- Bajar y subir el Motor Transacción SYBASE

En caso de no reaccionar.

- Subir el servidor de backup
- Levantar el ultimo respaldo de la noche anterior después del cierre de dia de la cinta copia que reposa en archivador-caja fuerte que reposa en el departamento de sistemas.
- Y Colocar en online la BDD

Nombre del Sistema: CONTABILIDAD

Lenguaje o Paquete en que fue creado el sistema:
VISUAL BASIC 6.0 front-ent, SYBASE back-end (BDD)

Gerencia, Departamento(s) que genera la información:

Cajas, Servicio al Cliente, Cartera, Contabilidad, Crédito y cobranzas

Las unidades o departamentos (internos/externos) que usan la información del Sistema:

INTERNAS

Cajas, Servicio al Cliente, Cartera, Contabilidad, Riesgos, Tesoreria, auditoria, Crédito y cobranzas.

Volumen de transacciones que maneja el sistema:

Diarias	105
Semanales	2,562
Mensuales	14,160

Equipo mínimo necesario para que el Sistema pueda seguir funcionando:

Hardware:

- CPU full 64 bits

- Procesador 250 Mz.
- RAM 1.5 GB
- HD 2 GB

Software:

- S.O. Sun Solaris
- Motor de base de datos SYBASE (SQL Server ASE)
- Kernel Central COBIS

Cuanto tiempo la Cooperativa puede funcionar de una forma adecuada, sin disponer de la información del sistema.

_____Horas _____Días

La Cooperativa de Ahorro y Crédito Alianza del Valle puede funcionar en forma adecuada hasta la reparación del módulo sin problemas.

Actividades a realizar para volver a contar con el Sistema de Información (actividades de Restore).

Hardware: En caso de daños de piezas y partes se mantiene un contrato de mantenimiento del Host Central de 24x7x365 con la empresa COMWARE con el compromiso de préstamo de equipo de iguales características en caso de no resolverse el problemas en forma inmediata con tiempos de respuesta para la solución de 2h00 como máximo.

Software:

- Chequeo de la BDD con DBCC propios de Sybase
- Bajar y subir el Motor Transacción SYBASE

En caso de no reaccionar.

- Subir el servidor de backup
- Levantar el último respaldo de la noche anterior después del cierre de día, de la cinta copia que reposa en archivador-caja fuerte que reposa en el departamento de sistemas.
- Y Colocar en online la BDD

Nombre del Sistema: FIRMAS

Lenguaje o Paquete en que fue creado el sistema:
VISUAL BASIC 6.0 front-ent, SYBASE back-end (BDD)

Gerencia, Departamento(s) que genera la información:

Cajas, Servicio al Cliente.

Las unidades o departamentos (internos/externos) que usan la información del Sistema:

INTERNAS

Cajas, Servicio al Cliente, auditoria.

Volumen de transacciones que maneja el sistema:

Diarias	62
Semanales	153
Mensuales	529

Equipo mínimo necesario para que el Sistema pueda seguir funcionando:

Hardware:

- CPU full 64 bits
- Procesador 250 Mz.
- RAM 1.5 GB
- HD 2 GB

Software:

- S.O. Sun Solaris
- Motor de base de datos SYBASE (SQL Server ASE)
- Kernel Central COBIS

Cuanto tiempo la Cooperativa puede funcionar de una forma adecuada, sin disponer de la información del sistema.

_____Horas _____Días

La Cooperativa de Ahorro y Crédito Alianza del Valle puede funcionar en forma adecuada hasta la reparación del módulo sin problemas.

Actividades a realizar para volver a contar con el Sistema de Información (actividades de Restore).

Hardware: En caso de daños de piezas y partes se mantiene un contrato de mantenimiento del Host Central de 24x7x365 con la empresa COMWARE con

el compromiso de préstamo de equipo de iguales características en caso de no resolverse el problemas en forma inmediata con tiempos de respuesta para la solución de 2h00 como máximo.

Software:

- Chequeo de la BDD con DBCC propios de Sybase
- Bajar y subir el Motor Transacción SYBASE

En caso de no reaccionar.

- Subir el servidor de backup
- Levantar el último respaldo de la noche anterior después del cierre de día, de la cinta copia que reposa en archivador-caja fuerte que reposa en el departamento de sistemas.
- Y Colocar en online la BDD

Nombre del Sistema: MIS

Lenguaje o Paquete en que fue creado el sistema:
VISUAL BASIC 6.0 front-ent, SYBASE back-end (BDD)

Gerencia, Departamento(s) que genera la información:

Servicio al Cliente.

Las unidades o departamentos (internos/externos) que usan la información del Sistema:

INTERNAS

Servicio al Cliente, auditoria, Cartera, Plazo Fijo.

Volumen de transacciones que maneja el sistema:

Diarias	46
Semanales	249
Mensuales	646

Equipo mínimo necesario para que el Sistema pueda seguir funcionando:

Hardware:

- CPU full 64 bits
- Procesador 250 Mz.
- RAM 1.5 GB
- HD 2 GB

Software:

- S.O. Sun Solaris
- Motor de base de datos SYBASE (SQL Server ASE)
- Kernel Central COBIS

Cuanto tiempo la Cooperativa puede funcionar de una forma adecuada, sin disponer de la información del sistema.

_____Horas _____Días

La Cooperativa de Ahorro y Crédito Alianza del Valle puede funcionar en forma adecuada hasta la reparación del módulo sin problemas.

Actividades a realizar para volver a contar con el Sistema de Información (actividades de Restore).

Hardware: En caso de daños de piezas y partes se mantiene un contrato de mantenimiento del Host Central de 24x7x365 con la empresa COMWARE con el compromiso de préstamo de equipo de iguales características en caso de no resolverse el problemas en forma inmediata con tiempos de respuesta para la solución de 2h00 como máximo.

Software:

- Chequeo de la BDD con DBCC propios de Sybase
- Bajar y subir el Motor Transacción SYBASE

En caso de no reaccionar.

- Subir el servidor de backup
- Levantar el último respaldo de la noche anterior después del cierre de día de la cinta copia que reposa en archivador-caja fuerte que reposa en el departamento de sistemas.
- Y Colocar en online la BDD

Nombre del Sistema: RIESGOS DE MERCADO Y LIQUIDEZ

Lenguaje o Paquete en que fue creado el sistema:
VISUAL BASIC 6.0 front-ent, SYBASE back-end (BDD)

Gerencia, Departamento(s) que genera la información:

Ahorros, Cartera; Plazo Fijo, Contabilidad, Tesorería, Riegos.

Las unidades o departamentos (internos/externos) que usan la información del Sistema:

INTERNAS

Riesgos, auditoria.

Volumen de transacciones que maneja el sistema:

Alimentado por los módulos de: Ahorros, Plazo Fijo y Cartera.

Diarias	
Semanales	
Mensuales	

Equipo mínimo necesario para que el Sistema pueda seguir funcionando:

Hardware:

- CPU full 64 bits
- Procesador 250 Mz.
- RAM 1.5 GB
- HD 2 GB

Software:

- S.O. Sun Solaris
- Motor de base de datos SYBASE (SQL Server ASE)
- Kernel Central COBIS

Cuanto tiempo la Cooperativa puede funcionar de una forma adecuada, sin disponer de la información del sistema.

_____Horas _____Días

La Cooperativa de Ahorro y Crédito Alianza del Valle puede funcionar en forma adecuada hasta la reparación del módulo sin problemas.

Actividades a realizar para volver a contar con el Sistema de Información (actividades de Restore).

Hardware: En caso de daños de piezas y partes se mantiene un contrato de mantenimiento del Host Central de 24x7x365 con la empresa COMWARE con el compromiso de préstamo de equipo de iguales características en caso de no resolverse el problemas en forma inmediata con tiempos de respuesta para la solución de 2h00 como máximo.

Software:

- Chequeo de la BDD con DBCC propios de Sybase
- Bajar y subir el Motor Transacción SYBASE

En caso de no reaccionar.

- Subir el servidor de backup
- Levantar el último respaldo de la noche anterior después del cierre de día, de la cinta copia que reposa en archivador-caja fuerte que reposa en el departamento de sistemas.
- Y Colocar en online la BDD

	INTERNOS										EXTERNOS					
DEPARTAMENTOS	Cajas	Contabilidad	Riesgos	Tesoreria	Negocios	Marketing	Servicio al Cliente	Cartera	Credito y Cobranzas	Auditoria	CONSEP	AGD	SRI	Superintendencia de Bancos	Dias (D) / Horas (H) que puede funcionar la Coop. de una forma adecuada Sin disponer del sistema	Impacto
MODULOS COBIS																
Ahorros	X	X	X	X	X	X	X	X	X	X	X	X			0 H	Catastrofico
Cartera		X	X	X	X	X	X	X	X	X	X		X	X	12 H	Critico
Credito		X	X	X					X	X					1 D	Critico
Plazo Fijo	X	X	X	X			X	X		X					6 D	Marginal
Contabilidad	X	X	X	X			X	X	X	X					mas de 30 D	Despreciable
Firmas	X						X			X					mas de 30 D	Despreciable
MIS							X	X		X					mas de 30 D	Despreciable
Riesgos de Mercado y Liquidez			X							X					mas de 30 D	Despreciable

Gráfico 2.17: Análisis de Módulos COBIS

Con la información recopilada el Ranking del Sw de aplicaciones queda de la siguiente manera:

Tabla 2.14 : Ranking del Software de aplicaciones de la Cooperativa

Ranking	Nombre del Sistema
1	Ahorros
2	Cartera
3	Crédito
4	Plazo Fijo
5	Contabilidad
6	Firmas
7	MIS
8	Riesgo de Mercado y Liquidez

2.1.12. Información (Base de datos)

Las Bases de datos son fundamentales para el normal desenvolvimiento de las funciones de todos los departamentos que conforman la Cooperativa, las cuales están expuestas a varios tipos de amenazas entre las principales tenemos:

- Acciones hostiles
  - Ataques de hackers y Crackers
  - Ataques por virus, gusanos, bombas lógicas
  - Robo de información
- Suspensión del servicio
  - Falla de conexión
  - Memoria insuficiente del servidor para atender las transacciones solicitadas.

