
# ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

## FACULTAD DE INGENIERÍA EN ELECTRICIDAD Y COMPUTACIÓN

## "Diseño y Operación del Primer CERT (Computer Emergency Response Team) en el Ecuador."

**TESINA DE SEMINARIO**

**Previo a la obtención del Título de:**

**INGENIERO EN CIENCIAS COMPUTACIONALES ESPECIALIZACIÓN SISTEMAS DE INFORMACIÓN, INGENIERO EN CIENCIAS COMPUTACIONALES ESPECIALIZACIÓN SISTEMAS MULTIMEDIA E INGENIERO EN ELECTRÓNICA Y TELECOMUNICACIONES**

**Presentado por:**

**Andrés Geovanny Romero Casañas**

**José Jonathan Ronquillo Panchana**

**Galo Fernando Tituana Vera**

**GUAYAQUIL – ECUADOR**

**AÑO: 2011**

# AGRADECIMIENTO

A Dios Todopoderoso por ser mi creador, el motor de mi vida, por no haber dejado que me rinda en ningún momento, llenando mi vida de dicha, bendiciones e iluminándome para salir siempre adelante.

A mis padres (Mario y Silvia) y abuelitos (Rosita y Estuardo) por todo su amor, apoyo y comprensión, guiándome por el buen camino, irradiando siempre energías positivas y contagiarme de sus mayores fortalezas.

A Maricela por estar siempre a mi lado desde que te conocí, tan bella siempre estas y estarás en mi corazón.

A mis maestros por su disposición y ayuda brindada y a mis amigos por estar siempre cuando más los he necesitado.

Andrés Geovanny Romero Casañas

# AGRADECIMIENTO

A Dios por sobre todo, por llenarme de conocimientos y guiarme siempre por el buen camino.

A mis padres por su sacrificio incondicional y desmedido, a mi hermano por su apoyo y ánimo. A todos ellos por su amor incomparable, que me han conducido por caminos de éxitos en mi vida.

A mis compañeros que a pesar de los obstáculos logramos salir adelante.

José Jonathan Ronquillo Panchana

# AGRADECIMIENTO

Agradezco a mis Padres, por el apoyo incondicional, por el sacrificio de mi madre, por darme una mejor educación y ser un buen profesional, eres la persona que influyo mucho para cumplir este objetivo, gracias.

A mi hermano, Freddy que siempre ha estado en las buenas y en las malas.

Agradezco a todos mis maestros, ya que con sus enseñanzas me han ayudado a crecer como profesional y a mis compañeros en general, por brindarme su amistad y su apoyo.

Galo Fernando Tituana Vera

# DEDICATORIA

Este proyecto va dedicado por sobre todo a Dios mi Creador, por todo lo que ha hecho por mí en todos los aspectos y por permitirme conocer personas valiosas y positivas que apoyaron para la culminación de este trabajo. A mis padres y abuelitos (Rosita y Estuardo) por su interminable apoyo en todo momento, por sus consejos, enseñanzas, paciencia, eterno amor y ejemplo de vida. A Maricela y principalmente a mi hija Sol por su infinito amor que constantemente ha sido apoyo y fuerza, por la paciencia y ternura con que resolvemos todo. A mis hermanos Diana, Mario Paúl y Juan Jesús por su compañía y apoyo que me brindan, se que cuento con ellos siempre. A mis familiares y amigos por ofrecer sus fuerzas en todo momento.

Andrés Geovanny Romero Casañas

# DEDICATORIA

Este proyecto va dedicado a Dios, por haber puesto en mi camino a personas de gran corazón que me ayudaron incondicionalmente en el desarrollo de este trabajo. A mis padres a quienes los amo y respeto, quienes han sido un gran ejemplo, motivo de inspiración y orgullo para culminar con éxito este trabajo, a mi hermano que siempre está conmigo en todo momento, mis familiares y amigos que siempre están dispuestos a darme la mano ante toda situación.

José Jonathan Ronquillo Panchana

# DEDICATORIA

Este proyecto va dedicado a mis padres porque han sido pilares fundamentales para poder alcanzar mis metas; Mami, tu rectitud, honestidad y valores me han servido para ser un hombre de bien, eres la motivación para superarme, y ser cada día mejor, y culminar uno de los objetivos más importantes de mi vida. Papi, tu apoyo y valentía me han enseñado a nunca rendirme ante ningún problema, con tus acciones me enseñaste a enfrentar los problemas.

Galo Fernando Tituana Vera

## TRIBUNAL DE SUSTENTACIÓN

Ing. Alfonso Aranda

Profesor del Seminario

Ing. Lenin Freire

Profesor Delegado del Decano

## DECLARACION EXPRESA

"La responsabilidad del contenido de este Trabajo de Grado, nos corresponde exclusivamente, y el patrimonio intelectual de la misma a la ESCUELA SUPERIOR POLITECNICA DEL LITORAL"

Andrés Geovanny Romero Casañas

José Jonathan Ronquillo Panchana

Galo Fernando Tituana Vera

## Resumen

Este proyecto tiene como finalidad el diseño y operación del primer Equipo de Respuestas a Emergencias Informáticas en Ecuador, para esto, en el Capítulo 1 se ha realizado un estudio sobre lo que es un Equipo de Respuestas a Emergencias Informáticas o CERT por su nombre en inglés, se presentan conceptos, definiciones, orígenes y antecedentes para conocer sobre el trabajo que realizan y la historia de estas organizaciones que se encuentran situadas en varios países del mundo y la importancia que tiene su creación en Ecuador.

En el Capítulo 2 se describe la estructura organizacional que se utilizará, para esto, se investiga sobre los requisitos necesarios para la creación de organizaciones en el país y se busca por aquellas que prestan servicios similares para estudiar sus estructuras organizacionales.

La inversión necesaria para llevar a cabo el proyecto se presenta en el Capítulo 3, se describen costos de la infraestructura y el equipo que será utilizado, un análisis financiero completo en el que se estiman los costos y financiamiento del proyecto realizado con la ayuda de tablas y herramientas para el análisis financiero.

El capítulo 4 muestra la planificación para la continuidad de operaciones del proyecto, en base a un análisis FODA se plantean las estrategias como ferias y congresos que permitirán la difusión y continuidad del proyecto.

Finalmente en al Capítulo 5 se muestran detalles sobre la metodología utilizada para la prestación de servicios, políticas a seguir y gráficos de los pasos utilizados en la realización de los servicios principales como los análisis forenses y consultorías.

## Índice General

## Índice de Gráficos



## Índice de Tablas

## Introducción

En la actualidad, la información de una persona u organización es uno de los activos más importantes de esta, por lo cual se toman medidas de seguridad para conservarla. El avance de la tecnología ha sido un gran beneficio, manipular grandes cantidades de información es más sencillo gracias a ello, sin embargo el acceso a esta información también se hace más fácil para personas no autorizadas causando que este activo de gran importancia sea vulnerable ante cualquier amenaza.

Para ayudar a las comunidades, se han creado los equipos de respuestas ante incidentes de seguridad informática, conocidos como CERT o CSCIRT, los cuales ofrecen ayuda a mantenerlas actualizadas con temas de seguridad en general.

En nuestro país los conocimientos sobre la importancia de la seguridad son muy bajos, sin embargo el crecimiento tecnológico es cada vez más alto, por lo que necesitamos que nuestra comunidad este consciente de todas las amenazas que rodean sus activos de información y la importancia que estos tienen.

