# ESTUDIO DE SEGURIDAD DEL SISTEMA INFORMÁTICO FINANCIERO Y SERVIDORES DE LA COOPERATIVA AVANZA

PROYECTO DE GRADO


**AUTOR**

**JAMES ARIEL MUÑOZ HUERTAS**

Código

1612010983



***INSTITUCIÓN UNIVERSITARIA POLITÉCNICO GRANCOLOMBIANO***
***FACULTAD DE INGENIERÍA Y CIENCIAS BÁSICAS***
***ESPECIALIZACIÓN EN SEGURIDAD DE LA INFORMACIÓN***
***COLOMBIA***
***2018***

# ESTUDIO DE SEGURIDAD DEL SISTEMA INFORMÁTICO FINANCIERO Y SERVIDORES DE LA COOPERATIVA AVANZA

PROYECTO DE GRADO


**AUTOR**

**JAMES ARIEL MUÑOZ HUERTAS**

Código

1612010983

**jamunozh1@poligran.edu.co**


Director

**WILMAR JAIMES FERNÁNDEZ**


***INSTITUCIÓN UNIVERSITARIA POLITÉCNICO GRANCOLOMBIANO***
***FACULTAD DE INGENIERÍA Y CIENCIAS BÁSICAS***
***ESPECIALIZACIÓN EN SEGURIDAD DE LA INFORMACIÓN***
***COLOMBIA***

***2018***

Nota de aceptación

_____
_____
_____
_____
_____
_____

_____

_____

_____

Firmas de los jurados

*Bogotá, Colombia*
*2018/05/07*

ÍNDICE GENERAL



ÍNDICE DE TABLAS



ÍNDICE DE FIGURAS

## I. INTRODUCCIÓN

La Cooperativa Avanza, decidió migrar desde su sistema de datos tradicional a uno integrado por dos servidores de rack y un Firewall en su sede principal y varias estaciones de trabajo inteligentes con un sistema informático financiero; los datos transmitidos no necesitan usar las redes públicas, más si se utiliza la infraestructura de Internet.

Es importante resaltar que el sistema informático financiero lo distribuye un proveedor nacional (Opa Ltda.).

Se manejan varios aspectos de naturaleza técnica de nivel 1, como son: la creación de una extensión IP en los servidores SQL Server y la configuración de la extensión IP con un protocolo versión 4 para las estaciones de trabajo.

Una vez identificadas las partes físicas como son las estaciones de trabajo IP y los servidores SQL Server, se configuran para que estos dispositivos acepten el sistema informático financiero de la Cooperativa Avanza y se comience a prestar un buen servicio en cuanto a suministro de Datos y Voz IP. [16]

## II. PLANTEAMIENTO DEL PROBLEMA

Desde que se crearon las nuevas tecnologías, la COOPERATIVA AVANZA, tiene una técnica de transmisión de datos vasados en direcciones IP, para conservar la transmisión de la información entre sucursales. [17]

Pero esas nuevas tecnologías deben desarrollar pericias contra la Ingeniería Social, toda vez que no existen políticas que regulen cierto tipo de aplicaciones en internet; es decir que estos casos no constituyen un delito informático, pues no existen políticas dentro de las redes sociales que establezcan una regulación sobre lo que se puede hacer o no. Normalmente no se tiene ningún tipo de procesos que emitan una alarma a la hora de estar siendo atacada y al no hacerlo es el usuario el que se da cuenta del error, hace el filtro o el análisis de la información después de que está se encuentra defraudada.

Existe una dificultad frente a esto y es que la mayoría de los procesos en la red se hace después de haber sido sustraídos sus contenidos; se debe a la política de algoritmos y a la política de velocidad en la transmisión de la información, porque finalmente lo hace a partir de una aplicación que pudo hacer compatible con la aplicación de la empresa irrumpida sin ningún control, sin alguien que le haga un filtro o que le diga si está bien o no la circulación de la información utilizada para hacer el fraude, este tipo de delitos no entran dentro de la tipología de lo que podríamos llamar delitos informáticos, en cuanto a publicación de información, que en ese aspecto sí existe una regulación por parte del Estado, porque este sí puede venir y bloquear páginas, sitios, hacer una serie de controles a la publicación que se hace.

Se considera que la Ingeniería Social es un tema, más que judicial, de la manera cómo estamos protegiendo los contenidos de las bases de datos sensibles, porque no nos estamos informando directamente por el delincuente en el momento que realiza un proceso de fraude sino que nos estamos informando directamente por la fuente titular y propietaria del contenido, es decir el usuario final, al cual hay que responder por la confianza depositada en la entidad, pero que representa una pérdida en los estados de resultados finales de la entidad afectada. [23]

## III. OBJETIVOS

- Suplir la ausencia de un medio de comunicación en línea que demande un mayor esfuerzo por parte de las ENTIDEDES para proteger los productos de sus clientes, toda vez que se está dejando este proceso a mensajes de texto y correo electrónico, para difundir el suceso cuando ya no hay nada que hacer.
- Elaborar procesos definidos para llevar a cabo la labor del departamento TIC en línea.
- Realizar un diagnóstico de seguridad mediante políticas de la ENTIDAD, a medios electrónicos existentes tales como: CAJEROS AUTOMÁTICOS DIGITALES, PÁGINAS WEB, DISPOSITIVOS APP, SISTEMA DE CORREOS DIRECTOS, MENSAJES DE VOZ, entre otros.
- Incluir dentro de la publicidad de la entidad (CARTELERAS Y VIDEOS INSTITUCIONALES, CIRCULARES INTERNAS Y EXTERNAS, entre otros), manuales de usuario, medidas de seguridad, líneas, canales de atención, así como los valores y principios que fundamenten la prevención de fraudes.
- Determinar los niveles de seguridad en un Software programado y compatible con un mecanismo, que permita detectar a tiempo un fraude de la Ingeniería Social.

## IV. METODOLIGÍA

La metodología del proyecto se basará a un proceso que seguiremos para gestionar nuestras actividades siguiendo unos requisitos y pasos, con el fin de encontrar rutas de trabajo optimizadas. Antes de empezar a aplicar algún método para elaborar el proyecto, es importante entender que dicho proyecto debe ser la unidad única del trabajo, en la que se realiza una gestión de recursos disponibles para alcanzar el objetivo específico del proyecto, todo ello en un periodo de tiempo claro y establecido en la planificación; de ahí, que para saber cómo hacer la metodología del proyecto, es preciso hablar, y mucho, de cómo planificarlo, pensando en el beneficio del usuario final, su naturaleza, requisitos, propósitos y demás elementos exactos. [1]

Se incluye una primera etapa que será el **generar un nuevo enfoque en la administración**, partiendo de que la seguridad de los datos y la comunicación es la base de su desarrollo y gestión de cambio y consecutivamente, propiciar el crecimiento sostenido de la Entidad haciendo el Software más Seguro, fomentando un mayor acercamiento con los clientes y su mayor conocimiento de los servicios que se adelanten, a la vez ofreciendo canales de comunicación más atractivos por su seguridad para la comunidad en general.

Esto permitirá que Entidad pueda crecer internamente a través de su segunda etapa que será el **desarrollo organizacional** "El Plan Estratégico de Transmisión de Datos y Comunicación en línea", para fortalecer los vínculos con los clientes, evitando que los mismos decidan trasladar sus productos de ahorro y crédito a otras Entidades al ser atraídos únicamente por tasas de interés más favorables y no por la seguridad de sus ahorros.

Finalmente se establecen unos tiempos de ejecución y puesta en marcha del proyecto. Para efectos de esta investigación se tendrá en cuenta que el prototipo del proyecto será realizado en el periodo comprendido entre el inicio del módulo y la entrega final. [15]

## V. DESCRIPCIÓN DE RESULTADOS

Se dará a conocer como producto final, Entregables con el prototipo del proyecto Seguridad de la Información de los Servidores de la Cooperativa contra la Ingeniería Social, con sus políticas, definición de canales de datos y comunicación en línea y garantizar que la seguridad de la información sea 24x7 necesaria para la continuidad del negocio.

## VI. ALCANCE

Actualmente las ENTIDADES FINANCIERAS son empresas con gran proyección a nivel nacional, las cuales son apoyadas por otras entidades de control y vigilancia, quienes brindan programas de orden preventivos contra posibles fraudes que se pueden presentar al interior de este tipo de Entidades; pero no disponen de recursos para hacer frente a fraudes que se presenten fuera de ellas, por lo cual a las Entidades Financieras les corresponde asumir las pérdidas que se presenten o crear nuevas medidas de seguridad para sus sistemas los cuales son frecuentemente vulnerados, por la cualidad que contiene sus productos (dinero).

El proyecto pretende desarrollar:

- Definir canales de datos y comunicación con los clientes en el momento que se detecte un acceso sospechoso a un producto.
- Introducir políticas y procesos (mecanismos), del ejercicio de los Servidores SQL Server, aplicaciones, directorio activo, entre otros y la información oportuna al cliente.
- Que el TIC pueda detectar oportunamente las vulnerabilidades mediante el Open Vas y pueda proteger los datos y las comunicaciones en línea, veinticuatro horas al día y siete días a la semana.

El proyecto cuenta con una limitación, la cual puede ser el factor tiempo.

## VII. JUSTIFICACIÓN

El presente trabajo está encaminado a establecer la necesidad de un plan de mejora en la seguridad de los datos y las comunicaciones, especialmente en línea, de las ENTIDADES FINANCIERAS, donde la información que viaje por los canales de comunicación sea segura en cuanto a autenticidad y puntualidad; donde se hace necesario desarrollar una solución, robusteciendo los canales de localización de intrusos, comunicaciones y vigilancia.
Las ENTIDADES FINANCIERAS deben aprovechar la importante labor que desarrollan para el mejoramiento de la calidad de vida de los clientes de cada Entidad y ganar el debido reconocimiento ante la sociedad, siendo indispensable iniciar un cambio al interior, para que sea transmitido a través de mejores canales de comunicación, pero cerca del mismo instante en que se presente la situación problema, sin importar la hora o el día y fundamentada mediante políticas estudiadas por cada Entidad, fortaleciendo sus Servidores para hacerlos menos vulnerables.

## VIII. ESTRATEGIA METODOLÓGICA

*A. Recaudo de características de los activos que ayudan a la transmisión de Datos y Voz IP de la Cooperativa.*

La transmisión de la Cooperativa, combina varios equipos emisores y receptores de Datos y Voz IP, que fueron preliminarmente referidos por funcionarios TIC de la Cooperativa en el inventario de dispositivos técnicos.