Una vez que se determinaron las principales amenazas a las que se encuentran expuestas las bases de datos de la cooperativa, a continuación se detalla el análisis de dichas amenazas y su impacto en la Cooperativa.

Tabla 2.15 : Análisis de las posibles amenazas que afectarían a las Base de datos que posee Cooperativa en el servidor central y su impacto sobre ella.

Base de Datos	Amenazas	Impacto	Calificación
Seguridades	° Acciones Hostiles ° Suspensión del servicio	Catastrófico	Imprescindible
Ahorros	° Acciones Hostiles ° Suspensión del servicio	Catastrófico	Imprescindible
Cartera	° Acciones Hostiles ° Suspensión del servicio	Catastrófico	Imprescindible
Crédito	° Acciones Hostiles ° Suspensión del servicio	Catastrófico	Imprescindible
Plazo Fijo	° Acciones Hostiles ° Suspensión del servicio	Crítico	Imprescindible
Contabilidad	° Acciones Hostiles ° Suspensión del servicio	Crítico	Imprescindible
Firmas	° Acciones Hostiles ° Suspensión del servicio	Marginal	Prioritario
MIS	° Acciones Hostiles ° Suspensión del servicio	Catastrófico	Imprescindible
Riesgos de Mercado	° Acciones Hostiles ° Suspensión del servicio	Marginal	Prioritario
Garantías	° Acciones Hostiles ° Suspensión del servicio	Crítico	Imprescindible

2.1.13. Comunicaciones

Las comunicaciones dentro de la Cooperativa es un punto de mucha importancia, es por eso que se debe tomar todas las medidas necesarias ante la presencia de amenazas que impidan su funcionamiento normal de la matriz o las agencias.

Entre las principales amenazas a las cuales se encuentran expuestas las comunicaciones tenemos las siguientes:

- Suspensión del servicio por factores internos
  - Falla del equipo a causa del mal uso o desconfiguración
  - Deterioro de cables
  - Saturación del ancho de banda
- Suspensión del servicio por factores externos
  - Perdida de las comunicaciones a causa de agentes naturales (lluvias, granizadas, tormentas eléctricas)
  - Interrupción del enlace dedicado por parte del proveedor del servicio

Una vez que se determinaron las principales amenazas a las que se encuentran expuestas las comunicaciones, a continuación se detalla el análisis de dichas amenazas y su impacto en la Cooperativa

Tabla 2.16 : Análisis de las posibles amenazas que afectarían el servicio de comunicaciones de la Cooperativa y su impacto sobre ella.

Equipo de Comunicación	Marca	Ubicación Agencia	Amenaza	Impacto	Calificación
Ruteador	Cisco 800	Matriz Inca Chillogallo	° Suspensión del servicio por factores internos ° Suspensión del servicio por factores externos	Catastrófico	Imprescindible

Switch de 16 Puertos	Cisco	Matriz	° Suspensión del servicio por factores internos ° Suspensión del servicio por factores externos	Catastrófico	Imprescindible
Switch de 12 Puertos	3Com	Matriz	° Suspensión del servicio por factores internos ° Suspensión del servicio por factores externos	Catastrófico	Imprescindible
Switch de 8 Puertos	Cnet	Ecuatoriana Conocoto	° Suspensión del servicio por factores internos ° Suspensión del servicio por factores externos	Catastrófico	Imprescindible
Hub de 16 Puertos	3Com	Machachi Amaguaña	° Suspensión del servicio por factores internos ° Suspensión del servicio por factores externos	Catastrófico	Imprescindible
Hub de 8 Puertos	3Com	Matriz Aloag Guamaní	° Suspensión del servicio por factores internos ° Suspensión del servicio por factores externos	Catastrófico	Imprescindible
Hub de 18 Puertos	3Com	Inca Chillogallo Sangolquí	° Suspensión del servicio por factores internos ° Suspensión del servicio por factores externos	Catastrófico	Imprescindible
Radio	Orinoco OR500	Matriz Sangolquí Machachi Conocoto Amaguaña Aloag	° Suspensión del servicio por factores internos ° Suspensión del servicio por factores externos	Catastrófico	Imprescindible

Radio	Rapid wave	Guamaní Ecuatoriana Inca Chillogallo	◦ Suspensión del servicio por factores internos ◦ Suspensión del servicio por factores externos	Catastrófico	Imprescindible
Antena Grilla		Matriz Inca Chillogallo Sangolquí Machachi Conocoto Amaguaña Aloag Ecuatoriana Guamaní	◦ Suspensión del servicio por factores internos ◦ Suspensión del servicio por factores externos	Catastrófico	Imprescindible

POLÍTICAS DE SEGURIDAD

Una vez que se conoce los posibles riegos y amenazas, se procede a diseñar las políticas de seguridad de la información, para evitar que éstas ocurran.

2.2. Políticas de seguridad para equipos informáticos y sistemas de Información

2.2.1. Alcance

Estas políticas se aplican a todo el personal de la COACAV que tengan a su cargo equipos informáticos.

2.2.2. Objetivos

- Normar el buen uso de los sistemas, claves o password de acceso, equipos e información Institucional.
- Instruir y evitar las sanciones por el mal uso de equipos, claves e información.
- Prevenir ingresos de usuarios no autorizados.

2.2.3. De la responsabilidad del usuario

El usuario es el responsable absoluto del buen uso y control de los accesos y claves otorgadas por la COACAV.

2.2.4. Del correcto uso del password. (Clave de acceso)

2.2.4.1. Mantener la contraseña confidencial: por ningún concepto la contraseña deberá ser: transferida, divulgada, publicada, escrita en lugares accesibles o entregada a terceras personas.

2.2.4.2. La contraseña inicial emitida a un nuevo usuario sólo debe ser válida para la primera sesión. En ese momento, el usuario debe escoger otra contraseña.

2.2.4.3. No permita gente a su alrededor cuando ingrese su contraseña.

2.2.4.4. **Password robusto:** la contraseña que usted ingrese deberá tener su nivel de complejidad:

- Utilice entre los caracteres al menos: una letra mayúscula, un número, caracteres especiales (#$%&/()=?¡", etc.) y letras minúsculas.
- La contraseña deberá tener mínimo siete caracteres.
- Nunca deje en blanco la contraseña
- No puede utilizar una contraseña que anteriormente haya registrado.
- La contraseña no deberá estar basada en nada personal fácilmente identificable o relacionada con: su nombre, número telefónico, fechas de nacimiento, nombre de miembros de su familia, etc.
- La contraseña no debe tener números o letras repetitivas.

2.2.4.5. **Cambio de contraseña:** el cambio de contraseña se realizará cada 40 días, en el caso de que requiera cambiarla en un lapso de tiempo menor, considere las recomendaciones del inciso anterior.

2.2.4.6. **Solicite ayuda a personal autorizado:** en el caso que olvide su contraseña, al tercer intento incorrecto se bloqueará su acceso y deberá comunicarse con el departamento de sistemas donde un técnico le ayudará para que usted pueda cambiar su clave por una nueva.

2.2.4.7. Los usuarios no deben intentar violar los sistemas de seguridad y de control de acceso. Acciones de esta naturaleza se consideran violatorias de las políticas de la COACAV, pudiendo ser causal de despido.

2.2.5. Del buen uso de los equipos

2.2.5.1. **Cuando no se encuentre en su lugar de trabajo**

Cuando usted tenga que alejarse momentáneamente de su computador bloquee la pantalla haciendo clic en el menú conexión (del sistema COBIS), y a continuación seleccione la opción bloquear terminal.

2.2.5.2. **Durante y al terminar su labor de trabajo**

- Se debe evitar el daño de los equipos absteniéndose de fumar, ingerir alimentos y bebidas, en las áreas de trabajo.
- Al terminar sus labores diarias, todos los sistemas y sus aplicaciones deben estar cerradas y los equipos apagados.

2.2.5.3. Los equipos de la COACAV sólo deben usarse para actividades de trabajo y no para otros fines, tales como juegos y pasatiempos.

2.2.5.4. Debe respetarse y no modificar la configuración de hardware y software establecida por el Departamento de Sistemas.

2.2.5.5. No pueden moverse los equipos o reubicarlos sin permiso. Para llevar un equipo fuera de la COACAV se requiere una autorización escrita.

2.2.5.6. La pérdida o robo de cualquier componente de hardware o programa de software debe ser reportada inmediatamente.

2.2.5.7. No deben usarse diskettes u otros medios de almacenamiento en cualquier computadora de la COACAV a menos que se haya previamente verificado que están libres de virus u otros agentes dañinos.

2.2.6. Del buen uso de la información

2.2.6.1. Los datos confidenciales que aparezcan en la pantalla deben protegerse de ser vistos por otras personas mediante disposición apropiada del mobiliario de la oficina y protector de pantalla. Cuando ya no se necesiten o no sean de utilidad, los datos confidenciales se deben borrar.

2.2.6.2. La información que ya no se necesita deben ser eliminada periódicamente de su área de almacenamiento. Con esto se reducen los riesgos de que otros puedan acceder a esa información y además se libera espacio en disco.

2.2.6.3. Los usuarios no deben copiar a un medio removible (como un diskette), el software o los datos residentes en las computadoras de la COACAV, sin la aprobación previa de la gerencia.

2.2.6.4. No pueden extraerse datos fuera de la sede de la COACAV sin la aprobación previa de la gerencia. Esta política es particularmente pertinente a aquellos que usan a computadoras portátiles o están conectados a redes como Internet.

2.2.7. De las Obligaciones, Infracciones y Sanciones

2.2.7.1. **Son Obligaciones del personal:**

- Conocer, cumplir y hacer cumplir las disposiciones, reglamentos, manuales y políticas expedidos por la COACAV.
- Regir su comportamiento bajo normas de la moral, la ética, las buenas costumbres, la disciplina, la responsabilidad y la cordialidad.