Se busca viabilizar la formación de uno de estos equipos, ECCERT será el referente ecuatoriano en cuanto a seguridad informática se refiere. Los objetivos de esta organización serán proveer servicios a los diferentes agentes de la sociedad ecuatoriana como son: Universidades, Estado, la empresa privada y personas naturales.

# Capítulo 1

## 1.1 Introducción a la Seguridad Informática

El término seguridad proviene de la palabra securitas del latín, la cual se refiere a la seguridad como la ausencia de riesgo o a la confianza en algo. Sin embargo, al referirnos al área de la Informática podemos entender como seguridad un estado de cualquier tipo de información que nos indica que ese sistema está libre de peligro, daño, riesgo o todo aquello que pueda afectar el buen funcionamiento de nuestro sistema. [1]

Generalmente, la Seguridad Informática consiste en asegurar, garantizar y preservar los recursos y activos de información de una organización. Se entiende como activos de información a todo hardware, software que transfiere, almacena, procesa algo que tiene valor para la organización.

El factor más importante de la protección de activos se basa en la administración de la Seguridad de la Información, de esta manera podemos definir a la Seguridad de la Información como la preservación de la confidencialidad, integridad y disponibilidad de la información, formando una triada como se muestra en el gráfico a continuación.

[1] Manual de Gestión de Incidentes de Seguridad Informática

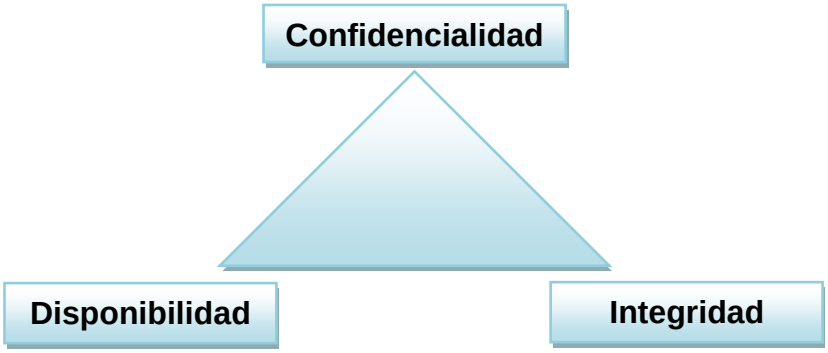


**Gráfico 1 "Triada de Seguridad"**
**Elaborado por: Autores**

### 1.2.1Integridad

La integridad es la propiedad que busca asegurar y salvaguardar la exactitud de los activos de información, manteniendo los mismos libres de modificaciones no autorizadas, es decir que esta información solo puede ser modificada por la persona encargada de gestionarla de manera controlada, garantizando de esta manera que los datos sean lo que se supone que son.

Los cambios o modificaciones autorizados que se realizan sobre los activos de información serán registrados debidamente lo que me constituirá que nadie pueda negar en el futuro alguna operación realizada, asegurando su precisión y confiabilidad.

De esta manera la Integridad de los activos de información la podemos subdividir en dos características de la Seguridad: Autenticidad e Irrefutabilidad de la información.

Un ejemplo de Integridad de un mensaje se obtiene adjuntándole otro conjunto de datos de comprobación de la integridad como la firma digital, ya que este es uno de los pilares fundamentales de la seguridad de la información.

Los usuarios suelen afectar a un sistema o la integridad de sus datos por error (aunque los usuarios internos También pueden cometer actos maliciosos). Por ejemplo, un usuario puede insertar valores incorrectos en una aplicación de procesamiento de datos, es una forma común en que los usuarios pueden accidentalmente ingresar datos corruptos, un error que puede tener efectos duraderos.

### 1.2.2Confidencialidad

La Confidencialidad es la propiedad de prevenir la divulgación de información disponible de nuestros activos a personas, entidades, procesos o sistemas no autorizados, es decir, preservar la confidencialidad de los datos sensibles y asegurar que esta información solo sea inteligible para los autorizados. [2]

Un ejemplo de pérdida de confidencialidad de la información puede ser adoptada de muchas manera. Cuando alguien mira por encima de su hombro, mientras usted tiene información confidencial en pantalla, cuando se publica información privada, cuando una laptop con información sensible sobre una empresa es robada, cuando se divulga información confidencial a través del teléfono, etc. Todos estos casos pueden constituir una violación de confidencialidad.

Los usuarios pueden intencionalmente o accidentalmente divulga la información al no cifrar antes de enviarlo a otra persona, al caer presa de una ingeniería social ataque, al compartir los secretos de una empresa comercial, o al no utilizar un cuidado especial para proteger la confidencialidad información cuando la transformación.

[2] Manual de Gestión de Incidentes de Seguridad Informática

La confidencialidad puede ser proporcionada mediante la encriptación de datos a medida que se almacena y se transmite;  mediante el relleno de tráfico de red, control de acceso estrictos, y clasificación de datos, y por la capacitación del personal sobre el método adecuado.

### 1.2.3Disponibilidad

La Disponibilidad es la propiedad, cualidad o condición de los activos de información de encontrarse a disposición y funcionando correctamente para quienes deben acceder a ellos cuando se requiera o necesite, sean estas personas, procesos o aplicaciones.

Podemos encontrar  Alta Disponibilidad en los Sistemas cuando se encuentran disponibles en todo momento, evitando interrupciones del servicio debido a cortes de energía, fallos de hardware, y actualizaciones del sistema. Garantizar la disponibilidad implica también la prevención de ataque de Denegación de Servicios.

La Disponibilidad es importante en el proceso de seguridad de la información, y también la podemos ver aplicada en varios mecanismos como en la implementación de infraestructura tecnológica, servidores de correo electrónico, de bases de datos de web, etc., mediante el uso de arreglos de discos, equipos en alta disponibilidad a nivel de red, enlaces redundantes, etc. La gama de posibilidades dependerá de lo que queramos proteger y el nivel de servicio que se quiera proporcionar.

La disponibilidad del sistema puede verse afectada por fallas en dispositivos o en el software. Se deben utilizar dispositivos de copias de seguridad y estar disponible para reemplazar rápidamente los sistemas críticos y los empleados deben estar capacitados y en la mano para hacer los ajustes necesarios para adaptar el sistema de nuevo en línea. Las cuestiones ambientales como el calor, la humedad el frío, la electricidad estática, y los contaminantes también pueden afectar la disponibilidad del sistema.

## 1.2 Definición de CERT

CERT (Computer Emergency Response Team) es un Equipo de Respuestas a Emergencias Informáticas. [3] Un CERT es un referente de seguridad informática, lleva a cabo tareas de investigación que tengan como finalidad mejorar la confiabilidad de los sistemas existentes, encontrando amenazas y vulnerabilidades que estos puedan tener, ya sean nuevas tecnologías o versiones de los mismos; es un apoyo a su comunidad al dar seguimiento a posibles incidentes informáticos reportados por esta, y enseña a la misma a cómo prevenir futuros incidentes, educándola y manteniéndola siempre informada. Está conformado por un grupo de personas que son responsables de identificar y brindar soluciones a las diferentes amenazas y vulnerabilidades que se presentan en los sistemas de información.

Los objetivos principales de un CERT son:

- Minimizar los daños ante cualquier ataque o amenaza.
- Proveer asistencia rápida y efectiva.
- Ayudar a la prevención de futuros incidentes.