En seguida se manifiesta en que se fundamenta cada activo de prestación del servicio hallado y la información seleccionada por ellos:

*A.1. Dos Servidores de Rack Dell:* De 128 RAM y dos Procesadores cada uno; por si se cae uno por desempeño, se estructura el otro y sigue transmitiendo.

Entre ellos mismos se conectan por red con tarjetas especiales de 10 Gigas, pero al conectarlos con el Switche se utiliza una tarjeta de 1 Giga.

Los servidores están conectados a los Switche dos veces, de igual manera se encuentran conectados con el dispositivo Firewall dos veces por si alguno falla.

Fig. 1

*A.2. Dispositivo hardware firewall Cisco:* Contiene un software que nos permite gestionar y filtrar la totalidad de trafico entrante y saliente que hay entre las 2 redes (exterior e interior) con los servidores de la misma red.

El software que contiene dicho dispositivo actúa como un aislamiento de procesos o entorno aislado (**San box** en inglés)


Fig. 2

*A.3. Un Servidor de Avanza Voz IP:*

Es un activo estándar de telefonía que permite la transmisión de voz sobre una red basada en IP. En el que fue situada una repartición para efectuar las comunicaciones agrupadas llamada Elastix, y se distribuye bajo licencia GPL. [2]

Todos los servidores de Datos y Voz IP, poseen un Switche que permite el uso de una red de Datos y Voz IP entre las seis sedes externas de la cooperativa, igualmente permite que los usuarios usen su red IP existente para gestionar sus necesidades de telefonía. Para que esto sea posible deben existir servidores de Datos y Voz IP con un router que sirve como puerta de enlace para gestionar el tráfico de Datos y Voz IP y para distribuir las llamadas de la misma forma en la que lo haría un sistema de teléfono análogo. Existen numerosos tipos diferentes de servidores de Datos y Voz IP, pero tienen la misma funcionalidad básica: proporcionar servicios de Datos y Voz IP a los usuarios. Los servidores de Datos y Voz IP no están publicados en internet, dichos servidores están conformados por dispositivos de la siguiente manera:

- Línea de los Servidores.
- Estándar de los Servidores.
- Sitio de los Servidores.
- Tipos de Procesadores.
- Monto de almacenamiento R.A.M.
- Total, D.D.
- Capacidad D.D.
- Reparación D.D.
- Total, de compatibilidades en la red.
- Trazados MAC de las compatibilidades de red.
- IPs de las Compatibilidades de red.
- Investigación del S.O.D
- Registro de programas instalados en el servidor.
- Colaboradores a los que se le asignaron dirección del Servidor.
- Dirección para SSH, WEB, TELNET.

Cabe decir que los servidores funcionan dentro de la Cooperativa como:
Servidor SQL Server. Servidor de Aplicaciones.
Servidor de Directorio Activo. Servidor Vcenter.

Fig. 3

*A.4. Estaciones de trabajo equipos Dell:* Equipadas con Windows 7 y 10, conectadas con el protocolo IP versión 4; se usan para internet, office y aplicación financiera Opa.

Las estaciones de trabajo locales (Sede Norte y Administrativa) que funciona como principal, se conectan directamente al Servidor. Mientras las estaciones de trabajo de las Sedes a nivel Nacional se conectan mediante Acceso Remoto.

La investigación tomada de estas terminales para bien de la parametrización, es la siguiente:

- Línea de los PC.
- Estándar de los PC.
- Serie del PC.
- Firmware utilizado.
- Última dirección IP conocida del computador.
- Funcionario al que le fue asignado el PC.
- Sitio de trabajo del PC.
- Funcionarios a los que les fue establecido la dirección de los PC.
- Canales de dirección para configuraciones (WEB, SSH, TELNET).

Fig. 4

*B. Reconocimiento de peligros y debilidades del Sistema de Datos y Voz IP de la Cooperativa Avanza*

*B.1 Orígenes de posibles daños de los Activos del Servicio de Datos y Voz IP de la Cooperativa Avanza*

Una vez determinados los primordiales Activos, el posterior paso radicó en determinar los peligros posibles y aplicables al ambiente de la Cooperativa Avanza. [3] Se utilizó como cita el catálogo de amenazas "*Libro 2 – Catálogo de elementos de la metodología MAGERIT v3*". (Amutio, Miguel A. & Candau, Javier, 2012)

A continuación, se presenta para cada Activo de Datos y Voz IP los primordiales peligros a la que éste se confronta.

*B.1.1 Peligros a los Servidores de Datos y Voz IP.*

Norma Magerit V3
5.1.1. [N.1] Quema - Combustión
5.1.2. [N.2] Agua – Avalanchas, inundaciones
5.1.3. [N.4, N.6, N.7] Catástrofes - Cataclismo, Clima y sismos.
3 5.2.1. [I.1] Quemas.
5.2.2. [I.2] Desastres por inundaciones.
5.2.3. [I.*] Catástrofe industrial – Exceso y cortes eléctricos.
5.2.4. [I.3] Infección por moho – Partículas y esporas.
5.2.6. [I.5] Daños de procedencia física. Daños en los Activos y/o daños en los programas. Pueden ser ocasionados a una falla de origen en la marcha.
5.2.7. [I.6] Interrupción del abastecimiento
5.2.9. [I.8] Daño en las comunicaciones
5.2.11. [I.10] Daño de los soportes de reserva.
5.3.2. [E.2] Equivocación humana.
5.3.3. [E.3] Desaciertos de control y vigilancia.
5.3.4. [E.4] Desacierto de ordenación.
5.3.7. [E.9] Desacierto de encaminamiento
5.3.13. [E.20] Flaqueza del Software.
5.3.15. [E.23] Fallas de manutención / actualización de equipos.
5.4.1. [A.3] Adulteración de licencias.
5.4.2. [A.4] Adulteración de ordenación.
5.4.3. [A.5] Usurpación de usuarios
5.4.4. [A.6] Extralimitación de libertades de entrada.
5.4.6. [A.8] Propagación de software perjudicial.
5.4.7. [A.9] [Re-] Desplazamiento de correos – Remisión de investigación a un rumbo erróneo por medio de una estructura o un sistema, que dirigen la información por donde no es correcto; por ejemplo, mensajes entre individuos, entre desarrollos o unos con otros. Un agresor puede coaccionar un correo para propagarse a través de un punto establecido de la red donde puede ser escuchado. Es propiamente recalcable la agresión de encarrila miento dirija una trasmisión ilegal, terminado la información en personas indebidas.
5.4.9. [A.11] Entrada no permitida
5.4.10. [A.12] Estudio y monitorización de tráfico.
5.4.12. [A.14] Apropiación de datos (escucha)
5.4.14. [A.18] Destrucción información.
5.4.17. [A.23] Manipulación Datos
5.4.18. [A.24] Prohibición de atención.
5.4.20. [A.26] Ofensiva

*B.1.2 Amenazas y peligros de las Tarjetas de Red que transportan Datos y Voz.*
5.1.1. [N.1] Quemas
5.1.2. [N.2] Desastres por inundaciones.
5.1.3. [N.4, N.6, N.7] Catástrofes.
5.2.1. [I.1] Quemas.
5.2.2. [I.2] Desastres por inundaciones
5.2.3. [I.*] Catástrofes fabriles – Exceso instalaciones eléctricas.
5.2.4. [I.3] Infección por moho – Partículas y esporas.
5.2.6. [I.5] Daños procedencia física – Daños Activos. Pueden ocasionarse a una falla en la marcha.
5.2.7. [I.6] Interrupción eléctrica.
5.3.2. [E.2] Errores del administrador.
5.4.18. [A.24] Interrupción de servicio.

*B.1.3 Peligros de las Estaciones de trabajo equipos Dell:*
5.1.1. [N.1] Quemas.
5.1.2. [N.2] Desastres por inundaciones.
5.1.3. [N.4, N.6, N.7] Catástrofes.
5.2.1. [I.1] Quemas
5.2.2. [I.2] Desastres por inundaciones.
5.2.3. [I.*] Catástrofes fabriles – Exceso de instalaciones eléctricas.
5.2.4. [I.3] Infección por moho – Esporas.
5.2.6. [I.5] Daños procedencia física – Daños en Activos. Pueden ser ocasionarse por fallas en la marcha.
5.2.7. [I.6] Interrupción eléctrica.
5.3.1. [E.1] Fallas de los usufructuarios
5.3.2. [E.2] Equivocaciones humanas.
5.3.3. [E.3] Equivocaciones de control y vigilancia.
5.3.4. [E.4] Equivocaciones de autenticación.
5.3.13. [E.20] Debilidades software.
5.3.15. [E.23] Equivocaciones cuidados / autenticación Activos
5.3.17. [E.25] Extravío de activos.
5.4.2. [A.4] Adulteración de la autenticación.
5.4.3. [A.5] Usurpación de usuarios.
5.4.4. [A.6] Extralimitación de acceso.
5.4.5. [A.7] Prácticas y usos sin sospecha.
5.4.9. [A.11] Entradas sin permiso.
5.4.10. [A.12] Estudio de tránsito.
5.4.12. [A.14] Escucha de datos.
5.4.17. [A.23] Adulteración de activos.
5.4.18. [A.24] Prohibición de atención.
5.4.19. [A.25] Hurto.
5.4.20. [A.26] Agresión dañina.

*B.1.4 Peligros al **Dispositivo** hardware firewall Cisco*.
5.1.1. [N.1] Quemas - Incendios.
5.1.2. [N.2] Desastres inundaciones.
5.1.3. [N.4, N.6, N.7] Catástrofes - Cataclismo, Clima y sismos.
5.2.1. [I.1] Quemas - Incendios.
5.2.2. [I.2] Desastres e inundaciones.
5.2.3. [I.*] Catástrofes fabriles – Exceso de instalaciones eléctricas.
5.2.4. [I.3] Infección por moho – Partículas y esporas.
5.2.6. [I.5] Daños procedencia física – Daños Activos. Pueden ocasionarse debido a una falla en la marcha.
5.2.7. [I.6] Interrupción del abastecimiento.
5.3.1. [E.1] Equivocaciones humanas.
5.3.2. [E.2] Equivocaciones de los usuarios.
5.3.3. [E.3] Equivocaciones de control y vigilancia.
5.3.4. [E.4] Equivocaciones de autenticación.
5.3.13. [E.20] Debilidades software.
5.3.15. [E.23] Equivocaciones cuidados / autenticación activos.
5.4.2. [A.4] Adulteración de la información.
5.4.3. [A.5] Usurpación de usuarios.
5.4.4. [A.6] Extralimitación de privilegios de entrada.
5.4.9. [A.11] Entradas sin permiso.