- Cuidar de los bienes de la COACAV y responder por aquellos bienes, equipos y herramientas que le fueren asignados o que estén a su cargo, restituyendo los materiales que no fueren utilizados.
- Dar aviso a su Jefe inmediato o a las autoridades de la COACAV, en forma inmediata, sobre actos, hechos o situaciones que pudieren causar daño, tanto a los recursos humanos como a las instalaciones o a los recursos materiales de la COACAV, así como los hechos que pudieren afectar a la buena imagen o a la productividad de la COACAV.
- Guardar escrupulosamente los secretos técnicos, comerciales, de construcción, instalación o proyectos de la COACAV, en cuya elaboración participe directa o indirectamente, o de los que tenga conocimiento en razón de su trabajo.
- Abstenerse de entregar a cualquier persona copias u originales de documentos, o disquetes en los que consten actas, contratos, anotaciones, diagramas, cálculos, planos u otros instrumentos que contengan datos o informaciones calificados como confidenciales, y que sean de propiedad de la COACAV, cuya difusión o conocimiento por parte de terceros pueda entrañar perjuicio comercial o de otra índole para la COACAV.

2.2.8. Son Infracciones y Faltas Graves

2.2.8.1. Utilizar indebidamente o para fines personales herramientas, útiles y otros bienes de propiedad de la COACAV, así como los servicios de comunicación (teléfono, fax), fotocopiado, y demás facilidades, sin el consentimiento y la aplicación de las normas de uso y restricciones determinados por la COACAV.

2.2.8.2. Divulgar o revelar cualquier información que tenga el carácter de reservada que hubiere conocido en razón de su trabajo, y que pueda perjudicar de cualquier manera a la COACAV, a sus funcionarios o trabajadores, a sus clientes o a sus socios, a menos que esté autorizado para ello en función de la labor que desempeña.

2.2.8.3. Realizar o permitir que se realice cualquier acto que cause daño a las pertenencias e instalaciones de la COACAV, o que ponga en peligro la seguridad e integridad del personal.

2.2.8.4. Incumplir las órdenes y disposiciones que les impartan los jefes para el cumplimiento de las tareas inherentes a sus obligaciones, en forma oportuna y eficiente.

2.2.9. Sanciones

En caso de incumplimiento de las disposiciones de estas Políticas por parte del empleado o trabajador, la autoridad correspondiente, tomando en cuenta la gravedad de la falta, la reincidencia y las condiciones de cada caso, procederá a la aplicación de las siguientes sanciones:

- Amonestación escrita;
- Visto Bueno para la terminación del contrato de trabajo.

2.2.10. Vigencia de la política

Las políticas de seguridad para equipos informáticos y sistemas de Información entraran en vigencia desde: (fecha en que entrará en vigencia la política)

Nota: Esta fecha depende de los directivos de la COACAV. La documentación se encuentra lista y aprobada para su implementación.

2.2.11. Frecuencia de revisión de la conveniencia y obsolescencia de la política.

Se evaluarán las políticas del presente documento, con una frecuencia anual a partir de la vigencia de las mismas o cuando el Jefe de Sistemas lo determine.

En caso de preguntas o sugerencias contactarse con el Jefe de Sistemas a los teléfonos 2335-372 - 2332-085 - 2330-060 ext. 112/113 o al correo electrónico: rllumiquinga@alianzadelvalle.fin.ec

2.2.12. Glosario de términos

COACAV: Cooperativa de ahorro y crédito “Alianza del Valle” Ltda.

Password: contraseña, identificación de acceso a la información de un sistema o servicio. Las palabras password y contraseña se utilizan indistintamente en este documento.

Usuario: Personal responsable que utiliza el computador, sistemas claves y programas.

Caracteres: Cualquier número, letra, símbolo o espacio en blanco que se genere por el teclado de un computador.

2.3. Políticas de seguridad para las Redes

2.3.1. Alcance

Esta política se aplica al personal técnico y temporal del departamento de sistemas de la COACAV.

2.3.2. Objetivo

- Establecer las directrices, los procedimientos y los requisitos para asegurar la protección apropiada de la COACAV al estar conectada a redes de computadoras.

2.3.3. De la responsabilidad del personal

Conocer, cumplir y hacer cumplir las disposiciones expedidas en esta política.

2.3.4. De las cuentas de usuarios

2.3.4.1. Cuando un usuario recibe una nueva cuenta, debe firmar un documento donde declara conocer las políticas y procedimientos de seguridad, y acepta sus responsabilidades con relación al uso de esa cuenta.

2.3.4.2. La solicitud de una nueva cuenta o el cambio de privilegios debe ser hecha por escrito y debe ser debidamente aprobada.

2.3.4.3. No debe concederse una cuenta a personas que no sean empleados de la COACAV a menos que estén debidamente autorizados, en cuyo caso la cuenta debe expirar automáticamente al cabo de un lapso de 30 días.

2.3.4.4. Privilegios especiales, tal como la posibilidad de modificar o borrar los archivos de otros usuarios, sólo deben otorgarse a aquellos directamente responsable de la administración o de la seguridad de los sistemas.

2.3.4.5. No deben otorgarse cuentas a técnicos de mantenimiento ni permitir su acceso remoto a menos que el Administrador de Sistemas o el Jefe de Sistemas determinen que es necesario. En todo caso esta facilidad sólo debe habilitarse para el periodo de tiempo requerido para efectuar el trabajo (como por ejemplo, el mantenimiento remoto).

2.3.4.6. Se prohíbe el uso de cuentas anónimas o de invitado (guest) y los usuarios deben entrar al sistema mediante cuentas que indiquen claramente su identidad. Esto también implica que los usuarios del sistema Sun Solaris no deben entrar inicialmente como “root”, sino primero empleando su propio ID y luego mediante “set userid” para obtener el acceso como "root". En cualquier caso debe registrarse en la bitácora todos los cambios de ID.

2.3.4.7. Toda cuenta queda automáticamente suspendida después de un cierto periodo de inactividad. El periodo recomendado es de 30 días.

2.3.4.8. Los privilegios del sistema concedidos a los usuarios deben ser ratificados cada 6 meses. El Administrador de Sistemas debe revocar rápidamente la cuenta o los privilegios de un usuario cuando reciba una orden de un superior, y en particular cuando un empleado cesa en sus funciones.

2.3.4.9. Cuando un empleado es despedido o renuncia a la COACAV, debe desactivarse su cuenta antes de que deje el cargo.

2.3.5. De los equipos de comunicación

2.3.5.1. Las contraseñas predefinidas que traen los equipos nuevos tales como routers, switchs, etc., deben cambiarse inmediatamente al ponerse en servicio el equipo.

2.3.5.2. Todos los cambios en la central telefónica (PABX) y en los servidores y equipos de red de la COACAV, incluyendo la instalación de el nuevo software, el cambio de direcciones IP, la reconfiguración de routers y switchs, deben ser documentados y debidamente aprobados, excepto si se trata de una situación de emergencia. Todo esto es para evitar problemas por cambios apresurados y que puedan causar interrupción de las comunicaciones, caída de la red, denegación de servicio o acceso inadvertido a información confidencial.

2.3.5.3. Para prevenir la intrusión de hackers a través de puertas traseras, no está permitido el uso de módems en PCs que tengan también conexión a la red local (LAN), a menos que sea debidamente autorizado.

2.3.5.4. Los archivos de bitácora (logs) y los registros de auditoria (audit trails) que graban los eventos relevantes sobre la seguridad de los sistemas informáticos y las comunicaciones, deben revisarse periódicamente y guardarse durante un tiempo prudencial de por lo menos tres meses. Dicho archivos son importantes para la detección de intrusos, brechas en la seguridad, investigaciones, y otras actividades de auditoria. Por tal razón deben protegerse para que nadie los pueda alterar y que sólo los pueden leer las personas autorizadas.

2.3.5.5. Los servidores de red y los equipos de comunicación (PABX, routers, etc.) deben estar ubicados en locales apropiados, protegidos contra daños y robo. Debe restringirse severamente el acceso a estos

locales y a los cuartos de cableado a personas no autorizadas mediante el uso de cerraduras y otros sistemas de acceso.

2.3.6. Sanciones

En caso de incumplimiento de las disposiciones de estas Políticas por parte del empleado o trabajador, la autoridad correspondiente, tomando en cuenta la gravedad de la falta, la reincidencia y las condiciones de cada caso, procederá a la aplicación de las siguientes sanciones:

- Amonestación escrita;
- Visto Bueno para la terminación del contrato de trabajo.

2.3.7. Vigencia de la política

Las políticas de seguridad para las Redes entraran en vigencia desde: (fecha en que entrará en vigencia la política)

Nota: Esta fecha depende de los directivos de la COACAV. La documentación se encuentra lista y aprobada para su implementación.

2.3.8. Frecuencia de revisión de la conveniencia y obsolescencia de la política.

Se evaluarán las políticas del presente documento, con una frecuencia anual a partir de la vigencia de las mismas o cuando el Jefe de Sistemas lo determine.

En caso de preguntas o sugerencias contactarse con el Jefe de Sistemas a los teléfonos 2335-372 - 2332-085 - 2330-060 ext. 112/113 o al correo electrónico: rllumiquinga@alianzadelvalle.fin.ec

2.3.9. Glosario de términos

COACAV: Cooperativa de ahorro y crédito “Alianza del Valle” Ltda.

Root: En sistemas basados en Unix se refiere a usuario principal.

Router: Dispositivo que envía paquetes de datos de una red a otra, mediante el uso de tablas y protocolos de enrutamiento. Selecciona el mejor camino para que la información atraviese la red.

Switch: Término general que se aplica a un dispositivo electrónico o mecánico que permite que una conexión se establezca según sea necesario y se termine cuando ya no haya ninguna sesión para soportar.

PABX: central para extensiones telefónicas, sistema de teléfonos pertenecientes a una organización.

Hacker: Experto en informática capaz de entrar en sistemas cuyo acceso es restringido. No necesariamente con malas intenciones.

2.4. Políticas de seguridad para las comunicaciones

2.4.1. Alcance

Estas políticas se aplican a todos los empleados y personal temporal de la COACAV.