[3] www.cert.org

A nivel mundial los CERT son conocidos con diferentes acrónimos tales como:

- **CSIRT:** Equipo de Respuesta a Incidentes de Seguridad Informática
- **CIRC:** Capacidad de Respuesta a Incidentes Informáticos
- **CIRT:** Equipo de Respuesta a Incidentes Informáticos
- **IRC:** Centro de Respuesta a Incidentes
- **IRT:** Equipo de Respuesta a Incidentes
- **SIRT:** Equipo de Respuesta a Incidentes de Seguridad

### 1.3.1 Origen y Antecedentes

El 22 de noviembre de 1988, aparece “Morris Worm”, el primer gusano de internet creado por Robbert Tapam Morris, el programa en mención fue lanzado desde un ordenador, su funcionamiento consistía en generar copias de sí mismo y auto enviarse a otros ordenadores, con un estimado de 60000 computadores que comprendía toda la red de internet a esa fecha, le bastó solo un par de horas para infectar aproximadamente el 10% de todas las máquinas; este incidente afectó a equipos de la Nasa, el Gobierno y Fuerza Aérea, destruyendo importante información y ocasionando millonarias pérdidas. A raíz de los acontecimientos, DARPA (Defense Advanced Research Projects Agency) agencia del Departamento de Defensa de los Estados Unidos responsable del desarrollo de nuevas tecnologías para uso militar, se encarga de crear el primer Equipo de Respuestas a Emergencias Informáticas en el Instituto de Ingeniería de Software de la Universidad Carnegie Mellon de los Estados Unidos de América, convirtiéndose luego en CERT/CC (Computer Emergency Response Team Coordination Center) es ahora el centro de coordinación de todos los CERTs en diferentes países.

### 1.3.2 Alcance

Un CERT debe estar conformado por un equipo especializado en temas seguridad informática, debe convertirse en un referente en la comunidad a la que brinda sus servicios, ofrecerle información para elevar la conciencia colectiva sobre temas de seguridad informática y llevar a cabo tareas de investigación que tengan como finalidad mejorar la seguridad de los sistemas existentes. Dar respuesta a incidentes de seguridad en sistemas de información que reporten los diversos organismos a los que les brinda servicio es uno de los beneficios que se obtiene de esta organización.

## 1.3 CERT en el exterior

A partir de la creación del primer CERT y los incidentes dados para la creación del mismo, las comunidades se alertan y se incentivan a poseer centros de respuestas ante incidentes de seguridad informática cerca de ellos, para así tener respuestas más rápidas y relacionadas con el ambiente que los rodea; siendo CERT/CC el centro de coordinación de todos. Actualmente hay cerca de 200 organizaciones reconocidas que prestan servicios a sus respectivas comunidades. En Latinoamérica tenemos CERTS en Argentina, Brasil, Chile y Uruguay, algunos de estos los podemos ver en la tabla 1, de los CERT en Latinoamérica.

| PAIS | NOMBRE | DIRECCIÓN WEB |
|---|---|---|
| Argentina | Computer Emergency Response Team of the Argentine Public Administration | http://www.arcert.gov.ar |
| Brasil | Computer Emergency Response Team Brazil | http://www.cert.br/ |
| Chile | Chilean Computer Emergency Response Team | http://www.clcert.cl/ |
| Uruguay | ANTEL's Computer and Telecommunications Security Incident Response Centre | http://www.csirt-antel.com.uy |

**Tabla 1. CERT en Latinoamérica**
**Elaborada por: Autores**

Los primeros CERT tuvieron su origen en el ámbito universitario en 1992, cada uno de los equipos existentes cumple con tres objetivos básicos:

- Informar sobre la importancia de la Seguridad.
- Prevención de Incidentes.
- Respuesta a incidentes que ocurran en la comunidad.

### 1.4.1Evolución

Debido a la gran importancia de los activos de información de las organizaciones y gobiernos, estos impulsan a la creación de CERT para que sean un apoyo más rápido y relacionado con el entorno de cada comunidad; sin embargo se trabaja en conjunto para poder ofrecer mejores servicios, el centro de coordinación ofrece ayuda para creación de nuevos CERTs y el apoyo en conjunto por medio de FIRST (Forum of Incident Responses and Security Teams) donde se intercambia información sobre nuevas amenazas que aparecen en las diferentes comunidades.

La iniciativa en cuanto a creación de un CERT surge ante la necesidad de incrementar la seguridad de las redes y sistemas de información con la finalidad de dar solución a las vulnerabilidades y proteger a los usuarios, y a la seguridad nacional de las constantes amenazas que se pueden ocasiona, en el gráfico a continuación podemos ver la ubicación de algunos CERT en el mundo.

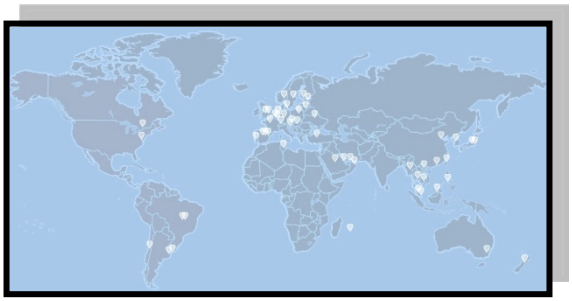

**Gráfico 2. CERT en el mundo**
**Fuente: http://www.cert.org/cert/map_open.html**[4]

### 1.4.2FIRST

Foro de Respuesta a Incidentes y Equipos de Seguridad es una organización que agrupa a todos los CERT del mundo, su sede se encuentra en los Estados Unidos, fue fundado en 1990. [5]

El objetivo de esta organización es fomentar la cooperación y la coordinación en la prevención de incidentes, promoviendo el intercambio de información y la colaboración entre todos los equipos a nivel mundial.
Algunos de los beneficios de pertenecer al FIRST son:

[4] www.cert.org

[5] www.first.org

- Disponibilidad de comunicación a través de foros entre los miembros de los diferentes CERT.
- Participación en las conferencias sobre Manejo de Incidentes de Seguridad.
- Para los equipos que pertenecen al FIRST se establecen reuniones cada dos años, con objetivos de compartir información.
- Todos los equipos que pertenecen al FIRST reciben apoyo, se le brinda colaboración e intercambio de ideas.

Para ser parte del FIRST uno de los requisitos que se debe cumplir es el proceso de auditoría, la misma que es realizada por un equipo que sea parte del FIRST, los aspectos que se evalúan son: estructura del equipo, procedimientos, conocimientos del personal en cuanto a metodología y procesos utilizados, entre otros aspectos. El FIRST cuenta en la actualidad con más de 180 miembros distribuidos en países de Europa, América, Asia y Oceanía, cada uno de los CERT que conforman este foro son de tipo gubernamental, educativo, empresarial y financiero.

## 1.4 CERT en Ecuador

Actualmente en nuestro medio no existe un centro donde converja un equipo de profesionales del área de la seguridad informática (CERT). No se cuenta con un centro donde se puedan ubicar estadísticas referentes a la seguridad informática a nivel nacional que sean de gran importancia para realizar estudios o investigaciones para implementación de nuevas tecnologías dentro de las organizaciones, así mismo reportes de incidentes informáticos que pueden ser de gran ayuda con respecto a la resolución de estos problemas en lo que se refiere a tiempos.