5.4.12. [A.14] Escucha de datos.
5.4.18. [A.24] Prohibición de atención.

*B.1.5 Peligros del bastidor de dos postes.*
5.1.1. [N.1] Quemas - Incendios.
5.1.2. [N.2] Desastres e inundaciones.
5.1.3. [N.4, N.6, N.7] Catástrofes – Cataclismo, Clima y Sismos.
5.2.1. [I.1] Quemas - Incendios.
5.2.2. [I.2] Desastres e inundaciones.
5.2.3. [I.*] Catástrofes fabriles – Exceso en instalaciones eléctricas.
5.2.4. [I.3] Infección por moho – Partículas y esporas.
5.2.6. [I.5] Daños procedencia física – Daños Activos. Pueden ser ocasionados a una falla de origen durante el transporte.
5.2.7. [I.6] Interrupción del servicio.
5.3.1. [E.1] Equivocaciones humanas.
5.3.2. [E.2] Equivocaciones del usuario.
5.3.3. [E.3] Equivocaciones de Control y vigilancia.
5.3.4. [E.4] Equivocaciones en montaje.
5.3.13. [E.20] Debilidades de los montajes (calidad de los materiales).
5.3.15. [E.23] Equivocaciones y cuidados / autenticación activos.
5.4.2. [A.4] Adulteración del armario (bastidor y postes).
5.4.3. [A.5] Usurpación humana de mantenimiento.
5.4.4. [A.6] Extralimitación de libertades de entrada.
5.4.9. [A.11] Entradas sin permiso.
5.4.12. [A.14] Escucha de datos, cuando se utiliza para otros fines (espía).
5.4.18. [A.24] Se utiliza para sabotear el servicio.

Fig. 5

*B.2 Orígenes de las Debilidades de los Activos del Suministro de Datos y Voz IP de la Cooperativa*

Una vez mejoradas las tablas de las debilidades, se ponen en claro que flaquezas posee el suministro de Datos y Voz IP de la cooperativa; por intermedio de la investigación de los arreglos efectuados a los activos, la reflexión de los conocimientos y operaciones, se recomienda utilizar herramientas automatizadas de busca de debilidades como (Open VAS, Nmap, SipVicious, Hydra, John, entre otros), la lectura de las Cartillas Metodológicas lograda en las asignaturas vistas en el Postgrado. Son el fruto de éste análisis, donde se obtienen detalles de las debilidades de cada Activo.[3]

Estas debilidades han sido evaluadas a través del sistema CVSS (Vulnerabilidades), una técnica creada por la FIRST para acordar y especificar lo crítico de las debilidades. Con el fin de acordar el golpe que significa una debilidad se manejó un escalafón del 0 al 10**.** Se trata de un sistema de puntaje diseñado para proveer un método estándar, que permite estimar el impacto derivado de vulnerabilidades identificados en tecnologías de información.[4]

Se encuentran diversas herramientas en la Red que ayudan a efectuar este procesamiento de datos y a continuación revelan diversas razones sobre las debilidades encontradas; de igual manera, las herramientas automatizadas de busca de debilidades como (Open VAS, Nmap, SipVicious, Hydra, Jo.hn, entre otros), para su eficaz funcionamiento descargan bases de datos con debilidades concurridas por NVDB.

TABLA I
Debilidades Servidor de Datos y Voz IP

| **Activo** | **Servidor de Datos y Voz IP** | |
|---|---|---|
| **Vulnerabilidad** | **Valor CVSS V2** | **Valoración** |
| No se encuentra Activo de emergencia, en caso que este se dañe. | 10.0 | Alta |
| Rebosamiento por correos SIP INVITE | 10.0 | Alta |
| Realización de comandos FreePBX 'index.php'. | 10.0 | Alta |
| El equipo no tiene con un Firewall adaptado | 9.0 | Alta |
| El equipo no cuenta con un sistema de entradas | 9.0 | Alta |
| Sin sistemas de mitigación fuego en la habitación. | 8.0 | Alta |
| Situado erradamente (Bajo la Mesa) | 8.0 | Alta |
| Parametro vtiger CRM 'onlyforuser' entre el Sistema Operativo (SQL) | 7,5 | Alta |
| Instalación remota de comandos Vtiger CRM | 7,5 | Alta |
| Sistema Operativo SQL Inyección Vtiger | 7,5 | Alta |
| Realización distante de direcciones en medio FreePBX, a través de series de ordenanza en lugares (XSS). | 7,5 | Alta |
| expuesto a amenazas individuo | 6,7 | Media |
| Ordenador de internet está expuesto a actividades de filtración suministradas de manera distante. | 5,7 | Media |
| Acceso a internet: TRACE XSS | 5,7 | Media |
| Sistema Manager despejado y sin limitaciones. | 4.9 | Media |
| Certificado para frecuentar páginas seguras de internet ya vencido. | 4.9 | Media |
| El servicio de teléfono, | 4.9 | Media |

| | | |
|---|---|---|
| desaprovecha la característica de cookie httpOnly. | | |
| Suministro de código PHP al servicio Tiger | 4,8 | Media |
| CRM ' | 4,2 | Media |
| Cantidad de series de órdenes en lugares cruzados (XSS), vtiger CRM. | 4,2 | Media |
| Páginas de internet seguras | 4,2 | Media |
| Utilización de páginas seguras de internet desusado. | 4,2 | Media |
| El OpenSSL colocado es tendente a evidenciar datos. | 4,2 | Media |
| Cantidad series de órdenes en (XSS), | 4,2 | Media |
| Seguridad en las marcas de tiempo TCP | 2,5 | Baja |

TABLA II
Vulnerabilidades de las Tarjetas de Red que transportan Datos y Voz

| **Activo** | **Tarjetas de Red que transportan Datos y Voz** | |
|---|---|---|
| **Debilidad - Vulnerabilidad** | **Valor CVSS V2** | **Valoración** |
| No se evidencia activo de emergencia, en caso que este se dañe. | 10.0 | Alta |
| Situado en un lugar no apto. (bajo el Escritorio) | 8.0 | Alta |
| Sin sistemas de mitigación de fuego en el área de comunicaciones. | 8.0 | Alta |

TABLA III
Debilidades y Vulnerabilidades de las Estaciones de trabajo

| **Activo** | **PC equipos Dell** | |
|---|---|---|
| **Debilidad - Vulnerabilidad** | **Valor CVSS V2** | **Valoración** |
| Aglomeración por datos | 10.0 | Alta |
| Realización abusiva de direcciones maliciosas | 4.9 | Media |
| Propagación de información. | 4.9 | Media |
| Seguridad en las marcas de tiempo TCP | 2,4 | Baja |
| Arriesgado a la mano de los – Asociados que se atienden en la Cooperativa. | 1.5 | Baja |

TABLA IV
Debilidades y Vulnerabilidades de las Estaciones de trabajo

| **Debilidades** | **Valor CVSS V2** | **Valoración** |
|---|---|---|
| Aglomeración por datos | 10.0 | Alta |
| Sin evidencia de equipos de emergencia. | 10.0 | Alta |
| Sin evidencian procedimientos de mitigación de fuego en el área de comunicaciones. | 8.0 | Alta |
| Seguridad en las marcas de tiempo TCP | 2,5 | Baja |

Seguridad en las marcas de tiempo TCP

TABLA V
Debilidades Cortafuegos

| **Activo** | **Firewall Cisco** | |
|---|---|---|
| **Debilidades** | **V2** | **Valor** |
| Aglomeración por datos | 10.0 | Alta |
| Sin evidencia de equipos de emergencia, en caso que este se dañe. | 10.0 | Alta |
| Sin evidencia de mitigación fuego en el área de comunicaciones. | 8.0 | Alta |
| Seguridad en las marcas de tiempo TCP | 2,5 | Baja |

VI
Debilidades Cortafuegos

| **Activo** | **Firewall Cisco** | |
|---|---|---|
| **Debilidad y Vulnerabilidad** | **Valor CVSS V2** | **Valoración** |
| Aglomeración por mensajes SIP INVITE | 10.0 | Alta |
| No se evidencia activo de emergencia, si este se daña. | 10.0 | Alta |
| Válido a login HTTP a traveés de credenciales por defecto. | 9.0 | Alta |
| Sin evidencia un método de mitigación de fuego en el área de comunicaciones. | 8.0 | Alta |

*C. Observaciones posibilidades de riesgos y su golpe según, las intimidaciones y debilidades preliminarmente encontradas*

Se evaluó la posibilidad de que el riesgo se cristalice y el daño que causaría a la Entidad en carácter cuantitativo y cualitativo. La evaluación de la posibilidad y el daño se fundaron a la hábito obtenido por los investigadores acerca de la prestación de la función observada.[5]

En seguida, se publican las representaciones cuantitativas y cualitativas empleados para evaluar el riesgo y el daño.[6]

*C.1 Probabilidades: Valores*

Cualitativos: 10 Cuantitativos: muy Alta: Caída, incidente, hecho del medio ambiente o interrupción es casi inequívoco que se provoque; o sucede más de cien veces al año.

Cualitativo: 8. Cuantitativo: Caída, incidente, hecho del medio ambiente o interrupción es crecientemente factible que provoque; o se produzca entre diez y cien veces al año.

Cualitativo: 5. Cuantitativo: Moderada: Caída, incidente, hecho del medio ambiente o interrupción es señal factible que suceda; u ocurra de una a diez veces al año.

Cualitativo: 2. Cuantitativo: Baja: Caída, incidente, hecho del medio ambiente o interrupción no factible que suceda.

Cualitativo uno (1). Cuantitativo: muy Baja: Caída, incidente, hecho del medio ambiente o interrupción es crecientemente irrealizable que se ocasione de una vez cada diez años.

*C.2 Impactos: Valores*

Cualitativo nueve (9) a diez (10). Cuantitativo: Muy alta: Del incidente riesgo se puede pensar que adquiera variados resultados desastrosos sobre los procedimientos de la Entidad, activos, personas o el Estado.

Cualitativo: 8 a 8.9. Cuantitativo: Alta: De la incidente amenaza se puede esperar que adquiera variados resultados desastrosos sobre los procedimientos de la Entidad, activos, personas o el Estado. El resultado desfavorable, peligroso o desastroso:

I. Ocasionar desventaja en el contenido de la misión a una categoría y estabilidad que la Entidad no está preparada para resolver los procedimientos principales.
II. Inducir a perjuicios de los patrimonios de la Entidad.
III. Provocar un daño financiero.
IV. Inducir a detrimentos graves o desastrosos a las vidas humanas.