2.4.2. Objetivos

- Mejorar la productividad de la COACAV.
- Promover el uso responsable de las comunicaciones en forma electrónica, en particular el teléfono, el correo electrónico, Internet y el fax.

2.4.3. De la responsabilidad de los usuarios

Conocer, cumplir y hacer cumplir las disposiciones expedidas en esta política.

2.4.4. De los sistemas de comunicación

2.4.4.1. Los sistemas de comunicación (teléfono, correo electrónico, Internet, fax) de la COACAV generalmente sólo deben usarse para actividades de trabajo. El uso personal en forma ocasional es permisible siempre y cuando consuma una cantidad mínima de tiempo y recursos, y además no interfiera con la productividad del empleado ni con las actividades de la COACAV.

2.4.4.2. Se prohibe el uso de los sistemas de comunicación para actividades comerciales privadas o para propósitos de entretenimiento y diversión.

2.4.5. Del Internet

2.4.5.1. Los recursos, servicios y conectividad disponibles vía Internet abren nuevas oportunidades, pero también introducen nuevos riesgos. En particular, no debe enviarse a través de Internet mensajes con información confidencial a menos que ésta se encuentre cifrada.

2.4.5.2. La navegación en Internet para fines personales no debe hacerse a expensas del tiempo y los recursos de la COACAV y en tal sentido deben usarse las horas no laborables.

2.4.5.3. No debe utilizarse software bajado de Internet y en general software que provenga de una fuente no confiable, a menos que se haya sido comprobado en forma rigurosa y que esté aprobado su uso por el Departamento de Sistemas.

2.4.5.4. Para prevenir demandas legales o la introducción de virus informáticos, se prohíbe estrictamente la instalación de software no autorizado, incluyendo el que haya sido adquirido por el propio usuario. Así mismo, no se permite el uso de software de distribución gratuita o shareware, a menos que haya sido previamente aprobado por el Departamento de Informática.

2.4.6. De la confidencialidad y privacidad

2.4.6.1. Los empleados y funcionarios de la COACAV no deben interceptar las comunicaciones o divulgar su contenido. Tampoco deben ayudar a otros para que lo hagan. La COACAV se compromete a respetar los derechos de sus empleados, incluyendo su privacidad. También se hace responsable del buen funcionamiento y del buen uso de sus redes de comunicación y para lograr esto, ocasionalmente es necesario interceptar ciertas comunicaciones.

2.4.6.2. Es política de la COACAV no monitorear regularmente las comunicaciones. Sin embargo, el uso y el contenido de las comunicaciones puede ocasionalmente ser supervisado en caso de ser necesario para actividades de mantenimiento, seguridad o auditoria. Puede ocurrir que el personal técnico vea el contenido de

un mensaje de un empleado individual durante el curso de resolución de un problema.

2.4.6.3. Cierta clase de información será capturada por parte del departamento de sistemas, para tener evidencias en casos de acciones disciplinarias y judiciales, cuando se sospeche que se esté llevando a cabo abuso, fraude u otro crimen que involucre los sistemas informáticos.

2.4.6.4. De manera consistente con prácticas generalmente aceptadas, la COACAV procesa datos estadísticos sobre el uso de los sistemas de comunicación. Como ejemplo, los reportes de la central telefónica (PABX) contienen detalles sobre el número llamado, la duración de la llamada, y la hora en que se efectuó la llamada.

2.4.7. Sanciones

En caso de incumplimiento de las disposiciones de estas Políticas por parte del empleado o trabajador, la autoridad correspondiente, tomando en cuenta la gravedad de la falta, la reincidencia y las condiciones de cada caso, procederá a la aplicación de las siguientes sanciones:

- Amonestación escrita;
- Visto Bueno para la terminación del contrato de trabajo.

2.4.8. Vigencia de la política

Las políticas de seguridad para las comunicaciones entraran en vigencia desde: (fecha en que entrará en vigencia la política).

Nota: Esta fecha depende de los directivos de la COACAV. La documentación se encuentra lista y aprobada para su implementación.

2.4.9. Frecuencia de revisión de la conveniencia y obsolescencia de la política.

Se evaluarán las políticas del presente documento, con una frecuencia anual a partir de la vigencia de las mismas o cuando el Jefe de Sistemas lo determine.

En caso de preguntas o sugerencias contactarse con el Jefe de Sistemas a los teléfonos 2335-372 - 2332-085 - 2330-060 ext. 112/113 o al correo electrónico: rllumiquinga@alianzadelvalle.fin.ec

2.4.1.0. Glosario de términos

COACAV: Cooperativa de ahorro y crédito “Alianza del Valle” Ltda.

Correo electrónico: Sistema de mensajería informática similar en muchos aspectos al correo ordinario pero muchísimo más rápido.

Internet: Red de ordenadores mundial que permite comunicación y transferencia de datos, noticias y opiniones entre personas y usuarios conectadas a ella.

Software: Término genérico que designa al conjunto de programas operativos que posibilitan el uso del ordenador.

Shareware: Software distribuido en calidad de prueba. Al cabo de cierto tiempo de uso (generalmente 30 días) el usuario tiene la opción de comprarlo.

Virus informático: Pieza de código ejecutable con habilidad de reproducirse, regularmente escondido en documentos electrónicos, que causan problemas al ocupar espacio de almacenamiento, así como destrucción de datos y reducción del desempeño de un equipo de cómputo.

CAPITULO III

Plan de Contingencias

Actividades previas al desastre

3.1. Medidas de Precaución (Plan de Prevención)

Al implementar un plan de prevención, estamos encaminados a procurar tener las medidas adecuadas para evitar que un desastre informático suceda y de presentarse, sus daños sean mínimos, ya que la continuidad del negocio, es vital para cualquier organización, al haber realizado, el análisis de riesgos, haber establecido la situación actual de la Cooperativa, se logra establecer y dar las recomendaciones adecuadas que nos llevarán a prevenir una interrupción en la organización.

En función, al análisis de riesgos, y a la situación actual de la Cooperativa, se recomienda lo siguiente:

La ejecución de las actividades recomendadas en el presente plan dependerá de los directivos de la Cooperativa.

3.1.1. Infraestructura Física

- Se debe retirar la alfombra existente en el departamento de sistemas con el fin de prevenir incendios.
- No debe existir materiales inflamables dentro de las instalaciones de la Cooperativa.

3.1.2. Acceso al departamento de sistemas

- Se debe mejorar la seguridad en el departamento de sistemas, para que su ingreso sea restringido solo para personal autorizado.

3.1.3. Instalaciones Eléctricas

- Se debe realizar la adaptación de un sistema automático para el encendido de la planta de energía eléctrica.
- Las instalaciones eléctricas deberán ser revisadas periódicamente para comprobar su correcto funcionamiento.

3.1.4. Detectores de humo y alarmas

- Se debe adquirir e instalar, un sistema de alarmas y detectores de humo para todo el edificio
- Para el cuarto de servidores instalar un sistema automático contra incendios a base de gas, por lo que es fundamental que el cuarto este bien cerrado sin escape de aire.

3.1.5. Extintores de Incendio

- Adquirir extintores de incendio de forma urgente, ubicarlos en lugares estratégicos y capacitar al personal que elabora en las instalaciones de la Cooperativa en el uso de dichos extintores.
- Para el cuarto de servidores se deberá adquirir extintores con componente de soda, material que se recomienda para que los equipos informáticos no sufran daños.

3.1.6. Cableado estructurado

- Contratar a una empresa calificada para que certifique y documente de una manera detallada el cableado estructurado, para que se cumpla con las normas y estándares establecidos.

3.1.7. Acceso al cuarto de servidores

- La puerta de ingreso al cuarto de servidores deberá estar permanecer cerrada con llave.

- Mejorar la seguridad del cuarto de servidores preferiblemente con una cerradura electrónica.

3.1.8. Hardware

- Realizar mantenimientos preventivos a todos los equipos de computación de la Cooperativa
- Se deberá contratar un seguro para los equipos de computación el cual permita recuperar los equipos aplicando la garantía, en el caso de presentarse algún desastre.
- Se colocara un sello de seguridad en el CPU para que no sean abiertos por personal no autorizado.
- Solo el personal de sistemas, estará autorizado para sacar equipos de computación fuera de las instalaciones de la Cooperativa.

3.1.9. Software

- Se debe adquirir las licencias para el correcto funcionamiento del software en los equipos que posee la Cooperativa, debido que al realizarse una inspección se estaría sujeto a sanciones.
- Mantener los manuales del software que posee la Cooperativa en un lugar accesible para el personal del departamento de sistemas.
- Solo el personal de sistemas estará autorizado para instalar programas en los equipos de computación de la Cooperativa.

3.1.10. Comunicaciones

- Se tiene que mantener en un lugar adecuado y de fácil acceso para el personal de sistemas, los manuales de los equipos de comunicación.
- Solo el personal de sistemas será autorizado para manipular los equipos de comunicación.

- Se deberá mantener equipos de comunicación como son Hubs, Switch, routers adicionales para que sirvan de backups.

3.2. Establecimiento del Plan de Acción

Toda vez que el Plan de acción es general y contempla una pérdida total en esta fase de planeamiento se debe establecer los procedimientos relativos a:

3.2.1. Sistemas de aplicación (Software)

Si Por motivos del desastre el Sistema COBIS deja funcionar correctamente o queda inhabilitado se deberá seguir los siguientes pasos:

La persona responsable y asignada para los sistemas de aplicación es la Tgla. Jenny Gualotuña la cual deberá realizar las siguientes acciones:

- Informar al Jefe de la Unidad de Sistemas (Ing. Ramiro Llumiquinga).