Dentro de los planes de CEDIA (Consorcio Ecuatoriano para el Desarrollo de Internet Avanzado) está por crearse el ECCERT, el cual está en proceso, que sería el referente para nuestro país en cuanto a información sobre temas de seguridad de información.

También hay grupos de profesionales que brindan servicios de auditorías e informan de alertas y vulnerabilidades, pero no son considerados centros o fuentes de información.

En las universidades se han creado grupos de investigación, de análisis que buscan ayudar a concientizar e informar sobre temas de seguridad pero son muy pocos.

En fin hay varias fuentes de información y se están impulsando varios proyectos que contribuyan a mejorar los niveles de seguridad de la comunidad, pero que hasta el momento no tenemos un centro que reúna toda esta información y realice un análisis verdadero de la seguridad informática en Ecuador.

### 1.5.1 Fuentes de información.

Toda persona u organización es capaz de proveer datos y puede ser considerada una fuente de información. Toda fuente de información se relaciona con su formato. Al comenzar la búsqueda de una fuente de información es fundamental poder identificar la potencialidad de la fuente y reconocer sus características. De esto resultara la identificación del propósito que guía la fuente. Distinguir entre fuentes primarias y secundarias simplificara la elección del tema si se trata de una investigación y aumentara las posibilidades de extraer la información más pertinente sobre el tema elegido.

Como políticas de seguridad de información debemos buscar fuentes de información confiables, en ese contexto es importante de donde proviene la información, cual es el medio, o quien reporto algún incidente o vulnerabilidad.

Es por eso que CERT, tendrá que definir cuáles serán sus fuentes de información sobre las cuales podrá basar sus informes. Entre ellas podemos citar:

- Universidades
- Organismos de Control
- Foros de discusión
- Empresas desarrolladoras de Software
- Empresas de Servicios, etc.

### 1.5.2 Conocimientos sobre seguridad de la información en Ecuador

Es crítico para las Organizaciones poder identificar amenazas que afectan la disponibilidad, integridad y confidencialidad de los datos y adoptar recomendaciones que permitan prevenir, detectar y protegerse de ellas. La diversidad de los sistemas de información que requieren las organizaciones actuales, sumado a la globalización a la que se enfrentan al conectar esos sistemas al mundo de Internet, genera un gran número de incertidumbres en lo referente a la Seguridad de la Información, para ello se debe aportar soluciones integrales de seguridad que abarcan desde el diagnóstico de la situación actual, hasta la implementación y puesta en marcha de las mismas en todos los niveles de la organización, incluyendo el análisis y la definición de los elementos de seguridad que deben ser implantados a nivel técnico.

La información que está expuesta a los usuarios puede ser las finanzas de la empresa, números de tarjetas de crédito, planes estratégicos, información relacionada con la investigación y el desarrollo de nuevos productos o servicios, etc.

Ecuador no está al margen de esta problemática, hoy en día tenemos un alto desarrollo de tecnología, sistemas en línea, pagos en línea, tarjetas de crédito, que ha originado que las empresas se pongan a trabajar en serio en seguridad informática, lo que hace unos años atrás nadie lo veía importante. Aunque falta mucho por desarrollar en este ámbito de la tecnología podemos decir que estamos empezando, ya que actualmente se conoce de auditorías que hacen sus empresas para saber que tan segura esta su información. Las empresas contratan sistemas de protección antivirus, firewalls, pero no tienen políticas de seguridad que es lo más importante, es por eso que hoy en día ya tenemos auditoras que hacen auditorias de seguridad de la información que básicamente es realizar y poner en marcha un buen plan de políticas de seguridad.

### 1.5.3 Importancia de un CERT en Ecuador

En los últimos años se ha registrado el nacimiento de una tendencia sobre la implementación de comunicaciones seguras dentro de una misma organización, es de gran importancia esta comunicación la cual debe estar siempre disponible y confidencial por lo que la seguridad tiene un papel muy importante dentro de ella.

Con el crecimiento de los sistemas de software, día a día las empresas se encuentran en constante búsqueda de disminuir los riesgos de las vulnerabilidades de la información, está se encuentra a disposición de los usuarios, y depende de ellos darle un buen uso y mantener las políticas de las organizaciones, sin embargo se pueden dar situaciones no intencionales por las que los sistemas deben estar con la capacidad de evitar estos inconvenientes.

Al tener un desarrollo tecnológico en el país es importante, saber cuidar la información, debido al poco conocimiento sobre la importancia de la seguridad de la información en nuestro país, es necesario capacitar a las personas y que nuestra comunidad este consciente de todas las amenazas que rodean sus activos de información y la importancia que estos tienen para ellos y sus organizaciones.

Actualmente en nuestro medio no existe un centro donde converja un equipo de profesionales del área de la seguridad informática (CERT), un referente al cual poder acudir por ayuda o documentos que puedan ser utilizados para la resolución de problemas en un tiempo mínimo.

## 1.5 Objetivo general

Se busca formar un CERT-EC que se convertirá en el referente ecuatoriano en cuanto a seguridad informática se refiere. Los objetivos de esta organización es proveer servicios a los diferentes agentes de la sociedad ecuatoriana como son:

- Universidades
- Estado
- Empresa privada
- Personas naturales.

## 1.6 Objetivos específicos

Entre los objetivos específicos de un CERT tenemos los siguientes:

- Informar sobre vulnerabilidades de seguridad y amenazas.
- Divulgar y poner a disposición de la comunidad información que permita prevenir resolver incidentes de seguridad.
- Realizar investigaciones relacionadas con la seguridad informática.
- Educar a la comunidad en general sobre temas de seguridad.
- Manejar estadísticas.

# Capítulo 2

## 2.1 Estudio organizacional

### 2.1.1Logo de la empresa

Nombre de la empresa que no exista dentro de las empresas ya constituidas: ECCERT (Ecuador Computer Emergency Response Team)


**Gráfico 3. Logotipo de ECCERT**
**Elaborado por: Autores**

## 2.2 Control organizacional

En el control organizacional ubicamos lo que será la misión y visión, las cuales fueron debidamente discutidas por los miembros del equipo de trabajo.

### 2.2.1Misión

Informar a la comunidad sobre técnicas de defensa y prevención ante las nuevas amenazas y vulnerabilidades de los sistemas, trabajando en conjunto con personas especializadas y de vastos conocimientos en tecnologías de seguridad informática, además, ayudaremos a garantizar la protección de sus activos de información.

### 2.2.2Visión

Ser el referente ecuatoriano y líder en servicios que permitan prevenir y resolver incidentes de seguridad informática a nivel Nacional.

## 2.3 Organigrama

Organigrama diseñado para cubrir los puestos necesarios para la Dirección de ECCERT.