Cualitativo: 5 a 7.9. Cuantitativo: Moderada: Del incidente riesgo se puede pensar que adquiera un variado resultado procedimientos de la Entidad, activos, personas, otras organizaciones, o el Estado. El resultado desfavorable, peligroso o desastroso:

I. Incitar a una degradación importante en el contenido de los objetivos.
II. Tratar completamente cualquier clase de daño a los equipos de la Entidad.
III. Inducir a significativos quebrantos financieros.
IV. Inducir pérdidas de vidas humanas.

Cualitativo dos (2) a cuatro con nueve (4.9). Cuantitativo: Baja: Resultado desfavorable pero limitado en donde se puede:

I. Daño en el contenido de los objetivos.
II. Daños mínimos en equipos.
III. Pérdida financiera.
IV. Menor daño a los individuos.

Cualitativo: 0 a 1.9. Cuantitativo: Muy baja: Se espera que no haya un efecto importante.

TABLA VII
Construcción de las cadenas causales de la situación problema

| Medio | Proceso de información |
|---|---|
| **Intrusos** | Empleados de otros departamentos<br>Proveedor de servicios informáticos<br>Operador de telefonía<br>Acceso a Internet<br>Por correo electrónico.<br>Por correo tradicional,<br>Por mensajería instantánea, |
| **Empleados** | Utilización segura de las aplicaciones servicios<br>Evitar la entrada de virus y otros códigos dañinos<br>Reconocer las técnicas de ingeniería social<br>Conocimiento de sus obligaciones y responsabilidades<br>Soportes informáticos<br>Reaccionar ante incidentes |
| **Dumpster diving** | Botar papeles corporativos a la papelera, el personal de limpieza toma la basura y la coloca en los tanques provistos para que los recoja el barrendero.<br>Se apropian de los papeles desde la basura antes que se los lleve el camión<br>Los papeles contienen información de nombres cargos y extensiones de ejecutivos de la empresa balances financieros.<br>Esta información es suficiente para lanzar un ataque exitoso de ingeniería social |
| **Correos** | Suplantan la identidad de otra persona u organización.<br>Incluyen ficheros o textos maliciosos |
| **Foros y chats** | Para conseguir tener acceso a determinados ficheros del sistema. |
| **Shoulder surfing** | Espionaje para obtener su nombre de usuario. |
| **Websites** | Maliciosos que tratan de engañar a sus usuarios |

[6]

VIII

Matriz Riesgo del Servidor Datos y Voz IP

| **Activo: Servidor de Datos y Voz IP** | **Impacto** | | | **Probabilidad** | | **Riesgo inherente** | |
|---|---|---|---|---|---|---|---|
| **Debilidad - Vulnerabilidad** | **V. cuantitativo** | **V. cualitativo** | **Amenazas (Catalogo Magerit V3)** | **V. cuantitativo** | **V. cualitativo** | **V. cuantitativo** | **V. cualitativo** |
| Sin evidencia de equipo de emergencia por daño | 10.0 | Muy alta | Quemas - Incendio | 1 | Bajo | 21 | Bajo riesgo |
| | | | Quemas - Incendio | 1 | Bajo | 21 | Bajo riesgo |
| | | | Infección moho | 1 | Bajo | 21 | Bajo riesgo |
| | | | Deterioro | 1 | Bajo | 21 | Bajo riesgo |
| | | | Equivocaciones humanas | 4 | Moderado | 51 | Moderado riesgo |
| | | | Debilidades software | 4 | Moderado | 51 | Moderado riesgo |
| | | | Equivocaciones autenticación hardware | 4 | Moderado | 50 | Moderado |
| | | | Equivocaciones autenticación hardware | 2 | Bajo | 20 | Bajo |
| | | | Agresión dañina | 2 | Bajo | 20 | Bajo |
| Aglomeración Datos | 10.0 | Muy alta | Desaprobación de servicio | 4 | Moderado | 50 | Modero |
| Realización distante órdenes | 10.0 | Muy alta | Adulteración de la configuración | 2 | Bajo | 20 | Bajo |
| | | | Usurpación de la identidad. | 2 | Bajo | 20 | Bajo |
| | | | Entradas no válidas. | 2 | Bajo | 20 | Bajo |
| | | | Escucha de información | 2 | Bajo | 20 | Bajo |
| Sin evidencia de un Firewall autorizado | 9.0 | Muy alta | Debilidades software | 4 | Moderado | 45.0 | moderado |
| | | | Adulteración | 2 | Bajo | 18.0 | bajo |
| | | | Usurpación | 2 | Bajo | 18.0 | bajo |
| | | | 5.4.4. [A.6] Extralimitación de privilegios de entrada | 2 | Bajo | 18.0 | bajo |
| | | | 5.4.9. [A.11] Entradas no válidas | 2 | Bajo | 18.0 | bajo |
| | | | 5.4.12. [A.14] Escucha de información | 2 | Bajo | 18.0 | bajo |
| | | | 5.4.18. [A.24] Desaprobación de servicio | 2 | Bajo | 18.0 | bajo |
| Sin evidencia scaneo de puertos | 9.0 | Muy alta | 5.4.9. [A.11] Entrada no válida | 4 | Moderado | 45.0 | moderado |
| | | | 5.4.12. [A.14] Escuha de información | 2 | Bajo | 18.0 | bajo |
| | | | 5.4.18. [A.24] Desaprobación de servicio | 2 | Bajo | 18.0 | bajo |
| Sin evidencia sistemas de localización, ni mitigación de incendios en el área. | 8.0 | Alta | 5.1.1. [N.1] Quemas - Incendios | 2 | Bajo | 16.0 | bajo |
| | | | 5.2.1. [I.1] Quemas - Incendios | 2 | Bajo | 16.0 | bajo |
| Instalado en sitio no apropiado. (bajo de un Escritorio) | 8.0 | Alta | 5.1.1. [N.1] Quemas - Incendios | 2 | Bajo | 16.0 | bajo |
| | | | 5.2.1. [I.1] Quemas - Incendios | 2 | Bajo | 16.0 | bajo |
| | | | 5.2.4. [I.3] Infección mecánica | 4 | Moderado | 40.0 | moderado |
| | | | Equivocaciones autenticación | 4 | Moderada | 41 | Moderado riesgo |
| CRM ' | 6,9 | Moderado | Debilidad software | 3 | Moderada | 36.0 | Moderado riesgo |
| | | | Adulteración | 1 | Baja | 14 | Bajo riesgo |
| | | | Usurpación | 1 | Baja | 14 | Bajo riesgo |
| | | | 5.4.9. [A.11] Entrada no válida | 1 | Baja | 14 | Bajo riesgo |
| | | | 5.4.12. [A.14] Escucha de información | 1 | Baja | 14 | Bajo riesgo |
| Realización distante CRM. | 6,9 | Moderado | Debilidades de los programas software | 3 | Moderada | 37 | moderado |
| | | | Adulteración | 1 | Baja | 14 | bajo |
| | | | 5.4.3. [A.5] Usurpación de la identidad. | 1 | Baja | 14 | bajo |
| | | | 5.4.9. [A.11] Entrada no válida | 1 | Baja | 14 | bajo |
| | | | 5.4.12. [A.14] Escucha de información | 1 | Baja | 14 | bajo |
| Diversidad | 6,9 | Moderado | Debilidades software | 4 | Moderada | 36 | moderado |
| | | | Adulteración | 1 | Baja | 14 | bajo |
| | | | Usurpación | 1 | Baja | 14.0 | bajo |
| | | | Entrada no válida | 1 | Bajo | 14.0 | bajo |
| | | | Escucha de información | 1 | Bajo | 14.0 | bajo |
| (XSS). | 7,4 | Moderado | Debilidades | 4 | Moderado | 37.0 | Moderado riesgo |
| | | | Adulteración | 1 | Bajo | 14.0 | Bajo riesgo |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | Usurpación | 1 | Bajo | 14.0 | Bajo riesgo |
| | | | Entrada no válida | 1 | Bajo | 14.0 | Bajo riesgo |
| | | | Escucha | 1 | Bajo | 14.0 | Bajo riesgo |
| CCS expuesto a agresiones del individuo | 5,7 | Moderado | Debilidad | 4 | Moderado | 33.0 | Moderado riesgo |
| | | | Adulteración | 1 | Bajo | 13.5 | Bajo riesgo |
| | | | Usurpación | 1 | Bajo | 13.5 | Bajo riesgo |
| | | | Entrada no válida | 1 | Bajo | 13.5 | Bajo riesgo |
| HTTP expuesto | 6,7 | Moderado | 5.Debilidades software | 4 | Moderado | 28.0 | Moderado riesgo |
| | | | Adulteración | 1 | Bajo | 11.5 | Bajo riesgo |
| | | | Usurpación | 1 | Bajo | 11.5 | Bajo riesgo |
| | | | Entrada no válida | 1 | Bajo | 11.5 | Bajo riesgo |
| XSS | 5,7 | Moderado | Debilidades software | 4 | Moderado | 28.0 | Moderado riesgo |
| | | | Adulteración | 1 | Bajo | 11.5 | Bajo riesgo |
| | | | Usurpación | 1 | Bajo | 11.5 | Bajo riesgo |
| | | | Entrada no válida | 1 | Bajo | 11.5 | Bajo riesgo |
| Certificado vencido. | 4.9 | Moderado | Debilidades software | 4 | Moderado | 24.1 | moderado |
| | | | Usurpación | 1 | Bajo | 11.1 | bajo |
| | | | Entrada no válida | 1 | Bajo | 11.1 | bajo |
| Ejecución característica de cookie httpOnly. | 4.9 | Moderado | Debilidades de software | 4 | Moderado | 24.1 | moderado riesgo |
| | | | Adulteración | 1 | Bajo | 11.1 | bajo |
| | | | Usurpación | 1 | Bajo | 11.1 | bajo |
| | | | Entrada no válida | 1 | Bajo | 10.0 | bajo |
| Introducción PHP | 3,8 | Baja | Debilidades software | 4 | Moderado | 24.0 | moderado |
| | | | adulteración | 2 | Bajo | 9.7 | bajo |
| | | | Entrada no válida | 2 | Bajo | 9.7 | bajo |
| Series (XSS), vtiger CRM. | 4,2 | Baja | Debilidades software | 4 | Moderada | 21.4 | moderado |
| | | | Adulteración | 2 | Baja | 8.5 | bajo |
| | | | Entrada no válida | 2 | Baja | 8.5 | bajo |
| Series (XSS), CRM. | 4,2 | Baja | Debilidades software | 5 | Moderado | 21.4 | moderado |
| | | | Adulteración | 2 | Bajo | 8.5 | bajo |
| | | | Entrada no válida | 2 | Bajo | 8.5 | bajo |
| SSL. | 4,2 | Baja | 5.3.13. [E.20] Debilidades de los programas (software) | 4 | Moderado | 21.4 | moderado |
| | | | 5.4.12. [A.14] Escucha de información (escucha) | 2 | Bajo | 8.5 | bajo |
| SSL2- SSL3 inadecuado. | 4,2 | Baja | 5.3.13. [E.20] Debilidades de los programas (software) | 4 | Moderado | 21.4 | moderado |
| | | | Escucha | 1 | Bajo | 8.5 | bajo |
| Open SSL instaurado esta expuesto | 4,2 | Baja | Debilidades | 4 | Moderado | 21.3 | moderado |
| | | | Escucha | 1 | Bajo | 8.4 | bajo |
| Cantidade de series de órdenes en lugares cruzados (XSS), Elastix. | 4,2 | Baja | Debilidades de los programas software | 4 | Moderado | 21.3 | bajo |
| Seguridad en las marcas de tiempo TCP | 3,5 | Baja | Desgastación de atención | 2 | Muy bajo | 2.4 | Muy bajo |