Lugar	# de Teléfono
Domicilio	2860671
Celular	094694187
Oficina	2335-372 - 2332-085 - 2330-060 ext. 112/113

- Verificar que módulos del sistema COBIS no funcionan correctamente.
- Se indicará al personal encargado para que retire los respaldos de Sistema Operativo, software base y software aplicativo (front end)
- Instalación o reparación de los archivos y programas en mal funcionamiento según lista priorizada (ranking) de los Sistemas de Información (Ver tabla 2.14)
- Llenar Bitácora

3.2.2. Información (Base de datos)

La persona responsable y asignada para los sistemas de aplicación es la Tgla. Jenny Gualotuña la cual deberá realizar las siguientes acciones:

- Informar al Jefe de la Unidad de Sistemas (Ing. Ramiro Llumiquinga) en que base de datos se encuentra el problema.

Lugar	# de Teléfono
Domicilio	2860671
Celular	094694187
Oficina	2335-372 - 2332-085 - 2330-060 ext. 112/113

- Bajar y subir el Motor Transacción SYBASE
- Chequeo de la BDD con DBCC propios de Sybase
- En caso de no se solucione el problema se indicara al personal encargado que retire el respaldo de la noche anterior después del cierre de día
- Subir el servidor de backup con el respaldo que se menciona en el paso anterior
- Por ultimo poner en Línea la BDD.

3.2.3. Equipos de cómputo (Hardware)

La persona responsable y asignada para los equipos de cómputo tanto en estaciones de trabajo como servidor central es el Tglo. Fernando Socasi el cual deberá realizar las siguientes acciones:

Estaciones de Trabajo

- Informar al Jefe de la Unidad de Sistemas (Ing. Ramiro Llumiquinga)

Lugar	# de Teléfono
Domicilio	2860671
Celular	094694187
Oficina	2335-372 - 2332-085 - 2330-060 ext. 112/113

- El departamento de sistemas deberá verificar el daño y su posible solución así como escoger el equipo informático que este en buenas condiciones para su utilización
- En caso que los equipos informáticos hayan sufrido daños irreparables, se procederá a la utilización de los equipos despreciables (baja prioridad según tabla 2.12 y que hayan sufrido menos daños), lo cual permitirá trabajar con estos equipos hasta proceder a reemplazarlos
- Llenar Bitácora
- Si no existiere equipo informático para que haya un normal desenvolvimiento de la Cooperativa, se hará la adquisición de nuevas computadoras

Servidor Central

- Informar al Jefe de la Unidad de Sistemas (Ing. Ramiro Llumiquinga)

Lugar	# de Teléfono
Domicilio	2860671
Celular	094694187
Oficina	2335-372 - 2332-085 - 2330-060 ext. 112/113

- Llamar a la empresa COMWARE con la cual se tiene un contrato de mantenimiento del Servidor Central de 24x7x365 con el compromiso de préstamo de equipo de iguales características

Lugar	# de Teléfono
Oficina	2266777

- Llenar Bitácora

Normas a tener en cuenta:

- Inventario actualizado de equipos
- Pólizas de Seguros Comerciales.
- Señalización o etiquetado de los Computadores.
- Es de mucha ayuda tener etiquetado los equipos informáticos de acuerdo a la importancia de su contenido, para ser priorizados en caso de evacuación.
- Los equipos de la Cooperativa se etiquetarán de la siguiente manera:

Color de Etiqueta	Equipos
Rojo	Servidores
Amarillo	Equipos con información importante o estratégica
Verde	Equipos con contenidos normales

3.2.4. Comunicaciones

La persona responsable y asignada para las comunicaciones es el Tglo. Fernando Socasi el cual deberá realizar las siguientes acciones:

- Informar al Jefe de la Unidad de Sistemas (Ing. Ramiro Llumiquinga)

Lugar	# de Teléfono
Domicilio	2860671
Celular	094694187
Oficina	2335-372 - 2332-085 - 2330-060 ext. 112/113

- Verificar con que agencias no se tiene comunicaciones
- Llamar a los Proveedores de enlaces dedicados para pedir la verificación del estado de la conexión, y poder recuperar las conexiones dedicadas en el menor tiempo posible.

Empresa	# de Teléfono
FULLDATA	2440972
TELEHOLDING	2560600

- Llenar Bitácora
- Si el problema es en los equipos de red
- El Administrador de la red deberá verificar el daño y su posible solución
- Verificar el estado de los Hubs, Switch y configuración del los Routers
- Probar cables de conexión
- En caso de que los equipos de comunicación hayan sufrido daños, reemplazar con los dispositivos de backup de hub, Switch y Router, para entrar en funcionamiento inmediatamente.

3.2.5. Cableado Estructurado

Debido a que no se mantiene ningún contrato con alguna empresa para el mantenimiento del cableado los problemas que se presentan deberán ser solucionados por parte del departamento de sistemas. La persona responsable y asignada para las comunicaciones es el Tglo. Alfredo Oña el cual deberá realizar las siguientes acciones:

Informar al Jefe de la Unidad de Sistemas (Ing. Ramiro Llumiquinga)

Lugar	# de Teléfono
Domicilio	2860671
Celular	094694187
Oficina	2335-372 - 2332-085 - 2330-060 ext. 112/113

- El Administrador de red deberá verificar los daños y su posible solución
- Llenar bitácora

Finalmente en caso de presentarse un siniestro en horas no hábiles o que la persona encargada para realizar las tareas mencionadas anteriormente en cada área no se encuentre en las instalaciones de la Cooperativa se detalla un cuadro con los números telefónicos de dichas personas.

Cuadro 3.1: Números telefónicos de las personas responsables de realizar las actividades del plan de acción.

Responsable	**Área**	**Teléfono Domicilio**	**Celular**
Jenny Gualotuña	▪ Sistemas de aplicación (COBIS) ▪ Base de Datos	2878541	094353677
Fernando Socasi	▪ Equipos de computo ▪ Comunicaciones	2878882	094694185
Alfredo Oña	▪ Cableado estructurado	No disponible	098588586

Actividades durante el Desastre

Una vez presentada la Contingencia o Siniestro, se deberá ejecutar las siguientes actividades:

3.3. Plan de Emergencias

3.3.1. Vías de salida o escape

Matriz

Existen dos vías de escape por donde el personal así como los clientes de la Cooperativa puede evacuar en caso de presentarse un siniestro.

La primera vía de escape es la entrada principal (norte), que da hacia la cancha de fútbol.

La segunda vía de escape es la entrada secundaria (Sur), que da hacia el parqueadero.

Agencias

En las agencias la única vía de escape que se tiene son las entradas principales de cada agencia.

3.3.2. Plan de evacuación del personal

Matriz

Los sitios de reunión son los siguientes:

Bloque A: Cancha de fútbol

El Bloque A queda conformado por los siguientes departamentos: Cartera, Cobranzas, Auditoria, Suministros, Legal y RRHH.

Bloque B: Área de estacionamiento

El Bloque B queda conformado por los siguientes departamentos: Sistemas, Cajas, Servicio al cliente, Tesorería, Contabilidad y Secretaria

Agencias

En el caso de las agencias el sitio de reunión será en las afueras de las entradas principales.

3.3.3. Recomendaciones generales para todo el personal

En el momento de la evacuación todo el personal debe salir libre de elementos (maletines, cartucheras, loncheras, etc.)

Que hacer Durante

Incendios

- Llame de inmediato a los bomberos y organismos de socorro (Persona encargada: Guardia)
- Evacuar el lugar, ubíquese en los sitios señalados y espere a que se normalice la situación.
- No corra, no grite, no haga ruidos innecesarios, no cause confusión
- Si se encuentra en un lugar lleno de humo salga agachado cubriéndose nariz y boca con algún textil húmedo, pues el humo tiende a subir y puede morir asfixiado.
- Si su ropa se incendia no corra, arrójese al suelo y dé vueltas.

Movimientos telúricos

- Conserve la calma y controle los brotes de pánico que se puedan generar
- Si se encuentra bajo techo protéjase de la caída de ladrillos, lámparas, artefactos eléctricos, maderas, bibliotecas, cuadros, equipos de computación, tableros, etc.
- Aléjese de vidrios y protéjase debajo de marcos de puertas, mesas, escritorios o de un lugar resistente de la edificación.

- En el área externa a la Cooperativa, aléjese de paredes, postes, árboles, cables eléctricos y otros elementos que puedan caerse.

Que hacer después

Incendio

- No obstruya la labor de los bomberos y organismos de socorro
- Cerciórese que no ha quedado ningún foco de nuevos incendios.
- Una vez apagado el incendio, cerciórese a través de personal experto, que la estructura no haya sufrido debilitamiento.

Movimiento Telúrico

- Evacuar el lugar y ubíquese en los sitios señalados por grupos y espere a que se normalice la situación.
- Se debe tener en cuenta que los organismos de socorro pueden estar ocupados atendiendo otras emergencias, por lo cual se debe tratar de resolver los problemas que se generen al interior de la Cooperativa.
- Si queda atrapado procure utilizar una señal visible o sonora
- No difunda rumores, ya que puede causar descontrol y desconcierto entre los compañeros y familiares.
- Antes de iniciar las actividades, revise el estado de deterioro en que quedaron las diferentes oficinas
- Observe si hay personas heridas, no mueva a los lesionados a no ser que estén en peligro de sufrir nuevas heridas.
- No pise escombros en forma indiscriminada, si requiere moverlos sea muy cuidadoso; al hacerlo puede pisar o tumbar muros o columnas

débiles ya que pueden estar soportando estructuras las cuales probablemente se caerán ante cualquier movimiento.

3.3.4. Plan de puesta a buen recaudo de los activos (incluyendo los activos de Información) de la Institución

Si bien la premisa básica es la protección de la Integridad del personal, en caso de que el siniestro lo permita (por estar en un inicio o estar en un área cercana, etc.), deberá de existir un equipo para el salvamento de los recursos Informáticos.

3.3.4.1. Equipos de cómputo (Hardware)

Al presentarse el siniestro los operadores (Hardware) del plan deberán evacuar y poner en el lugar destinado para dicho efecto, los equipos de acuerdo a los lineamientos o importancia de su contenido según el color de las etiquetas colocadas para tal fin.

3.3.4.2. Información (BDD)

De la misma manera el operador (BDD) del plan deberá evacuar las cintas correspondientes a los respaldos antes y después del cierre del día anterior.