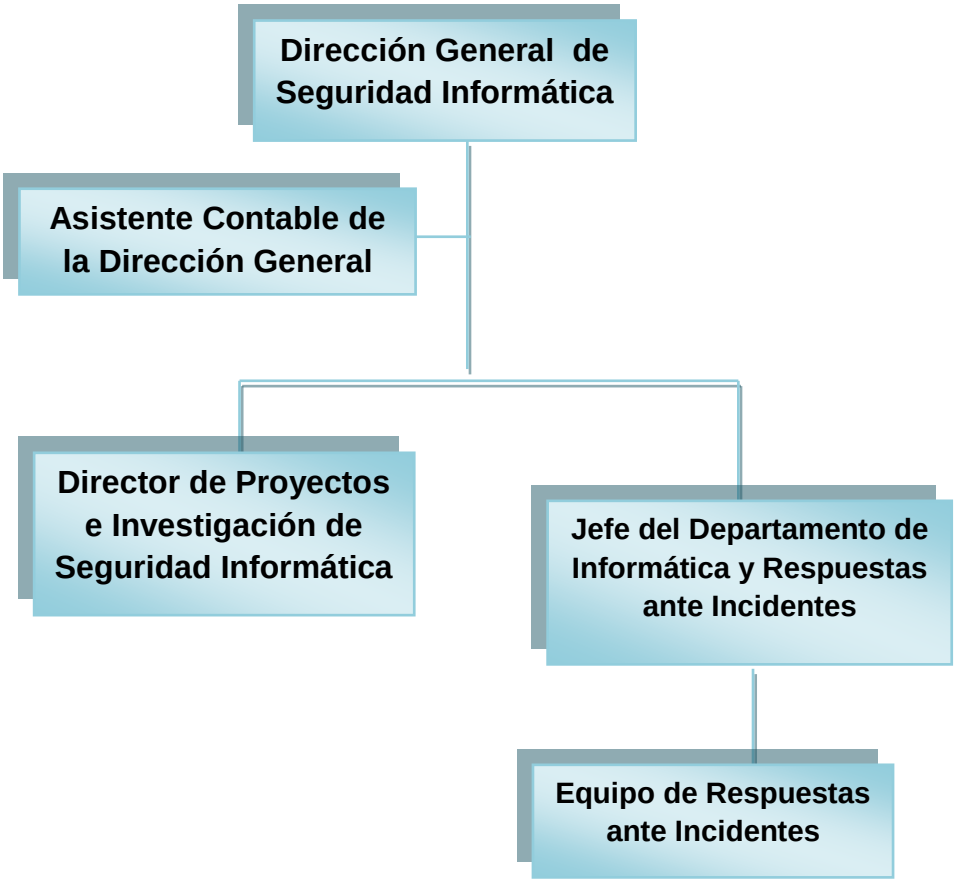


**Gráfico 4. Organigrama**
**Elaborado por: Autores**

## 2.4 Descripción de Personal

Esta sección incluye a todas las personas necesarias para que el Ecuador Computer Emergency Response Team funcione de la mejor manera en su comienzo. Las variables evaluadas para este tema son costo unitario de cada persona, el desempeño que se le asignaría, la situación del campo de la seguridad informática en Ecuador, las leyes y regulaciones existentes.

### 2.4.1Balance del Personal.

A continuación se muestran los cargos del organigrama con el número de personas necesarias para cubrir los puestos.

| DESCRIPCION DEL PERSONAL | CANTIDAD |
|---|---|
| Director General de Seguridad Informática | 1 |
| Director de Proyectos e Investigación de Seguridad Informática | 1 |
| Jefe del Departamento de Informática Y Respuesta ante Incidentes | 1 |
| Asistente Contable de la Dirección General | 1 |
| Equipo de Respuestas ante Incidentes | 4 |

**Tabla 2. Descripción de Personal**
**Elaborada por: Autores**

### 2.4.2Habilidades Personales

- Tener capacidad de comunicación.
- Relaciones humanas.
- Espíritu de Equipo.
- Innovadores, analíticos e íntegros, son un equipo que trabaja dando soluciones a problemas.
- Capaces de tomar decisiones rápidas ante ataques y situaciones de emergencias de manera que nada quede sin dar respuesta.
- Capacidad de seguir políticas y procedimientos.

### 2.4.3 Habilidades técnicas

- Conocimientos de seguridad de la información.
- Conocimiento de los sistemas operativos que utilizan en la organización.
- Realizar la supervisión constante de los sistemas para evitar y localizar infracciones en las seguridades.
- Las labores que se realizan deberán servir para enviar informes de los incidentes encontrados.
- Conocimiento de aplicaciones y protocolos de internet.
- Realizar auditorías a los sistemas tanto a nivel de software y hardware.
- Brindar servicios de capacitación.

### 2.4.4 Tareas Específicas

A continuación se detalla las tareas específicas de cada miembro del equipo:

#### 2.4. 4.1 Director General y Capacitación.

Estará orientado a la preparación de profesionistas con habilidades de comunicación multicultural, de liderazgo en el Área de Sistemas, deberá tener vastos conocimientos de seguridad de informática, protección de activos de información y sistemas en general en las diversas áreas donde este se presente.

Desarrollará programas de capacitación, información y educación sobre vulnerabilidades, amenazas y temas de seguridad en general, implementara estrategias para la continuidad de operaciones, así como de administrar las operaciones del ECCERT en el servicio a la comunidad en general; asesorará a los diferentes agentes interesados de la sociedad ecuatoriana, planificara y coordinara los objetivos para el cumplimiento de los diferentes servicios a brindar.

### 2.4. 4.2 Director de Proyectos e Investigación.

Profesional capacitado para analizar la implementación y desarrollo de políticas de seguridad en función de la optimización de sus diferentes niveles e investigar las dificultades de ingreso de los servicios de ECCERT en las diferentes áreas de la sociedad ecuatoriana, con una visión integradora para la resolución de los problemas inherentes a la seguridad informática y con capacidad de innovación ante la realidad cambiante del campo.

Realizará trabajos de investigación ante nuevas y posibles vulnerabilidades y amenazas relacionado con la seguridad informática para el servicio de los diferentes agentes de la sociedad ecuatoriana interesados.

Identificará, evaluara y aplicara las opciones de financiamientos disponibles para ECCERT.

### 2.4. 4.3 Jefe del Departamento de Informática Y Respuesta ante Incidentes.

Profesional encargado de mantener actualizado la base de alertas, vulnerabilidades y amenazas del sistema, capacitará a los Usuarios del Sistema para el correcto uso de la herramienta y a los nuevos integrantes del Equipo de Respuestas ante Incidentes que se agreguen dependiendo de los diferentes servicios que se vallan creando para la sociedad ecuatoriana.

Administrará la base de datos. Además, deberá tener alta capacidad de análisis y planeación, empuje, enfocado a resultados, capacidad de toma de decisión, excelente comunicación a todos los niveles, flexibilidad y alta capacidad. Será el puente y encargado del contacto permanente entre el Equipo y los Directivos de ECCERT.

Manejara las Estadísticas y definirá la inversión, infraestructura y personal para el comienzo de las operaciones, en base a todos los servicios que se prestarán.

### 2.4. 4.4 Asistente de Dirección General / Contable.

Encargado de dar soporte al Director General. Además, de dar seguimiento a la nómina de trabajadores, de afiliaciones al Seguro social y demás actividades de recursos humanos dando soporte al Contador.

Será el encargado de atender a los clientes y dar información acerca de ECCERT, planificar, coordinar, implementar, ejecutar y controlar las actividades inherentes de aspectos económicos y financieros. Por otro lado, será el encargado de las nóminas de trabajadores, contratos y todo lo relacionado a recursos humanos. Encargada de realizar estados de resultados, balances generales y asientos de transacciones.

### 2.4. 4.5 Equipo de Respuestas ante Incidentes.

El Profesional en Seguridad de Informática estará preparado, en los aspectos técnico-científicos de Tecnologías de la Información, elaborara criterios que posibiliten el desarrollo de nuevas y posibles formas de protección antes los diferentes y variados tipos de ataques que se existan y que llegasen a crearse.