TABLA IX
Matriz Riesgo Tarjeta Red

| **Activo: Tarjeta de Red** | **Impacto** | | | **Probabilidad** | | **Riesgo inherente** | |
|---|---|---|---|---|---|---|---|
| **Vulnerabilidad Debilidad** | **Valor cuantitativo** | **Valor cualitativo** | **Amenazas** | **Valor cuantitativo** | **Valor cualitativo** | **Valor cuantitativo** | **Valor cualitativo** |
| Sin evidencia equipos de emergencia. | 10.0 | Muy alta | 5.1.1. [N.1] Quemas Incendios | 2 | Bajo | 20.1 | bajo |
| | | | Quemas Incendios | 1 | Bajo | 20.1 | bajo |
| | | | Infección moho | 1 | Bajo | 20.1 | bajo |
| | | | 5.3.2. [E.2] Fallas del administrador | 4 | Moderada | 50.0 | Moderado riesgo |
| | | | Debilidades software | 4 | Moderado | 49 | moderado |
| | | | Fallas autenticación | 1 | Bajo | 19 | bajo |
| | | | Agresión dañina | 1 | Bajo | 19 | bajo |
| Localizado en un sitio no apto. (bajo de un Escritorio) | 8.0 | Alta | Quemas Incendios | 1 | Bajo | 15 | bajo |
| | | | 5.2.1. [I.1] Quemas Incendios | 1 | Bajo | 16 | bajo |
| | | | Infección mecánica | 5 | Moderada | 40 | moderado |
| | | | Fallas autenticación | 4 | Modera | 39 | moderado |
| Sin evidencia mitigación de fuego. | 8.0 | Alta | Quemas Incendios | 2 | Baja | 15 | bajo |
| | | | 5.2.1. [I.1] Quemas Incendios | 2 | Baja | 15 | bajo |

X
Riesgo Estaciones trabajo

| **Activo: PC equipos Dell** | **Impacto** | | | **Probabilidad** | | **Riesgo inherente** | |
|---|---|---|---|---|---|---|---|
| **Vulnerabilidad - Debilidades** | **Valor cuantitativo** | **Valor cualitativo** | **Amenaza** | **Valor cuantitativo** | **Valor cualitativo** | **Valor cuantitativo** | **Valor cualitativo** |
| Realización abusiva | 4.9 | moderado | Debilidades software | 5 | Moderada | 25.1 | moderado |
| | | | adulteración | 1 | bajo | 11.1 | bajo |
| | | | Interceptación escucha | 2 | bajo | 11.1 | bajo |
| | | | Adulteración activos | 2 | bajo | 10.0 | bajo |
| httpdd | 4.9 | moderado | Debilidades software | 4 | moderado | 26.1 | moderado |
| | | | Adulteración | 1 | bajo | 11.1 | bajo |
| | | | Escucha de información | 1 | bajo | 11.1 | bajo |
| | | | Adulteración de activos | 1 | bajo | 11.1 | bajo |
| Seguridad en las marcas de tiempo TCP | 2,5 | bajo | servicio | 2 | muy bajo | 1.5 | muy bajo |
| Exhibido a los Asociados | 1.5 | muy bajo | Quemas Incendios | 1 | bajo | 2.1 | muy bajo |
| | | | Inundaciones | 4 | moderado | 9.1 | bajo |
| | | | Infección moho | 1 | bajo | 2.1 | muy bajo |
| | | | Hurto | 4 | moderado | 9.1 | bajo |
| | | | Agresión dañina | 1 | bajo | 2.1 | bajo |

XI
Dispositivo Cortafuegos

| **Activo: Firewall Cisco** | **Impacto** | | | **Probabilidad** | | **Riesgo inherente** | |
|---|---|---|---|---|---|---|---|
| **Vulnerabilidad - Debilidad** | **Valor cuantitativo** | **Valor cualitativo** | **Amenaza** | **Valor cuantitativo** | **Valor cualitativo** | **Valor cuantitativo** | **Valor cualitativo** |
| Sin evidencia equipo de emergencia | 10.0 | Muy alta | Quemas Incendios | 2.1 | bajo | 21.1 | bajo |
| | | | Quemas Incendios | 2.1 | bajo | 21.1 | bajo |
| | | | Infección moho | 2.1 | bajo | 10.1 | bajo |
| | | | Fallas | 5.1 | moderado | 49.1 | moderado |
| | | | Debilidades software | 5 | moderado | 49.1 | moderado |
| | | | Fallas autenticación | 2.1 | bajo | 21.1 | bajo |
| | | | Agresión dañina | 2.1 | bajo | 21.1 | bajo |
| Sin evidencia mitigación de fuego. | 8.0 | Alta | Quemas Incendios | 2.1 | bajo | 15.1 | bajo |
| | | | Quemas Incendios | 2 | bajo | 15.1 | bajo |
| TCP Timestamp. | 2,6 | bajo | Degradación de servicio | 1 | muy bajo | 2.6 | Muy Bajo |

Tabla XII
Dispositivo Cortafuegos

| **Activo: Firewall Cisco** | **Impacto** | | | **Probabilidad** | | **Riesgo inherente** | |
|---|---|---|---|---|---|---|---|
| **Debilidad** | **Valor cuantitativo** | **Valor cualitativo** | **Amenaza** | **Valor cuantitativo** | **Valor cualitativo** | **Valor cuantitativo** | **Valor** |
| Sin evidencia equipos de emergencia. | 10.0 | Muy alta | Quemas Incendios | 1.1 | bajo | 21.1 | bajo |
| | | | Quemas Incendios | 1.1 | bajo | 21.1 | bajo |
| | | | Infección moho | 2.1 | bajo | 21.1 | bajo |
| | | | Fallas | 4 | moderado | 51.1 | moderado |
| | | | Debilidades software | 4 | moderado | 50.1 | moderado |
| | | | Fallas autenticación | 1 | bajo | 20.1 | bajo |
| | | | Agresión dañina | 1.1 | bajo | 20.1 | bajo |
| Afirmativo HTTP a través de credenciales por defecto. | 9.0 | Muy alta | Adulteración de la configuración | 4 | moderado | 45.0 | moderado |
| | | | Usurpación | 4 | moderado | 45.1 | moderado |
| | | | Entrada no válida | 4 | moderado | 45.1 | moderado |
| | | | Escucha de información | 1.1 | bajo | 18.1 | bajo |
| Sin evidencia mitigación de fuego | 8.0 | Alta | Quemas Incendios | 1.1 | bajo | 16.1 | bajo |
| | | | Quemas Incendios | 2.1 | bajo | 15.1 | bajo |

*E. Observaciones sobre las debilidades, amenazas, impacto, posibilidades y peligros esenciales evidenciados en el servicio de Datos y Voz IP de la Cooperativa Avanza*

*E.1 Comentarios Generales*

Inicialmente, es inevitable interpretar que excepto de las Estaciones de Trabajo IP, todos los equipos del servicio de Voz IP, no cuentan con un sistema o activo que avale que, ante el daño del principal, estos puedan ser prontamente sustituidos y siga la continuidad del negocio.

Igualmente, se complementa que el área de equipos no tiene medios de localización, mitigación de fuego y el apaga fuegos se encuentra a 22 mts. alejado del área de comunicaciones. En caso de una verdadera contingencia por fuego no solo se vería dañados los vitales equipos del servicio de Voz IP, (servidor Voz IP), sino también los diversos equipos de red y servidores que posee la cooperativa Avanza.

Sin embargo, la no presentación de contingencias que deje sin Datos y Voz IP a la cooperativa, es porque el cuarto de Sistemas se ha implementado cabalmente un sistema de suministro eléctrico con procedimientos redundantes y reguladores de voltajes; igualmente se posee unos excelentes equipos de aires acondicionados que evitan calor garrafal de todos los equipos.

El servidor de Voz IP y los teléfonos IP, poseen una misma vulnerabilidad conocida como TCP timestamps. TCP es un protocolo simétrico que permite enviar datos en cualquier momento en cualquier dirección y, por lo tanto, el eco de la marca de tiempo puede producirse en cualquier dirección. Por simplicidad y simetría, especificamos que las marcas de tiempo siempre se envían y repiten en ambas direcciones. Para mayor eficiencia, combinamos los campos de respuesta de indicación de fecha y hora en una única opción de marca de tiempo TCP. [7]

A continuación, se presentan comentarios específicos por cada uno de los equipos de Datos y Voz IP Avanza

*E.2 Servidores de Datos y Voz IP*

Sobre los servidores de Datos y Voz IP, se encuentran varias debilidades de software de alto impacto, con varias amenazas. Lo que ha tranquilizado la probabilidad de que dichas amenazas se plasmen, es que los servicios de Datos y Voz IP, no se encuentran publicados hacia internet, es decir los servidores de Datos y Voz IP son posibles desde la red de la Cooperativa, las cuales, por seguridad, (por razones de privacidad no pueden ser explicadas en este párrafo), muestran ciertos desafíos para que los agresores puedan aprovecharse de dichas fragilidades.