3.3.5. Asignación de funciones

Coordinador General del Plan de Evacuación: Ing. Ramiro Llumiquinga

Sus funciones serán:

- Comunicar al personal del lugar destinado para guardar los elementos evacuados.
- Informar sobre los daños o pérdidas presentadas durante la aplicación real del plan.
- Es responsable de velar por los elementos evacuados.

- Ordenar la elaboración de inventarios después de presentado el siniestro, con el fin de constatar el estado en que se encuentran los elementos evacuados y cuantificar las pérdidas.
- Estar enterado del contenido del plan.

Operadores (hardware) del Plan: Fernando Socasi, Alfredo Oña

Sus funciones serán:

- Evacuar los equipos de computación y de comunicación según la importancia de su contenido.
- Deben estar enterados del contenido del plan

Operador (BDD) del Plan: Jenny Gualotuña

Sus funciones serán:

- Evacuar las ultimas cintas de respaldos de las BDD
- Debe estar enterada del contenido del plan

3.3.6. Entrenamiento

Establecer un programa de prácticas periódicas de todo el personal en la lucha contra los diferentes tipos de siniestros, de acuerdo a los roles que se le hayan asignado en los planes de evacuación del personal o equipos, para minimizar costos se puede aprovechar fechas de recarga de extinguidores, charlas de los proveedores, etc.

Un aspecto importante es que el personal tome conciencia de que los siniestros (incendios, inundaciones, terremotos, apagones, etc.) pueden realmente ocurrir, y tomen con seriedad y responsabilidad estos entrenamientos, para estos efectos es conveniente que participen los elementos directivos, dando el ejemplo de la importancia que la alta dirección otorga a la Seguridad Institucional.

Actividades después del desastre

Después de ocurrido el Siniestro o Desastre es necesario realizar las actividades que se detallan a continuación:

3.4. Evaluación de daños

Inmediatamente después que el siniestro ha concluido, se deberá evaluar la magnitud del daño que se ha producido, que sistemas se están afectando o no funcionan, que equipos han quedado no operativos, cuales se pueden recuperar, y en cuanto tiempo, etc.

Adicionalmente si el servidor central sufriera daños se deberá lanzar un preaviso a la Institución COMWARE con la cual se tiene un convenio de respaldo, para ir avanzando en las labores de preparación de entrega del equipo por dicha Institución.

Empresa	# de Teléfono
COMWARE (Soporte Server)	2266777

3.4.1. Priorización de Acciones del Plan de Acción

Una vez concluida la evaluación de daños reales se debe realizar una comparación contra el Plan, esto nos dará la lista de las actividades que debemos realizar, siempre priorizándola en vista a las actividades estratégicas y urgentes de nuestra Institución.

3.4.2. Ejecución de Actividades

Los trabajos de recuperación tendrán dos etapas, la primera la restauración del servicio usando los recursos de la Institución o local de respaldo, y la segunda etapa es volver a contar con los recursos en las cantidades y lugares propios

del Sistema de Información, debiendo ser esta última etapa lo suficientemente rápida y eficiente para no perjudicar el buen servicio de nuestro Sistema e imagen Institucional, como para no perjudicar la operatividad de la Institución o local de respaldo.

3.4.3. Evaluación de resultados

Una vez concluidas las labores de Recuperación del (los) Sistema(s) que fueron afectado (s) por el siniestro, debemos de evaluar objetivamente, todas las actividades realizadas, que tan bien se hicieron, que tiempo tomaron, que circunstancias modificaron (aceleraron o entorpecieron) las actividades del plan de acción, como se comportaron los equipos de trabajo, etc.

De la Evaluación de resultados y del siniestro en si, deberían de salir dos tipos de recomendaciones, una la retroalimentación del plan de Contingencias y otra una lista de recomendaciones para minimizar los riesgos y pérdida que ocasionaron el siniestro.

3.4.4. Retroalimentación del Plan de Acción

Con la evaluación de resultados, debemos de optimizar el plan de acción original, mejorando las actividades que tuvieron algún tipo de dificultad y reforzando los elementos que funcionaron adecuadamente.

El otro elemento es evaluar cual hubiera sido el costo de no haber tenido nuestra Institución el plan de contingencias llevado a cabo.

CAPITULO IV

PRUEBAS

Una vez redactado el plan, hay que probarlo y estar seguro que el plan va a funcionar. Por consiguiente, se realizó las pruebas para encontrar problemas, tomar nota de ellos y corregir el plan.

Por motivos del tipo de negocio de la Cooperativa, no se pudo suspender el servicio informático para ver si se es capaz de recuperarlo, pero se realizaron las siguientes pruebas que pueden ahorrar mucho tiempo en el caso de ponerse en marcha el plan de contingencia:

- Se realizó llamadas telefónicas a todos los colaboradores incluidos en las listas del plan (esto incluye a todas las personas que conforman el departamento de sistemas, empresas que prestan los servicios de comunicaciones FULLDATA y TELEHOLDING) constatando que los datos son actuales.
- Se llamó a la empresa COMWARE para verificar si tiene un equipo con las mismas características del servidor central, ya que con dicha empresa se tiene un contrato con el compromiso de préstamo de equipo en caso de que el host principal sufra algún desperfecto o avería, a lo cual nos supieron manifestar que si poseen equipos con iguales o mejores características que el servidor central.

En lo referente a información (Base de Datos) se realizaron las siguientes pruebas:

- Se verificó los procedimientos que se emplea para realizar los respaldos, constatando que dichos backups finalizaron correctamente.
- Se procedió a levantar dicho respaldo en el servidor de backup, y poner en línea la Base de Datos.

- Se verificó si los usuarios pueden acceder a los datos, desde diferentes terminales, los cuales no tuvieron ningún tipo de problemas al momento de acceder a la información requerida.

Para comunicaciones se realizaron pruebas con los dispositivos de backup Hub, Switch y Router.

El Router que sirve de backup, se encuentra configurado para realizar las conexiones respectivas con las de más agencias, al momento de hacer las pruebas de dicho dispositivo no se tuvo problemas de comunicaciones con las sucursales de la Cooperativa.

El Switch no es administrable al igual que el Hub, por tal razón la conexión es sencilla y rápida para entrar en funcionamiento

4.1. Distribución y Mantenimiento del Plan

El presente plan será distribuido a todas las personas que conforman el departamento de Sistemas y a la Gerencia General.

Se enviara una copia a la agencia Sangolquí por su cercanía a la matriz para que sea guardado en la bóveda de seguridad de dicha agencia, para así tener una copia extra fuera del lugar de trabajo.

Cuando se actualice el plan, se sustituirá todas las copias y se procederá a recoger las versiones previas.

El mantenimiento del plan es un proceso sencillo. Se comienza con una revisión del plan existente y se examina en su totalidad, realizando cambios a cualquier información que pueda haber variado. En ese instante, se debe volver a evaluar los sistemas de aplicación y determinar cuáles son los más importantes para la organización. Las modificaciones a esta parte del plan causarán modificaciones consecutivas a los procedimientos de recuperación. Sin embargo, esto no debería verse como un problema porque probablemente la sección de procedimientos tenga que actualizarse de todas formas debido a otros cambios.

CAPITULO V

CONCLUSIONES

- Al realizar el estudio respectivo de la situación actual del departamento de sistemas de la COACAV, se detectó inseguridades físicas que atentan contra su funcionamiento normal.
- De este estudio se logró identificar las amenazas y riesgos tanto internos como externos más probables de ocurrencia, que al afectar al departamento de sistemas produciría una paralización en las operaciones de la COACAV.
- Para la elaboración de las Políticas de Seguridad, se siguió una metodología, basándose en los estudios previos de las amenazas y en el análisis de riesgos que incurre la COACAV y tomando muy en cuenta el ciclo de vida de una Política de Seguridad.
- Para fortalecer los aspectos de seguridad a más de tener unas políticas de seguridad bien claras se hizo necesario la creación de un plan de contingencias el cual va muy ligado a estas políticas para de esta manera minimizar el impacto en la organización a causa de cualquier tipo de ataque y catástrofe que pueda alterar el funcionamiento de la COACAV.
- Con el desarrollo del Plan de Contingencias nosotros aportamos con los mecanismos e información necesaria, la cual se encuentra en este documento para que en el caso de ocurrencia de cualquier tipo de desastre, la COACAV, no tenga necesidad de parar sus operaciones.

- Una vez estructurado y comprendido el Plan de Contingencias se conformó equipos de trabajo para cada área de aplicación del plan de acción, teniendo en cada departamento un responsable directo para que se de cumplimiento de manera efectiva e inmediata el plan de contingencias.

RECOMENDACIONES

- Una vez hecho todo el estudio de amenazas, riesgos e impactos para la COACAV, recomendamos de manera urgente la distribución del plan de contingencia y la puesta en marcha de las políticas de seguridad para evitar cualquier tipo de inconveniente.
- Concientizar al personal del la COACAV mediante charlas sobre la importancia de cumplir y hacer cumplir estas políticas, haciendo entender que la información que manejan es de vital importancia para la organización.
- En caso de ocurrir un siniestro de cualquier tipo de índole, recomendamos poner en marcha el plan de contingencias que se realizó de acuerdo a las necesidades de la COACAV
- No se debe olvidar que las políticas de seguridad tiene un ciclo de vida, es por eso que éstas deben ser revisadas y evaluar la conveniencia y obsolescencia de dichas políticas con una frecuencia anual. De la misma manera es de mucha importancia tener actualizado el Plan de Contingencias para que las instalaciones, personal e información de la COACAV se encuentren salvaguardadas.
- Con el desarrollo de este proyecto de tesis a más de proporcionar un documento con normas y directrices a ser utilizadas en caso de siniestros, nuestro objetivo también es proporcionar y contribuir con toda la información necesaria para los ámbitos de seguridades informáticas.