Deberá conocer, además, la operatoria de la Seguridad Informática a nivel Internacional, así como la normativa que regula la Seguridad de Activos de Información en todos sus aspectos.

## 2.5 Descripción de servicios

ECCERT contará con una base de datos de los agentes interesados en los servicios que provee, logrando así una mejor comunicación entre ambas partes y logrando obtener el mayor beneficio posible a los servicios disponibles, entre los cuales destacamos:

- Análisis forenses
- Escaneo de vulnerabilidades
- Seguimiento de incidentes
- Consultoría de seguridad
- Capacitaciones

Con los servicios se buscará brindar respuesta, a cualquier solicitud de asistencia y cualquier amenaza o ataque que hayan ocurrido en los sistemas, los mismos pueden ser ocasionados por terceras personas o de manera accidental por el personal de una organización; se realizaran reportes de las tareas llevadas a cabo y se planificaran estrategias posteriores al ataque, siendo estos de respuestas ante el incidente y de prevención de futuros ataques.

### 2.5.1 Análisis Forenses.

El análisis forense consiste en la recolección de evidencias digitales de computador o red, datos visibles, desconocidos y ocultos, y utilizar dicha información digital tanto para procedimientos legales, administrativos como para mejorar la seguridad de una organización.

El análisis forense se utiliza en los casos donde es necesario analizar las causas que generan un delito informático o un incidente de seguridad, con el objetivo de averiguar cómo fue realizado el crimen, datos del suceso, reconstrucción cronológica de tiempo, identificación de técnicas del ataque, los recursos comprometidos, las personas implicadas, los daños ocasionados y, finalmente, identificar los actores protagónicos del incidente.

El poder que tienen las herramientas de la informática forense para obtener información almacenada en medios digitales es sorprendente, por lo que gracias a esto nada queda oculto en los dispositivos modernos. Incluso, la información que ha sido alterada, eliminada o modificada, mediante técnicas de la informática forense, hoy en día se plantea la viabilidad de recuperar la información y reconstruir las evidencias digitales necesarias para identificar un ataque informático o un incidente de seguridad.

La recolección de la evidencia forense incluye, realizar una copia bit a bit del disco duro de los sistemas afectados, la búsqueda de cambios en el sistema, como la instalación de nuevos programas, archivos, etc.

Algunos pasos empleados para el levantamiento de evidencia forense son:

### 2.5. 1.1 En equipos

- Realizar una sesión fotográfica de la sala antes de comenzar la tarea. Las fotos deben de tener sobreimpresa digitalmente la fecha y hora.
- Fotografiar el ordenador de frente con los cables y por detrás, así como dispositivos conectados tal y como se encuentran.
- No se debe utilizar el ordenador.
- Realizar un diagrama si es una red y crear etiquetas de los dispositivos conectados.
- Mantener todos los medios de comunicación, incluido el equipo, lejos de los elementos potencialmente dañinos.
- Recopilar manuales de instrucciones, documentación y posibles notas que hubiera en el lugar.
- Documentar todos los pasos implicados en la adquisición del ordenador y sus componentes.

### 2.5. 1.2 En dispositivos móviles

- Con una PDA o teléfonos móviles, si el dispositivo está encendido, no se debe apagar.
- Etiquetar y recoger todos los cables (incluyendo la fuente de alimentación).
- Intentar que el dispositivo mantenga la batería en la medida de lo posible
- Etiquetar el almacenamiento adicional de los dispositivos.
- Documentar todos los pasos implicados en la adquisición del móvil y sus componentes.

### 2.5.2Escaneo de vulnerabilidades

Una vulnerabilidad en seguridad informática hace referencia a una debilidad en un sistema permitiendo a un atacante violar la confidencialidad, integridad, disponibilidad, control de acceso y consistencia del sistema o de sus datos y aplicaciones.

Las vulnerabilidades son el resultado de bugs o de fallos en el diseño del sistema. Aunque, en un sentido más amplio, también pueden ser el resultado de las propias limitaciones tecnológicas, porque, en principio, no existe sistema 100% seguro. Por lo tanto existen vulnerabilidades teóricas y vulnerabilidades reales.

Las vulnerabilidades en las aplicaciones suelen corregirse con parches, o con cambios de versión. En tanto algunas otras requieren un cambio físico en un sistema informático.

Las vulnerabilidades se descubren muy seguidas en grandes sistemas, y el hecho de que se publiquen rápidamente por todo internet (mucho antes de que exista una solución al problema), es motivo de debate. Mientras más conocida se haga una vulnerabilidad, más probabilidades de que existan intrusos informáticos que quieran aprovecharse de ellas.

Algunas vulnerabilidades típicas suelen ser:

- Desbordes de pila y otros buffers.
- Errores en la validación de entradas como: inyección SQL, bug en el formato de cadenas, etc.
- Secuestro de sesiones.
- Ejecución de código remoto.

Para organizaciones muy grandes, es importante realizar el escaneo de vulnerabilidades como parte del análisis de seguridad regular con una mayor cantidad de escaneos, mucho más frecuente (un ejemplo podría ser realizar el escaneo de vulnerabilidades, de forma exhaustiva, cada 4 meses, es decir unas 3 veces al año)

### 2.5. 2.1 Tipos de escáner

- **Escáner de Red:** escáner de uso general usado para encontrar vulnerabilidades potenciales en la red de la empresa.
- **Escáner de Puerto:** software diseñado para buscar en una red los puertos abiertos que podrían ser usados por los atacantes como puntos de entrada.

- **Escáner para la Seguridad de aplicaciones web:** Permite a los negocios realizar evaluaciones de riesgo para identificar las vulnerabilidad en aplicaciones web y así evitar ataques. Este tipo de escáneres deberían ser utilizados también por el departamento de desarrollo (programación) de una aplicación web, ayudando así a encontrar todos los bugs que puedan generarse durante la creación de la aplicación, antes de poner la aplicación a un entorno de producción.
- **Escáner de Base de datos:** permite encontrar puntos débiles en bases de datos, protegiendo así el activo más importante de una empresa.

### 2.5. 2.2 Escáneres

Estos son ejemplos de algunas herramientas que actualmente son muy utilizadas por los administradores de redes y encargados de seguridad. Algunos son de pago y otros son gratuitos.

- **Acunetix Web Vulnerability Scanner:** Este software incluye un escáner de seguridad Web, una consola para el análisis de informes y una base de datos para gestionar todas las plataformas principales del servidor web.
- **GFI LANguard Network Security scanner:** Esta solución incluye la exploración de vulnerabilidades de red y también sirve para realizar auditorías informáticas de seguridad.
- **Teneble Nessus 3:** Compatible con varios tipos de Unix, este producto ejecuta más de 900 comprobaciones de seguridad y sugiere soluciones para los problemas encontrados (open source)
- **Nmap:** Es un escáner de puerto utilizado para la exploración de la red o la revisión de seguridad (open source)

- **Retina Network Security Scanner:** Su distribuidor es la firma eEye Digital Security Inc. Afirman que su escáner de vulnerabilidad descubre tanto las vulnerabilidades conocidas como las vulnerabilidades denominadas “zero days”. El producto también proporciona la opción de realizar análisis de riesgos basados en la seguridad ayudando a la empresa a ejecutar y poner las mejores prácticas, ayuda a reforzar las políticas y a manejar las auditorias.
- **SAINT Network Vulnerability Scanner:** Este escáner de vulnerabilidad de red está integrado con un sistema para realizar pruebas de penetración (pentest) permitiendo así al usuario a explotar las vulnerabilidades encontradas.
- **WATCHFIRE RATIONAL APPSCAN:** Escáner de IBM utilizado para aplicaciones web.
- **ISS Internet Scanner:** Escáner de vulnerabilidades de red de la compañía IBM.