Entre la totalidad de las debilidades de software detectadas, algunas son conexas a una debilidad del sistema de dirección gráfica del servicio de Voz IP, la vulnerabilidad concretamente es la CVE: 2014-7235 que permite a los atacantes remotos ejecutar código arbitrario a través de la cookie ari_auth, relacionada con la función PHP unserialize, explotada en estado salvaje en septiembre de 2014. [8]

Esta vulnerabilidad aprovechada por un usuario perverso o agresor, acepta ignorar la seguridad y permitir actuar como si fuera uno de los administradores autorizados. Esta debilidad agrupada y verificadas de tipo XSS o establecidas como series de órdenes en sitios cruzados, (*Cross-site scripting*), aprobarían en algún momento una revisión total del servidor de Voz IP. Las debilidades XSS que se relacionan con la debilidad principal de para logar el cometido anteriormente mencionado son:

- Realización remota de comandos alrededor, A través de series de órdenes en lugares cruzados (XSS), CVE-2012-4869.
- Cantidad de series de órdenes en lugares cruzados (XSS).

Otras vulnerabilidades de software encontradas, son las relacionadas con el CRM vTiger, que están implícitos e ubicados por descarte con la adaptación a la planta, es un software de cifrado directo, para la dirección con individuos, el cual, incorporado con un servicio de Datos y Voz IP, Consiente que cuando se implante una comunicación de red o telefónica con un Asociado, instintivamente en el computador del asesor de servicios se desarrolle todo el historial de operaciones e investigación personal de este. Con esto las Entidades puedan implantan una relación efectiva y rápida con sus clientes. [9]

Las vulnerabilidades más importantes encontrada con respecto a vTiger, con la cual agresores remotos pueden establecer comandos SQL inoportunos a través del parámetro onlyforuser en una acción índex a index.php, obteniendo vía al servidor. [10]

Otras vulnerabilidades que se pueden asociar para obtener un alto impacto son:

- Realización remota de comandos Vtiger CRM 'class.phpmailer.php', BID:49946.
- Ejecución de código PHP al programa vTiger CRM, CVE-2013-3214.
- Series de órdenes en lugares cruzados (XSS), vtiger CRM 'vtigerservice.php', BID:47267.
- Cantidad de series de órdenes en lugares cruzados (XSS), Elastix, CVE-2011-4670.

El CRM vTiger, como ya se ilustraba en el artículo anterior, están ubicados en uno de los servidores de Voz IP de la Entidad. Al ser examinado por los funcionarios TIC de la Avanza acerca de lo anterior, informo que existía noción de su presencia, pero que no estaba siendo utilizado.

Para la incorporación a las sesiones de administración gráfica web, se reveló que la clase de cifrado por el protocolo HTTP convincente era arcaico y divulgaba los datos de la versión de SSL había vencido. Las debilidades evidenciadas sobre SSL, aprobarían a un usuario mal intencionado o agresor a ejecutar una agresión del tipo "*man-in-the-middle*" y poder entender texto que se encuentra cifrado. [11]

Las vulnerabilidades SSL encontradas son:

- Openssl CCS expuesto a agresiones del individuo en el medio, CVE-2014-0224.
- Certificado SSL expiró y serán reemplazados con nuevas actualizaciones.
  *Certificate details:*
  *fingerprint: 6909A65569CFF51F62733BC53065CC9F7C7B8F4E*""
- El OpenSSL instalado es tendiente a propagar información, CVE-2014-3566.

Sobre los protocolos utilizados por los servidores de Datos y Voz IP para instaurar la señalización de todos las terminales (PC de las Estaciones de Trabajo, Teléfonos IP y Tarjetas de Red), se halló propenso a agresiones, la cual velozmente extingue implementos de máquina y puede ocasionar que se encuentre fuera de funcionamiento.

En relación con el hardware, es alarmante que, aunque el equipo se localiza en las áreas que corresponde (cuarto de equipos) y cuentan Aires acondicionados, el servidor físicamente se encuentra ubicado bajo un escritorio de madera y no en el rack principal, algo que con seguridad ninguna norma, ni recomendación técnica avalaría. Al estar localizado en este lugar, existe la posibilidad de una aglomeración de calor, que lleva a la avería de las partes electrónicas de los aparatos o a la probabilidad de quemarse. En razón de encontrase ubicado en un lugar de difícil paso las reparaciones del equipo, se confunden más de lo normal, con el riesgo de presentarse fallas de manejo por parte de los funcionarios TIC de la Entidad.

*E.3 PC Dell (Estaciones de Trabajo)*

Todos los computadores analizados tienen una dirección IP, se les encontró una debilidad en sus sistemas de administración y ordenación gráfica (*miniHTTPD*), en donde un agresor toma control del computador y tendría acceso como revisar y/o modificar los datos de configuración, hasta manipular los datos e interceptar las comunicaciones.

*E.4 Sistema Informático Financiero (Opa Ltda.)*

No se presentaron debilidades importantes en el servidor, sin embargo, ocurren eventos de compatibilidad y programación.

*E5. Gateway Freego 2008QA (Servidor de voz)*

Igualdad de contraseña lo que permitiría que usuarios malintencionados y atacantes pueden fácilmente sacar provecho.

*F. Sugerencias para disminuir los peligros de Datos y Voz IP de la Entidad Avanza*

En general, todos los equipos de Datos y Voz IP de Avanza se localizan en riesgo bajo y moderado, debido a dos factores: el primero, por algunas atenciones de protocolo presentes en la red de la Entidad, y por otro lado, No es posible acceder al servicio desde internet. Desafortunadamente por estas medidas, se desperdician otros servicios importantes y necesarios para la Entidad a dispositivos como Smartphone, tabletas y laptops.

En los servidores de Datos y Voz IP se recomienda realizar un proceso de hardening que incluye:

- Ejecutar todas las actualizaciones disponibles para la distribución que está siendo utilizada.
- Establecer un firewall en los servidores, creando políticas de acceso por ACL, dirección IP y usuarios.
- Autorizar la integridad de los ejecutables del sistema con herramientas como chkrootkit o rkhunter.
- Controlar la integridad de los directorios y archivos por medio de cálculo hash.
- Contar con extensiones SIP e IAX2, usado para fomentar la separación de privilegios.
- Cambiar periódicamente todas las claves de acceso a los servidores.

*A. Marco Conceptual*

*1) La ingeniería social:* Es el arte de obtener información confidencial a través de la manipulación de usuarios legítimos sin que la persona que está siendo "atacada" se dé cuenta. Son técnicas basadas en engaños que se emplean para dirigir la conducta de una persona u obtener información sensible.

Es decir que implica valerse de cualquier medio para obtener información acerca de una o varias personas, con el fin de obtener lucro o perjudicar y causar daño.

*2) Ingeniería social en la empresa:* Dentro de la ingeniería social hay una frase que es la respuesta a toda premisa "una cadena se rompe siempre por el eslabón más débil".
De nada servirá si la red es cien por ciento segura como afirman los empresarios, si las personas que laboran en ella no están bien capacitadas, si no hay unos protocolos de actuación bien definidos [18].

*3)* Sin embargo, la vulnerabilidad puede estar en la persona, es decir cuando ésta suministra información el ataque será más fácil.
*4) Vulnerabilidades de Seguridad Física:* En teoría la seguridad física debería impedir cualquier fuga de información, pero tratando de cumplir con dicho cometido, hay que tomar precauciones adicionales.
Toda persona que ingrese a las instalaciones debe portar en un lugar visible su carnet de funcionario o de visitante. Todos los documentos que contengan información sensible deben ser almacenados bajo custodia.
Los documentos que contengan información sensible y que deban ser desechados deben ser procesados en una trituradora de papel. Todos los medios de almacenamiento digital que se vayan a desechar deben ser desechados quizás contratando una empresa que los destruya.
Las canecas de basura deben mantenerse bajo llave en áreas que estén monitoreadas por los servicios de seguridad con que cuente la Organización.

*5) Internet*: Una de las herramientas tecnológicas que más ha tenido impacto en la sociedad y se ha convertido en el sistema de comunicaciones de alcance mundial, económico el cual ha sido de fácil manejo.
Está presente continuamente en la vida de todas las personas, es una de las herramientas tecnológicas más revolucionarias y poderosas de los últimos tiempos, influye fácilmente en las actividades humanas.
Se puede obtener información sobre cualquier tema de interés.
Su importancia es tal que muchas empresas tienen sitios en Internet en donde muestran información acerca de sus productos y servicios y tienen una mejor relación con sus clientes [19]
Uno de los servicios más importantes de Internet al mundo es el servicio educativo por esa vía.
No obstante, las barreras políticas entre países, distancias entre personas e incluso entre lenguajes, la educación se manifiesta en Internet como uno de los atributos más favorables y productivos a todos los niveles y esferas sociales en todos los países.

Esta investigación está dirigida a todo tipo de empresas que procesan datos que sean custodios de información, de cualquier sector público, privado económico o industrial.
Se busca obtener unos beneficios con la implementación de este proyecto, con el fin de prevenir o reducir eficazmente el nivel de riesgo, mediante la implementación de controles adecuados; de esta forma poder preparar a la comunidad ante posibles emergencias con el fin de garantizar la continuidad del proyecto, teniendo en cuenta la política, la estructura organizativa, los procedimientos y los recursos de seguridad en términos de integridad, confidencialidad y disponibilidad.
Se busca incrementar el nivel de concientización del personal respecto a los temas de seguridad informática.

*B. Principios de la Seguridad Informática*
*1) Confidencialidad:* "se trata de la cualidad que debe poseer un documento o archivo para que éste sólo se entienda de manera comprensible o sea leído por la persona o sistema que esté autorizado"[20]

*2) Integridad:* "es la cualidad que posee un documento o archivo que no ha sido alterado y que además permite comprobar que no se ha producido manipulación alguna en el documento original".

*3) Disponibilidad:* la NTC-ISO/IEC 27001 la define como aquella cualidad de la información que le permite ser accesible y utilizable sólo por una entidad autorizada.

*C. Entorno Del Proyecto*
Está relacionado con todos y cada uno de los elementos externos que pueden afectar e influir sobre él y que pueden ser influenciados, dentro de este se puede encontrar el entorno general que es aquel que afecta de la misma forma a los aspectos legales, económicos, tecnológicos y factores socio culturales, por otra parte, se encuentra el entorno especifico que es aquel donde los elementos afectan de forma directa al proyecto.
De igual manera se establecen unos tiempos de ejecución y puesta en marcha del proyecto.
Para efectos de la presente investigación se toma como referencia una entidad financiera, se pretende analizar el manejo y control que se le da a la información tanto en el área personal como empresarial.
La información está catalogada como un activo valioso por consiguiente debe estar protegida adecuadamente, garantizando la continuidad de los sistemas de información, minimizando los riesgos de daño y contribuyendo de esta manera a una mejor gestión.
Se requiere contar con estrategias que permitan el control y administración efectiva de los datos y de quienes acceden y la utilizan. Hoy en día se está expuesto a muchos incidentes como el fraude, actos de espionaje, vandalismo, sabotaje, hurto entre otras.
De igual manera los riesgos de daño y pérdida de información por causa de código malicioso, cada vez se hacen más frecuentes.