BIBLIOGRAFÍA

- AUDITORIA EN INFORMÁTICA. Echenique, José Antonio
- Téllez Valdez, Julio. Derecho Informático. 2ª Edición. MC Graw Hill. México
- Lima de la Luz, María. Criminalia Nº 1-6 L.Delitos Electrónicos. Ediciones. Porrua
- COBIT, Directrices de Auditoria, 2ª Edición.
- HUERTA, Antonio Villalón. Seguridad de Unix y Redes. (Versión 1.2)
- RFC 1244: Site Security Handbook. J. Reinolds. – P. Holbrook
- ADELGANI, Gustavo. Miguel. Seguridad Informática MP ediciones Argentina. 1997 Página 22.
- CALVO, Rafael Fernández. Glosario Básico Ingles – Español para usuarios de Internet 1994 – 2000.
- TUDOR, Jan Killmeyer, Information Securyte Architecture, Auerbach Publications, New York, 2001
- PELTIER, Thomas R., Information Security Policies and Procedures, Auerbach Publications, New York, 1999
- Instituto Nacional de Estándares y Tecnología, Una introducción a la seguridad Informática, Publicación especial 800 – 12, Octubre 1995

Internet

Por el continuo movimiento de las direcciones de Internet es posible que algunas de las numeradas a continuación no se encuentren disponibles para consulta.

- www.monografias.com
- www.delitosinformaticos.com/propiedadindustrial/auditorias.html
- www.ilustrados.com
- www.isaca.org
- www.netconsul.com
- www.iaia.org.ar
- www.cica.ca/idea/index.htm
- www.audinet.net.org
- www.audiserve.com/articles/
- www.acl.org
- www.gestiopolis.com/
- www.microsoft.com/latam/technet/articulos/200011
- www.delitosinformaticos.com/tesis/htm
- www.microsoft.com/latam/technet/security/1
- www.seguridadcorporativa.org
- www.geocities/SiliconValley/way/4651
- www.rediris.es/cert
- www.udec.cl/˜rhunrich/index.htm

ANEXO A

Cuadro 1: Hardware que posee la Cooperativa con posible ocurrencia de amenaza e impacto.

Agencia	Modelo del Computador	Impresora	Amenazas	Impacto	Calificación
JEFATURA					
Matriz	Portátil AMD	HP Desk Jet	° Fallas eléctricas ° Fallas en el equipo ° Uso indebido del HW ° Acciones Hostiles	Despreciable	Baja Prioridad
Inca	Pentium Pro (R) 333 Mhz	Hp Desk Jet 695C	° Fallas eléctricas ° Fallas en el equipo ° Uso indebido del HW ° Acciones Hostiles	Despreciable	Baja Prioridad
Chillogallo	Intel P. IV de 1.8 Ghz	LEXMARK Z12	° Fallas eléctricas ° Fallas en el equipo ° Uso indebido del HW ° Acciones Hostiles	Despreciable	Baja Prioridad

Sangolquí	Intel	Canon BJC-250	◦ Fallas eléctricas ◦ Fallas en el equipo ◦ Uso indebido del HW ◦ Acciones Hostiles	Despreciable	Baja Prioridad
Amaguaña	Pentium III de 600 Mhz	Lexmark Z12	◦ Fallas eléctricas ◦ Fallas en el equipo ◦ Uso indebido del HW ◦ Acciones Hostiles	Despreciable	Baja Prioridad
Machachi	Pentium III 800 EB Mhz	Hp Deskjet	◦ Fallas eléctricas ◦ Fallas en el equipo ◦ Uso indebido del HW ◦ Acciones Hostiles	Despreciable	Baja Prioridad
Conocoto	Celeron™ MMX CPU at 333 MHz	Epson Lx-300+	◦ Fallas eléctricas ◦ Fallas en el equipo ◦ Uso	Despreciable	Baja Prioridad

			◦ Uso indebido del HW ◦ Acciones Hostiles		
Guamaní	INTEL PENTIUM IV DE 1.8 GHZ	EPSON STYLUS 1500	◦ Fallas eléctricas ◦ Fallas en el equipo ◦ Uso indebido del HW ◦ Acciones Hostiles	Despreciable	Baja Prioridad
SERVICIO AL CLIENTE					
Matriz	Authentic AMD	No	◦ Fallas eléctricas ◦ Fallas en el equipo ◦ Uso indebido del HW ◦ Acciones Hostiles	Marginal	Prioritario
	Pentium Pro de 300 MHz	Epson LX 300	◦ Fallas eléctricas ◦ Fallas en el equipo ◦ Uso indebido del HW ◦ Acciones Hostiles	Crítico	Prioritario

Inca	Pentium Pro ® 333 Mhz	Epson LX 300	◦ Fallas eléctricas ◦ Fallas en el equipo ◦ Uso indebido del HW ◦ Acciones Hostiles	Crítico	Prioritario
Chillogallo	Intel Pentium II de 400 Mhz	Epson LX-300	◦ Fallas eléctricas ◦ Fallas en el equipo ◦ Uso indebido del HW ◦ Acciones Hostiles	Crítico	Prioritario
	Intel Pentium II 400 Mhz	No	◦ Fallas eléctricas ◦ Fallas en el equipo ◦ Uso indebido del HW ◦ Acciones Hostiles	Marginal	Prioritario
Sangolquí	Pentium II 450MHz	Epson FX-880+	◦ Fallas eléctricas ◦ Fallas en el equipo ◦ Uso indebido	Crítico	Prioritario

			del HW ° Acciones Hostiles		
	Pentium III 450 MHz	Epson LX-300 +	° Fallas eléctricas ° Fallas en el equipo ° Uso indebido del HW ° Acciones Hostiles	Marginal	Prioritario
	Pentium II 300 Mhz	HP LASER 1300	° Fallas eléctricas ° Fallas en el equipo ° Uso indebido del HW ° Acciones Hostiles	Crítico	Prioritario
	Intel Pentium IV de 2.8	LEXMARK E210 LASER	° Fallas eléctricas ° Fallas en el equipo ° Uso indebido del HW ° Acciones Hostiles	Crítico	Prioritario
	Pentium Pro	No	° Fallas	Marginal	Prioritario

	200 MHz		eléctricas ° Fallas en el equipo ° Uso indebido del HW ° Acciones Hostiles		
Amaguaña	Autentic AMD K6 de 266 Mhz	EPSON FX-890	° Fallas eléctricas ° Fallas en el equipo ° Uso indebido del HW ° Acciones Hostiles	Crítico	Prioritario
Machachi	Celeron™ MMX CPU Ethernet Adapter 333Mhz	Epson Fx-880+	° Fallas eléctricas ° Fallas en el equipo ° Uso indebido del HW ° Acciones Hostiles	Crítico	Prioritario
Conocoto	Pentium (R) 4CPU 1.80 GHz	HP DESK JET	° Fallas eléctricas ° Fallas en el equipo ° Uso indebido del HW	Crítico	Prioritario

			° Acciones Hostiles		
Guamaní	INTEL P II de 400 Mhz	EPSON LX 300+	° Fallas eléctricas ° Fallas en el equipo ° Uso indebido del HW ° Acciones Hostiles	Crítico	Prioritario
La Ecuatoriana	Intel Pentium IV de 1.8 Ghz	EPSON LX -300+	° Fallas eléctricas ° Fallas en el equipo ° Uso indebido del HW ° Acciones Hostiles	Crítico	Prioritario
Aloag	Intel Pentium III de 866 Mhz	No	° Fallas eléctricas ° Fallas en el equipo ° Uso indebido del HW ° Acciones Hostiles	Crítico	Prioritario
CARTERA Y CRÉDITO					
Matriz	Intel ®	HP	° Fallas	Marginal	Baja

	Pentuim 4 1.80 GHz		eléctricas ° Fallas en el equipo ° Uso indebido del HW ° Acciones Hostiles		Prioridad
	Authentic AMD	No	° Fallas eléctricas ° Fallas en el equipo ° Uso indebido del HW ° Acciones Hostiles	Marginal	Baja Prioridad
Inca	Pentium Pro 333 Mhz	HP 1200	° Fallas eléctricas ° Fallas en el equipo ° Uso indebido del HW ° Acciones Hostiles	Marginal	Baja Prioridad
	Intel Celeron de 400 Mhz	HP 1200	° Fallas eléctricas ° Fallas en el equipo ° Uso indebido del HW	Marginal	Baja Prioridad

			◦ Acciones Hostiles		
Chillogallo	Intel Pentium II de 400 Mhz	HP 1000	◦ Fallas eléctricas ◦ Fallas en el equipo ◦ Uso indebido del HW ◦ Acciones Hostiles	Marginal	Baja Prioridad
	INTEL PENTIUM II DE 400 Mhz	EPSON LQ 2180	◦ Fallas eléctricas ◦ Fallas en el equipo ◦ Uso indebido del HW ◦ Acciones Hostiles	Marginal	Baja Prioridad
Sangolquí	Celeron (TM) MMX 333 MHZ	No	◦ Fallas eléctricas ◦ Fallas en el equipo ◦ Uso indebido del HW ◦ Acciones Hostiles	Marginal	Baja Prioridad
Amaguaña	Autentic AMD K6 de 266 Mhz	EPSON FX-890	◦ Fallas eléctricas ◦ Fallas en	Marginal	Baja Prioridad

			el equipo ° Uso indebido del HW ° Acciones Hostiles		
Machachi	Intel Celeron 300 Mhz	Epson LX-300+	° Fallas eléctricas ° Fallas en el equipo ° Uso indebido del HW ° Acciones Hostiles	Marginal	Baja Prioridad
COBRANZAS					
Matriz	Intel Celeron 333 Mhz	Epson LX 300	° Fallas eléctricas ° Fallas en el equipo ° Uso indebido del HW ° Acciones Hostiles	Despreciable	Baja Prioridad
Inca	Intel Pentium Pro 333 Mhz	No	° Fallas eléctricas ° Fallas en el equipo	Despreciable	Baja Prioridad