### 2.5.3 Seguimiento de incidentes

Consiste en la evaluación de toda la información que se ha recolectado acerca de un incidente, con esta información se realiza una evaluación de los daños que el incidente ha causado para comenzar a restaurarlos y determinar estrategias de respuesta para mitigar en el menor tiempo posible los efectos de este ataque.

Se realiza una revisión minuciosa de los sistemas afectados, y se efectúa un seguimiento para saber la hora en que el intruso tuvo acceso al sistema, cómo ingreso al sistema, que redes utilizó para lograr el acceso, etc.

### 2.5.4Consultoría de seguridad

Los miembros del equipo se encargan de brindar asesoramiento a los miembros de la organización o comunidad a la que van dirigidos los servicios en el campo de la seguridad de la información, la elaboración de políticas y mejores prácticas de seguridad, asesoramiento en la instalación de aplicaciones, etc.

#### 2.5.4.1 Beneficios de una consultoría

- Aportan conocimientos y técnicas especiales.
- Se puede recurrir a consultores cuando una organización carece de las personas capaces de abordar un problema con la misma posibilidad de éxito. Para ello se requieren a menudo métodos y técnicas especiales en que el consultor es un experto.
- Aportan una intensa ayuda profesional con carácter temporal.
- En otras situaciones, la organización puede disponer de los conocimientos técnicos requeridos, pero los directores de alto nivel o los especialistas del personal tienen que concentrarse en un trabajo a fondo y constante sobre un problema o proyecto principal. El funcionamiento cotidiano de la organización les deja escaso tiempo y no es fácil ocuparse simultáneamente de cuestiones prácticas y conceptuales. Los consultores no sólo aportan el tiempo, sino que dejan la organización una vez que han terminado su contenido.
- Aportan una opinión externa imparcial.
- Incluso los mejores elementos de una organización puede estar demasiado influido por su participación personal y por las tradiciones y valores existentes para captar un problema en su verdadera dimensión y pensar en soluciones factibles. En cambio, debido a su independencia de la organización del cliente y a que

no está influido por los hábitos de la organización, un consultor puede aportar un nuevo punto de vista y ser imparcial en situaciones donde ningún miembro de la organización los sería.

- Justifican las decisiones de la dirección.
- En ocasiones se pide a los consultores que realicen tareas y presenten informes con el fin de que un director pueda justificar su decisión refiriéndose a las recomendaciones de los consultores.

### 2.5.5 Capacitaciones

Servicio que tiene como fin elevar cultura de la comunidad, orientar a las personas en temas de seguridad informática en general, labor realizada a través de talleres o seminarios en los cuales se provea la información necesaria del tema a tratar, llevada a cabo por uno o más integrantes expertos y con experiencia en casos reales.

### 2.5.6 Consultorías y Capacitaciones

La consultoría es inseparable de la capacitación. En todo en enfoque de consultoría eficaz el componente de aprendizaje es muy importante. El cliente aprende del consultor, pero el consultor aprende también del cliente y esto lo ayuda a ajustar su enfoque en las fases siguientes de su cometido y acumular experiencia para futuros contratos.

## 2.6 Sistema de Alertas de Seguridad

Las alertas de seguridad son una herramienta para mejorar ciertos procedimientos en una organización, teniendo como principal objetivo la prevención de posibles incidentes o la resolución de problemas en el menor tiempo posible.

Las alertas consisten en recibir y entregar información sobre nuevas vulnerabilidades, alertas de intrusión, código malicioso y ataques de intrusos, dados por virus, gusanos, troyanos o robo de contraseñas. La información recibida también incluye las acciones que se recomiendan para la resolución de problemas en el menor tiempo posible.

Esta información puede ser generada por el equipo, especialmente el personal de investigación, y también puede ser recibida por parte de organizaciones, o personas particulares. Estos comunicados siguen siempre el mismo esquema:

- Recopilación de información
- Evaluación de la información sobre la pertinencia y la fuente
- Evaluación del riesgo basada en la información recopilada
- Distribución de la información

### 2.6.1 Recopilación de la Información

Esta labor realizada por el personal de investigación consiste en obtener información de los últimos avances en lo que se refiere a nuevas formas de ataque, el cómo prevenirlas y evitarlas, mantenerse en contacto con otros CERT que tienen experiencia para resolver incidentes, la utilización de listas de correo, sitios web de seguridad y artículos actuales en el campo de la tecnología.

### 2.6.2Evaluación de la información sobre la pertinencia y la fuente

La fuente de la información entrante sobre vulnerabilidad siempre ha de ser identificada, y antes de transmitir la información al grupo atendido se ha de determinar si la fuente es de confianza. En caso contrario, se podrían generar alertas innecesarias que provocarían molestias gratuitas en los procesos empresariales y al final perjudicarían a la reputación de ECCERT.

### 2.6.3Evaluación del riesgo basada en la información recopilada

Existen diversos métodos para determinar el riesgo y las consecuencias de una posible vulnerabilidad. Algunos de los factores más importantes que cabe tener en cuenta son:

- ¿Es bien conocida la vulnerabilidad?
- ¿Está muy extendida?
- ¿Es fácil de explotar?

Todas estas preguntas ayudan a formarse una idea adecuada de la gravedad de la vulnerabilidad.

Para calcular el riesgo se puede recurrir a una fórmula muy sencilla: Impacto = Riesgo x Daños Potenciales.

Tras contestar a estas preguntas se puede añadir una clasificación global al aviso, informando de riesgos y daños potenciales. Se suelen usar términos simples como BAJO, MEDIO y ALTO.

### 2.6.4Distribución de la información

Cada CERT puede elegir entre diferentes métodos de distribución, según las preferencias del grupo de clientes atendido y su propia estrategia de comunicación:

- Sitio web
- Correo electrónico
- Informes
- Archivo e investigación.

Los avisos de seguridad distribuidos por un CERT deben seguir siempre la misma estructura, para mejorar la legibilidad y permitir que el lector encuentre rápidamente la información pertinente. La difusión de la información proporciona toda la información útil para mejorar la seguridad.

#### 2.6.4.1 Sitio Web

ECCERT contara con su propio sitio web, por lo que será el medio principal para distribuir su información, ya sean noticias sobre liberaciones o nuevas amenazas encontradas.

#### 2.6.4.2 Correo electrónico

Además de contar con la información en el sitio web, ECCERT distribuirá mediante correo electrónico información específica referente a las nuevas amenazas o vulnerabilidades, noticias sobre liberación de parches o versiones de los sistemas utilizados por las organizaciones registradas en la base de datos de ECERT.

## 2.7 Información para la comunidad

Por tratarse de un referente en cuanto a seguridad informática se refiere, ECCERT contara con la mayor cantidad de información relacionada a temas de seguridad dentro de la comunidad, la que será de gran utilidad para manejar amenazas similares que se puedan presentar y para realizar estudios.