*D. Identificación de los actores relevantes*

*1) Directores:* Conocen conceptualmente las características de un trabajo en equipo, se produce entre saber lo que hay que hacer y efectivamente ser capaces de hacerlo, de acuerdo a las necesidades de su organización. Entonces, el director será el que manda, normalmente trabaja a instancias de una relación mando-obediencia, ordena, guía y dispone todo cuanto debe hacerse en orden a conseguir los objetivos propuestos en su tarea o emprendimiento [21].

*2) Asesores:* Se designa a aquel individuo que como actividad profesional se encarga de brindar asesoría a determinadas personas que se encuentran ante determinadas circunstancias, preferentemente sobre imagen, gobierno, finanzas, política, ciencia, entre otras.

*3) Asesor Financiero:* Encargado de descubrir las necesidades financieras de su cliente, analizando una determinada cantidad de cuestiones pasadas, presentes y futuras de éste, teniendo en cuenta además su edad, patrimonio disponible, tipo impositivo, situación familiar y profesional. Una vez analizadas todas estas variables, el asesor, le brindará a su cliente una serie de alternativas y recomendaciones de inversión que se ajusten a todo ello que se analizó [22].

*4) Cliente:* Es aquel individuo que, mediando una transacción financiera, adquiere un producto y/o servicio de cualquier tipo (tecnológico, gastronómico, decorativo, mueble o inmueble, etcétera). Un cliente es sinónimo de comprador o de consumidor y se los clasifica en activos e inactivos, de compra frecuente u ocasional, de alto o bajo volumen de compra, satisfecha o insatisfecha, debe asegurarse de tomar en cuenta tanto las necesidades como las expectativas de cada cliente. Es tanto para los negocios y el marketing como para la informática un individuo, sujeto o entidad que accede a recursos, productos o servicios brindados por otra.

5) *Secretaria:* Es aquella persona que se ocupa de la realización de actividades elementales de oficina, ya sea en una empresa privada o pública, además de ser la estrecha colaboradora del directivo o ejecutivo al cual asiste.

7) *Profesionales de control:* En cumplimiento de la gestión debe ser controlado con el fin de garantizar que los servicios a cargo de la entidad, prestados a través de sus empleados, cumplan con los objetivos y funciones asignadas.

*8) Vigilancia:* Consiste en el monitoreo del comportamiento de personas, de objetos o de procesos que se encuentran insertos dentro de un determinado sistema con el objetivo de detectar a aquellos que interfieran con la conformidad de las normas vigentes, deseadas o esperadas, intrusos, ladrones, espías, entre otros.

9) *Intruso:* Persona que se ha introducido en una propiedad, lugar, asunto o actividad sin derecho o autorización.

*E. Responsabilidad de los actores*

1) *Los usuarios:* No tienen claro la importancia de salvaguardar la información, no son cautos al momento de dar las diferentes claves de acceso o cuando suministran información a terceros.

2) *Los empleados:* No están capacitados, con respecto a los protocolos de seguridad, y si en alguna ocasión les han dado esta información no la ponen en práctica, dicho en ingeniería social podría sacar información suficiente de la empresa sin ser descubierto en tan solo unas horas.

“Con esto se debe tener en cuenta que dentro de la seguridad existe una cadena y que, si esta se rompe, siempre por el eslabón más débil".

Por último y de acuerdo a lo anterior la función principal del Administrador del Sistema, debe dar como resultado final proteger la información que se encuentra en los servidores, valiéndose de herramientas tecnológicas y físicas contra factores externos dentro y fuera de la Entidad.

## X. DISCUSIÓN Y CONCLUSIONES

El servicio que prestan los Servidores de la Cooperativa Avanza se encuentra en un pequeño a un módico nivel de inseguridad, esto se logra optimizar si se efectúan las encomiendas marcadas en este trabajo. Las medidas de seguridad desarrollados con el cableado de las redes locales han apoyado a que no sucedan muestras de incidencias de seguridad en la prestación del servicio. Sera sensato ejecutar un estudio de inseguridad a dicha red para que descubra debilidades y reducir los peligros; de esta manera cualquier servicio informático de la cooperativa se verá beneficiado.

Se hallan medidas con el Backup para asistencia de almacenamiento de Datos y de Voz IP con una planta telefónica implementada hace algunos años, los equipos contra incendios en el cuarto de máquinas y comunicaciones son necesarios, así que los funcionarios TIC y la alta dirigencia de la Entidad consideren y desarrollen esta problemática lo más rápido posible. (quedara resuelto al trasladarnos a la nueva Sede)

Los funcionarios TIC de la Entidad, se comprometerían a estar más atentos en la relación con los proveedores de mantenimiento del servicio de Datos y Voz IP, ya que en materia de seguridad no conceden una buena asistencia.

Existen diferentes oportunidades de negocios, que brindan la asistencia de Datos y Voz IP. Se debe estudiar cuál de ellas consiguen ser favorables para la Entidad y que involucra colocarlas en curso.

Discusión de los resultados obtenidos, impacto resultante en la empresa o entidad al implementar nuevos procesos, aspectos relevantes que se hayan descubierto en el proceso de construcción de los entregables y aprendizajes resultantes de dicho proceso.

LA EMPRESA COOPERATIVA AVANZA

Por último, la organización es una empresa de capital privado de tamaño medio (podemos suponer más de 100 empleados en todas sus Agencias) dedicada al ahorro y al crédito, sus aplicaciones son de tipo bancario basadas en tecnologías web y criptográficas, como, por ejemplo: portales de banca electrónica para clientes finales, terminales financieros, etc.

Los negocios más habituales se refieren a captar y prestar dinero; negocio bancario que interaccionan con un host / mainframe. La arquitectura de las aplicaciones ofrece a los clientes tecnologías web y siguen la estructura de aplicaciones de tres capas.

Respecto a sus TIC

Nos disponemos a llegar a un diagrama de alto nivel con la arquitectura de los sistemas propios, como se evidencia a continuación: [26]

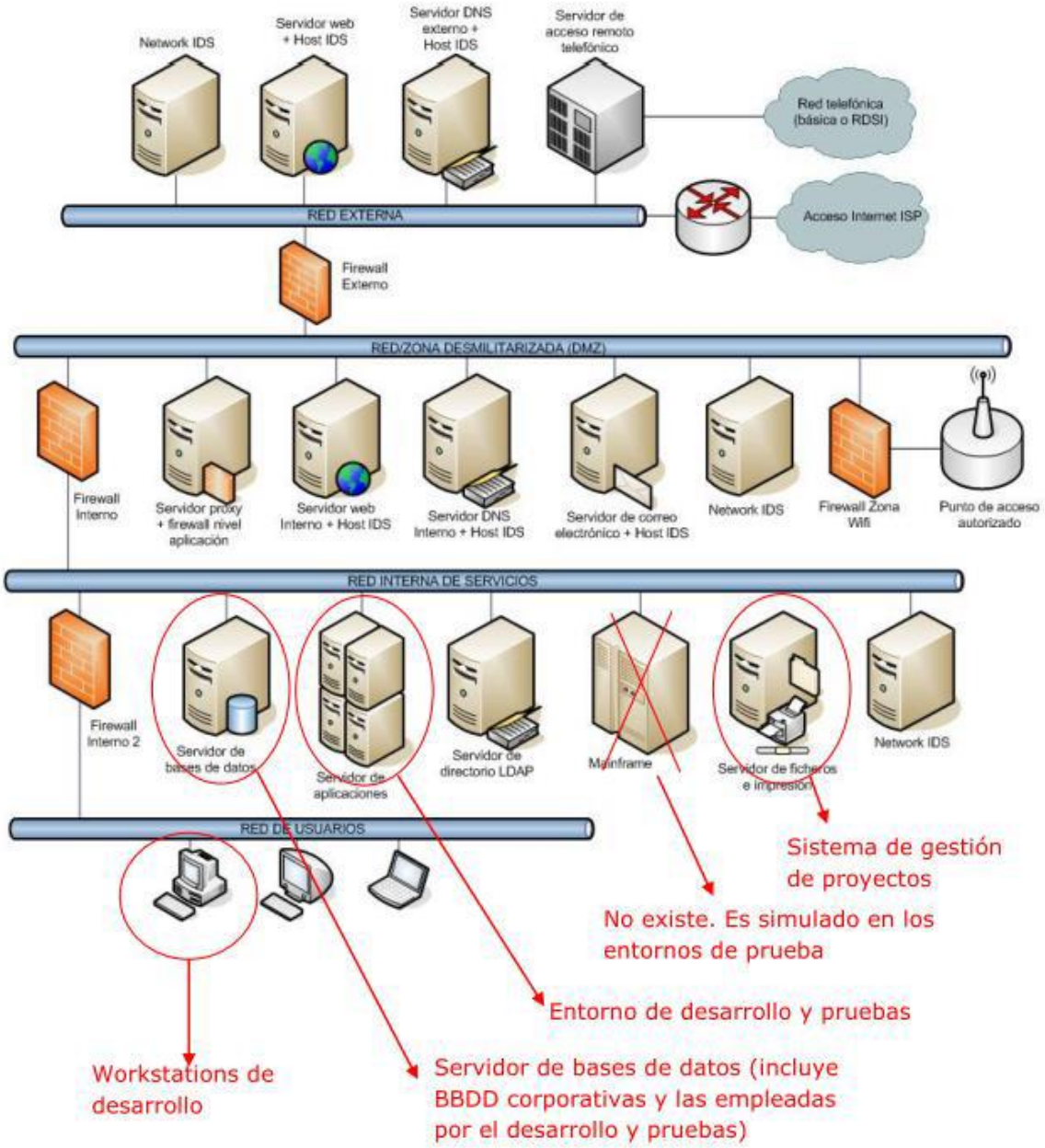


Fig. 5

RECONOCIMIENTOS

El autor agradece a la Cooperativa Avanza en cabeza de su Gerente el Doctor Geovani Muñoz Chávez, por haberme permitido desarrollar el presente artículo. Agradezco también al Director de Sistemas de la Cooperativa Avanza Ingeniero Fabián Benjumea Loaiza por haberme asesorado respectivamente en la parte técnica del artículo.