			◦ Uso indebido del HW ◦ Acciones Hostiles		
Sangolquí	Celeron (TM) MMX 333 MHZ	No	◦ Fallas eléctricas ◦ Fallas en el equipo ◦ Uso indebido del HW ◦ Acciones Hostiles	Despreciable	Baja Prioridad
Amaguaña	Autentic AMD K6 de 266 Mhz	EPSON FX-890	◦ Fallas eléctricas ◦ Fallas en el equipo ◦ Uso indebido del HW ◦ Acciones Hostiles	Despreciable	Baja Prioridad
CAJAS					
Matriz	Intel Pentium 4	Epson FX 880	◦ Fallas eléctricas ◦ Fallas en el equipo	Crítico	Prioritario

			◦ Uso indebido del HW ◦ Acciones Hostiles		
	Pentium Pro 300Mhz	No	◦ Fallas eléctricas ◦ Fallas en el equipo ◦ Uso indebido del HW ◦ Acciones Hostiles	Crítico	Prioritario
Inca	Intel Celeron de 333 MHZ	Epson FX-880+	◦ Fallas eléctricas ◦ Fallas en el equipo ◦ Uso indebido del HW ◦ Acciones Hostiles	Crítico	Prioritario
	Intel pentium IV de 1.8 GHz	Epson FX-880+	◦ Fallas eléctricas ◦ Fallas en el equipo ◦ Uso indebido del HW ◦ Acciones Hostiles	Crítico	Prioritario
	Pentium Pro (R) 333 Mhz	No	◦ Fallas	Crítico	Prioritario

			eléctricas ° Fallas en el equipo ° Uso indebido del HW ° Acciones Hostiles		
Chillogallo	INTEL CELERON DE 333 Mhz	EPSON FX-880+	° Fallas eléctricas ° Fallas en el equipo ° Uso indebido del HW ° Acciones Hostiles	Crítico	Prioritario
	Intel Pentium Pro ® de 333 Mhz	Epson Fx - 880+	° Fallas eléctricas ° Fallas en el equipo ° Uso indebido del HW ° Acciones Hostiles	Crítico	Prioritario
Sangolquí	Pentium III 450 Mhz	Epson Lx-300+	° Fallas eléctricas ° Fallas en el equipo ° Uso indebido del HW ° Acciones	Crítico	Prioritario

			Hostiles		
	Celeron (TM) -MMX 333 MHZ	Epson Lx-300+	° Fallas eléctricas ° Fallas en el equipo ° Uso indebido del HW ° Acciones Hostiles	Crítico	Prioritario
Amaguaña	Intel Celeron de 400 Mhz	EPSON FX-880+	° Fallas eléctricas ° Fallas en el equipo ° Uso indebido del HW ° Acciones Hostiles	Crítico	Prioritario
	Pc Chips	No	° Fallas eléctricas ° Fallas en el equipo ° Uso indebido del HW ° Acciones Hostiles	Crítico	Prioritario
Machachi	Autentic AMD K6 266 Mhz	Epson Fx-880+	° Fallas eléctricas ° Fallas en el equipo ° Uso indebido	Crítico	Prioritario

			del HW ° Acciones Hostiles		
Conocoto	Intel Pentium III de 1 Ghz	Epson FX-880	° Fallas eléctricas ° Fallas en el equipo ° Uso indebido del HW ° Acciones Hostiles	Crítico	Prioritario
Guamaní	INTEL P II de 400 Mhz	EPSON LX 300+	° Fallas eléctricas ° Fallas en el equipo ° Uso indebido del HW ° Acciones Hostiles	Crítico	Prioritario
La Ecuatoriana	Intel Celeron de 366 Mhz	EPSON LX-300+	° Fallas eléctricas ° Fallas en el equipo ° Uso indebido del HW ° Acciones Hostiles	Crítico	Prioritario
Aloag	Intel Celeron	Epson FX-	° Fallas	Crítico	Prioritario

	de 333 Mhz	880+	eléctricas ° Fallas en el equipo ° Uso indebido del HW ° Acciones Hostiles		
SISTEMAS					
Matriz	Intel (Portátil) Intel P4 1.8 GHz	No	° Fallas eléctricas ° Fallas en el equipo ° Uso indebido del HW ° Acciones Hostiles	Crítico	Prioritario
	Intel P4 1.8 GHz	No	° Fallas eléctricas ° Fallas en el equipo ° Uso indebido del HW ° Acciones Hostiles	Crítico	Prioritario
	Intel P4 1.8 GHz	No	° Fallas eléctricas ° Fallas en el equipo ° Uso indebido	Crítico	Imprescindible

			del HW ° Acciones Hostiles		
	Intel P3 1.8 GHz		° Fallas eléctricas ° Fallas en el equipo ° Uso indebido del HW ° Acciones Hostiles	Crítico	Prioritario
Inca	HP X86 Family 6 Model 5 Stepping 2	No	° Fallas eléctricas ° Fallas en el equipo ° Uso indebido del HW ° Acciones Hostiles	Catastrófico	Imprescindible
	Amd Athlon(TM) XP 2400	No	° Fallas eléctricas ° Fallas en el equipo ° Uso indebido del HW ° Acciones Hostiles	Catastrófico	Imprescindible
Chillogallo	Intel Pentium III de 800 Mhz	No	° Fallas eléctricas	Catastrófico	Imprescindible

			◦ Fallas en el equipo ◦ Uso indebido del HW ◦ Acciones Hostiles		
Sangolqui	X86 Family 6 model 8 stepping 63 AT/AT Compatible	No	◦ Fallas eléctricas ◦ Fallas en el equipo ◦ Uso indebido del HW ◦ Acciones Hostiles	Catastrófico	Imprescindible
	Intel Pentium IV de 2.8	No	◦ Fallas eléctricas ◦ Fallas en el equipo ◦ Uso indebido del HW ◦ Acciones Hostiles	Catastrófico	Imprescindible
Machachi	HP Intel P III X86 Family 6 Modem 8 stepping 10/AT compatible	No	◦ Fallas eléctricas ◦ Fallas en el equipo ◦ Uso indebido del HW ◦ Acciones	Catastrófico	Imprescindible

			Hostiles		
Amaguaña	Acer Verition X86 Family 15 Model 1 stepping 2 AT/AT compatible	No	° Fallas eléctricas ° Fallas en el equipo ° Uso indebido del HW ° Acciones Hostiles	Catastrófico	Imprescindible
CUARTO DE SERVIDORES					
Matriz	Servidor Sun Full Power (Ultra Spak 250)	No	° Fallas eléctricas ° Fallas en el equipo ° Uso indebido del HW ° Acciones Hostiles	Catastrófico	Imprescindible
	HP Net Server LC 3 (AT/AT Compatible Pentium II)	No	° Fallas eléctricas ° Fallas en el equipo ° Uso indebido del HW ° Acciones Hostiles	Catastrófico	Imprescindible
	Servidor Sun Full Power (Ultra Spak 250)	No	° Fallas eléctricas ° Fallas en	Catastrófico	Imprescindible

			el equipo ◦ Uso indebido del HW ◦ Acciones Hostiles		
OTROS (Departamentos que se encuentran en Matriz)					
Secretaria	Intel P3 16 Hz	Epson	◦ Fallas eléctricas ◦ Fallas en el equipo ◦ Uso indebido del HW ◦ Acciones Hostiles	Marginal	Baja Prioridad
Contabilidad	Intel P4 1.8 GHz	Canon	◦ Fallas eléctricas ◦ Fallas en el equipo ◦ Uso indebido del HW ◦ Acciones Hostiles	Marginal	Baja Prioridad
	AMD 266 MHz	Epson G716	◦ Fallas eléctricas ◦ Fallas en el equipo ◦ Uso indebido del HW	Marginal	Baja Prioridad

			◦ Acciones Hostiles		
	Intel Celeron (TM) -366 MHz	No	◦ Fallas eléctricas ◦ Fallas en el equipo ◦ Uso indebido del HW ◦ Acciones Hostiles	Marginal	Baja Prioridad
	Intel Celeron de 333 MHz	Epson LQ 2070	◦ Fallas eléctricas ◦ Fallas en el equipo ◦ Uso indebido del HW ◦ Acciones Hostiles	Marginal	Baja Prioridad
Tesorería	Intel (R) Pentuim III 1.80GHz	Compaq FX-880	◦ Fallas eléctricas ◦ Fallas en el equipo ◦ Uso indebido del HW ◦ Acciones Hostiles	Marginal	Baja Prioridad
Auditoria Interna	Pentium (R) 200 MHz	Canon BJC-1000	◦ Fallas eléctricas ◦ Fallas en el equipo	Marginal	Baja Prioridad

			◦ Uso indebido del HW ◦ Acciones Hostiles		
Dto. Legal	Pentium-s CPU 120MHz	No	◦ Fallas eléctricas ◦ Fallas en el equipo ◦ Uso indebido del HW ◦ Acciones Hostiles	Marginal	Baja Prioridad
Secretaria Consejo Administración	Pentium I 166 MHz	Epson LX-300	◦ Fallas eléctricas ◦ Fallas en el equipo ◦ Uso indebido del HW ◦ Acciones Hostiles	Marginal	Baja Prioridad
Consejo Administración	Celeron (TM)-MMX CPU 366 MHz	No	◦ Fallas eléctricas ◦ Fallas en el equipo ◦ Uso indebido del HW ◦ Acciones Hostiles	Marginal	Baja Prioridad
Consejo	GenuineIntel x 86	No	◦ Fallas	Marginal	Baja

Vigilancia			eléctricas ° Fallas en el equipo ° Uso indebido del HW ° Acciones Hostiles		Prioridad

ÍNDICE

ÍNDICE DE GRÁFICOS

ÍNDICE DE TABLAS

ESCUELA POLITÉCNICA DEL EJÉRCITO

FACULTAD DE SISTEMAS E INFORMÁTICA

DISEÑO DE LAS POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN Y DESARROLLO DEL PLAN DE CONTINGENCIA PARA EL ÁREA DE SISTEMAS DE LA COOPERATIVA DE AHORRO Y CRÉDITO ALIANZA DEL VALLE

Previa a la obtención del Título de:
Ingeniero en Sistemas e Informática

AUTORES

CRISTHIAN VINICIO LLUMIQUINGA MARCILLO
PATRICIO FERNANDO VALLEJO

SANGOLQUÍ, ABRIL DEL 2005