BIBLIOGRAFÍA

[1] https://www.sinnaps.com/blog-gestion-proyectos/metodologia-de-un-proyecto
[2] E. Landívar, "Comunicaciones Unificadas con Elastix
[3] USERSHOP.
[4] CVSS.
[5] [Online]. BlogSegurid/analisis sencillo.
[6] NIST National Institute of Standars, Sep-2012.
[7] https://translate.google.com.co.
[8] https://cve.mitre.org/cgi-bin/cvename.
[9] *Wikipedia, la enciclopedia*
[10] CVE-2011-4559. [Accessed: 25-Nov-2015].
[11] CVE-2014-3566 Red Hat, Inc, [Accessed: 23-Nov-2015].
[12] L*os extintores*, 2010. [Online]. Available, los-extintores. [Accessed: 25-Nov-2015].
[13] "SP800-58-final.pdf."Kuhn, D. Richard, Walsh, Thomas J., and Steffen, Fries,
[14] security checklist," *GitHub*, 24-Sep-2015. [Online] 25-Nov-2015].
[15] Cartilla Metodológica Politécnico Grancolombiano.
[16] Estatutos vigentes. Cooperativa Nacional de Ahorro y Crédito Avanza.
[17] Informe Gestión y Mercadeo Cooperativa Nacional de Ahorro y Crédito Avanza.
[18] Leyden, John. 18 de abril de 2003. (ingles) Office workers give away passwords for a cheap pen. The Register
[19] http://www.elmundo.com.ve/Firmas/Moises-Bittan/Informatica-e-Internet--tecnologia-y-redes-
[20] COSTAS SANTOS, Jesús. Seguridad Informática. Madrid: Ra-Ma, 2014. 301 p. ISBN 978-84-9964-313-7.
[21] http://www.definicionabc.com/general/director.php
[22] http://www.definicionabc.com/general/asesor.phphttp://elblogdecharitodr.blogspot.com/2011/04/concurrencia-del-conyuge-la-herencia-y.html
[23] http://www.cronicadelquindio.com/noticia
[24] Trabajo Guía de la Universidad Pontificia Bolivariana, realizado a la Cooperativa Nacional de Ahorro y Crédito Avanza
[25] http://en.wikipedia.org/wiki/Multitier_architecture#Three-tier_architecture

ANEXO 1 RIESGOS

| MATRIZ DE RIESGOS | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| # | Riesgo (si) | Posible resultado (entonces) | Síntoma | Probabilidad (A/M/B) | Impacto (A/M/B) | Prioridad (1 - 9) | Respuesta | Responsable de la acción de respuesta |
| 1 | Cuando la ejecución depende de factores externos al proyecto. | Actividades del proyecto no cumplidas en los plazos establecidos. | Retraso en las actividades programadas. | Media | Alto | 3 | Identificar y dar seguimiento a las actividades específicas prioritarias del cronograma que deben ser realizadas para producir los diferentes productos entregables del proyecto. | Coordinación |
| 2 | Retrasos en la ejecución debido a que los fondos proveidos dependen de otros órganos de la Institución. | Falta de eficiencia en la ejecución del Programa. | Retraso en la recepción de desembolsos. | Alta | Alto | 1 | Realizar motitoreo permanente a las Solicitudes de Desembolso de acuerdo al Cronograma de ejecución. | Coordinación |
| 3 | Capacidad de gestión reducida. | Ineficiencia en la gestión del Proyecto. | Dificultad para sacar adelante las actividades del proyecto. | Media | Bajo | 7 | Contratación de personal con habilidades y experiencia apropiada para trabajar en el proyecto. | Coordinación |
| 4 | Dificultad de lograr el nivel requerido de calidad del producto y/o servicio prestado y del proceso para lograrlo. | Dificultad para lograr que el resultado final alcanzado cumpla con los requerimientos especificados. | Cambios en el alcance del proyecto. | Baja | Medio | 8 | Minimizar los cambios potenciales que se podrían realizar sobre los objetivos del proyecto. | Coordinación |
| 5 | Cuando resulta difícil satisfacer las necesidades requeridas por parte de los beneficiarios. | Incumplimiento de los objetivos del proyecto. | Dificultad del proyecto para satisfacer los requerimientos de los beneficiarios, cantidad de funcionarios capacitados y dotación de equipos infomáticos. | Media | Bajo | 7 | Realizar visitas de apoyo y capacitación en los juzgados de diversas Circunscripciones Judiciales<br>Realizar talleres de capacitación<br>Adquisición y dotación de equipos informáticos. | Coordinación |
| 6 | Decisiones en las prioridades dependen de consenso de factores políticos. | Atraso en las fechas de ejecución. | Retraso en la ejecución de las actividades establecidas en el Cronograma del Proyecto. | Media | Alto | 3 | Exposición de los objetivos y alcances del Programa dirigida a los responsables de la toma de decisiones. | Coordinación |
| 7 | Que no se entregue el equipo en tiempo. | Retraso en el proyecto. | El proveedor no proporciona una respuesta concreta, sólo da largas a la entrega del equipo. Recuerda que no todos los riesgos tienen síntomas. | Media | Alto | 3 | Monitorar la aprobación, estado y revisión del código por parte del personal encargado | Coordinación |
| 8 | Las próximas elecciones presidenciales pueden modificar de manera negativa el compromiso del gobierno con el proyecto. Las elecciones | Cambios al alcance del proyecto. | Declaraciones negativas emitidas por los candidatos a la presidencia respecto al proyecto. | Alta | Medio | 3 | Exposición del alcance, importancia y objetivos del proyecto dirigida a los candidatos a la presidencia. | Junta de Dirección del Proyecto |
| 9 | Las últimas temporadas del estado del tiempo han sido desmedidas; las fuertes lluvias | Retrasos en la ejecucion de las obras. | Pronósticos emitidos por el servicio meteorológico. | Alta | Alto | 1 | Monitorear las condiciones climatológicas a través de pronósticos del tiempo. | Especialista en proyectos |
| 10 | Dificultad en la oferta de profesionales y bienes de acuerdo a los perfiles requeridos. | Llamados a Concursos de consultorias y/o servicios declarados desiertos por falta de presentación de ofertas de profesionales calificados. | Dificultad para llevar adelante el proceso de selección y contratar profesionales/firmas para la ejecución optima de las consultorías y servicios. | Media | Alto | 3 | Elaboración de términos de referencias y/o especificaciones técnicas considerando la oferta existente en el mercado. | Coordinación |

ANEXO 2 IMPACTO

**TABLA DE IMPACTO POR RIESGOS ASOCIADOS**

| Calificación | Consecuencia | Perdidas económicas | Pérdida de reputación | Sanciones | Contagio |
|---|---|---|---|---|---|
| 1 | Insignificante | Se incurre en costos de reproceso (no existe desembolso de dinero). | Algunos funcionarios de la entidad creen que existen debilidades en las políticas y procedimientos de prevención y se toman medidas poco efectivas. | La entidad recibe recomendaciones de mejoramiento de la gestión de riesgos por parte de autoridades competentes. | Se reciben información por canales no oficiales sobre la vinculacion de personajes de la Compañía vinculados al Riesgo |
| 2 | Menor | Se requiere redefinir, reestructurar y reimplantar algunos procesos, actividades o controles; por personal interno. | Un número representativo de funcionarios de la entidad creen que existen debilidades en las políticas y procedimientos de prevención y no se toman medidas. | La entidad recibe llamados de atención sobre la ineficacia de algunos procedimientos de la gestión de riesgos por parte de autoridades competentes. | Se abre una investigacion formal a los directivos de la Compañia por parte de la Fiscalia |
| 3 | Moderado | Se requiere redefinir, reestructurar y reimplantar procesos, actividades o controles fundamentales y revisar algunas actividades ejecutadas; por personal interno. | Varios clientes de la entidad perciben que no se tienen o no se aplican políticas y procedimientos de prevención y la entidad pierde negocios. | Las autoridades competentes exigen a la entidad planes de acción en tiempo limitado con informes de resultados.<br>La entidad recibe algunas denuncias de clientes que le generan costos jurídicos. | La Fiscalia abre juicio contra los directivos de la Compañía al tener pruebas de posible vinculación de capital malicioso |
| 4 | Mayor | Se incurre en gastos al tener que ajustar o reconstruir una parte importante de la estructura del sistema de prevención y rehacer algunas actividades ejecutadas; por personal interno. | Entes de control o entidades representativas con influencia nacional e internacional cuestionan la actuación de la entidad frente a la prevención, generando posibles efectos publicitarios con pérdida de clientes o consecuencias moderadas, administrables por la entidad. | Las autoridades nacionales o internacionales competentes sancionan económicamente a la entidad por incumplimiento en normas de prevención y limitan la operación nacional o internacional de la entidad, y exigen planes de acción en tiempo limitado.<br>La entidad recibe demandas que le generan costos jurídicos y algunas perdidas económicas moderadas. | Las autoridades internacionales anuncian medidas contra la Compañía y esta es incluida en listas de control |
| 5 | Catastrófica | Se incurre en gastos significativos no presupuestados al tener que ajustar o desarrollar una nueva estructura y rehacer las actividades realizadas de un proceso crítico; es necesario contratar personal externo. | Entes de control, entidades representativas con influencia nacional e internacional determinan que la entidad está relacionado con posibles actividades fraudulentas, generando efectos publicitarios de alto impacto, con pérdida de clientes y/o de líneas de fondeo o captación de recursos. | La entidad recibe significativas sanciones económicas por parte de autoridades competentes y/o congelamiento de recursos y cierre de negocios por parte de reguladores internacionales.<br>La entidad recibe demandas que le generan costos jurídicos y perdidas económicas representativas. | La entidad es intervenida y sus activos congelados lo cual la coloca en estado de quiebra |

ANEXO 3 PROBABILIDAD

## MATRIZ DE PROBABILIDAD DE OCURRENCIA DE RIESGOS

| NIVEL | CATEGORIA | DESCRIPCION DE LA FRECUENCIA DE LA PROBABILIDAD |
|---|---|---|
| 5 | Casi Certeza | El Riesgo se materializa de forma diaria |
| 4 | Probable | El Riesgo se materializa una vez al mes |
| 3 | Posible | El Riesgo se materializa una vez cada tres meses |
| 2 | Improbable | El Riesgo se materializa una vez al año |
| 1 | Rara | El Riesgo nunca se ha materializado |