### 2.7.1 Investigaciones

ECCERT estará siempre investigando los últimos avances en lo que se refiere a nuevas formas de ataque, el cómo prevenirlas y evitarlas en un futuro, existirá constante comunicación con otros CERT que tienen experiencia para resolver incidentes, los cuales utilizan otros tipos de información como listas de correo, sitios web de seguridad y artículos actuales en el campo de la tecnología.

### 2.7.2 Control de estadísticas

ECCERT registrará cada suceso e incidente que registre o llegue como información compartida, información recibida de incidentes y vulnerabilidades encontrados, de esta forma se podrá llevar un control estadístico que luego sea útil a la comunidad, proporcionando valores sobre todos los abusos y vulnerabilidades reportadas ya sean estas semanales, mensuales o anuales.

## 2.8 Agentes interesados

Los agentes interesados son todas aquellas organizaciones de la comunidad que se encuentran relacionadas con los servicios de ECCERT, entre las que podemos mencionar:

- Universidades
- Estado
- Empresa privada
- Personas naturales

### 2.8.1 Universidades.

Al ser la Universidad una fuente de conocimiento, el sector académico siempre estará interesado en la protección de sus activos de información; por lo general las instituciones más reconocidas a nivel nacional cuentan con sus propios equipos de defensa informáticos sean estos mecánicos o humanos, razón por la cual ECCERT trabajara con las Universidades de manera colaborativa y en los servicios que esta se interese.

Los clientes atendidos por ECCERT en este sector serán el personal y los estudiantes de las universidades.

### 2.8.2 Estado.

El Estado y los órganos públicos serán los potenciales clientes, al cual ECCERT mostrara más atención en sus primeros pasos, de estará manera se buscara subvenciones y participación mediante los concursos de merito que el Estado realiza para el desarrollo de alguna nueva actividad en el campo de la Seguridad Informática, de esta manera se podrá financiar en sus inicios, pues en la actualidad el Estado ha mostrado mucho interés en el desarrollo y manejo de Tecnologías de la Información, encontrando ahí una forma de mostrarles la necesidad de protección a sus activos de información ante los avances de la tecnología.

En cuanto a los Ministerios y entes del Estado, sus equipos tecnológico-informáticos tanto humanos como mecánicos, por lo general, se encuentran ubicados en la capital ecuatoriana, razón por la cual los Ministerios, Subsecretarias, Direcciones y entes en general que se encuentran en otros sitios son monitoreados remotamente o gestionan a un persona que se encargue de la red, existiendo así muchas falencias en el control de la Seguridad Informática, esta falta de presencia podrá ser suplida por ECCERT.

### 2.8.3 Empresa privada.

La Empresa privada es una agente  muy importante para el cual nuestros servicios estarían siempre a disposición, al inicio  de la creación de ECCERT será difícil entrar en este campo, debido a que ellos escogen a sus servidores de manera más cerrada.

Por lo general las Empresas Privadas con base en el exterior y relacionadas con la Tecnología y el Internet poseen su propia infraestructura y equipos remotos de seguridad, razón por la cual ECCERT trabajaría de manera local, dándole soporte y ofreciendo servicios a estas Empresas.

### 2.8.4 Personas naturales

Las personas naturales también son agentes interesados muy importantes, debido a que las personas naturales interesadas en la Seguridad de sus activos de información manejan pequeñas y medianas empresas, que incluso pueden ser estas familiares.

Se divulgara y pondrá a disposición de la comunidad información que permitirá prevenir y resolver incidentes de seguridad, de esta manera se ofrecerán servicios gratuitos educando a las personas naturales sobre seguridad informática.

## 2.9 Beneficios

Los beneficios que ofrecerá ECCERT sobre sus servicios son variados, reflejando así su misión en los diferentes campos donde ECCERT actúe, sean estos, el sector académico, público, privado, etc.

Planificando y creando servicios acorde con la necesidad del sector y el cliente, revisando paso a paso que estos servicios van a satisfacer al cliente, y ejecutándolos brindado así beneficios a corto y largo y plazo, tanto como para ECCERT y nuestros clientes, manteniendo siempre a la vista la Visión.

## 2.10 Políticas de servicios

Las políticas de servicio son las herramientas que se manejaran para poder brindar un servicio de total satisfacción, considerando el tiempo y la logística que requiere brindar el servicio.

- Los horarios de servicio serán de lunes a viernes, de 8h30 am a 6h00 pm.
- La página web estará disponible las 24 horas.
- Disponibilidad a adaptarse a las necesidades del cliente, se brindaran los servicios en otros horarios.
- Para solicitar los servicios, estará disponible un número telefónico y correo electrónico.
- El tiempo de atención a la orden será máximo de 24 horas, siempre tratando de atender el servicio inmediatamente. Es importante señalar que el servicio no pasará del día siguiente.
- Si el servicio solicitado requiere que sea en un horario especial, nuestro personal podría tardarse hasta 48 horas para atenderlo, siempre tratando de atender el incidente inmediatamente.
- Si se va a necesitar factura, se tendrá que proporcionar un RUC

## 2.11 Organizaciones que prestan servicios similares

Se consulto sobre las organizaciones que prestan servicios similares y que llegarían a ser competencia para ECCERT, para esto se uso información de las organizaciones registradas en la base de datos de la Cámara de Comercio de Guayaquil, encontrando un gran número de organizaciones involucradas con el desarrollo de software pero muy pocas con referentes sobre servicios de seguridad informática, a continuación una lista con algunas de las organizaciones que antes mencionamos.

| ORGANIZACIONES QUE PRESTAN SERVICIOSSIMILARES | | | |
|---|---|---|---|
| **Nº** | **Razón Social** | **Email** | **Dirección del Negocio** |
| 1 | I.B.M. DEL ECUADOR AGENCIA EN GUAYAQUIL | mdecalle@ec.ibm.com | AV. JOAQUIN ORRANTIA Y AV. JUAN TANCA MARENGO EDIF. EXECUTIVE CENTER MEZZANINE |
| 2 | OPTIMAL SOLUTIONS OPTSOL S.A. | larmijos@jbgye.org.ec | AV. DECIMA # 822 Y GOMEZ RENDON |
| 3 | COMEXLINK S.A. LINCOMEX | jbailon@comexlink.com.ec | CDLA. LAS ORQUIDIAS AV. ISIDRO AYORA Y AV. FRANCISCO DE ORELLANA MZ. 1043 V. 19 PISO 2 |
| 4 | BASTIDAS JIMENEZ REPRESENTACIONES S.A. BAJIRESA | bajiresa@hotmail.com | NUEVA KENNEDY CALLE OCTAVA # 208 E/ LA B Y D |
| 5 | SOLUCIONES INFORMATICAS DEL ECUADOR SINFOEC S.A. | smprog@sinfoec.com | LOTIZACION FRANCISCO DE ORELLANA MZ.1327 SOLAR 22 C.C. FRANCISCO DE ORELLANA OFIC.17 (JUNTO AL HIPERMARKET) |
| 6 | CENTRO DE SERVICIOS INFORMATICOS S.A. CENINFOR | lcruz@ceninforonline.com | GARCIA AVILES # 408 Y LUQUE EDIF. FINEC PISO 8 OFIC. 807 |
| 7 | OPEN MIND TECHNOLOGY C.A. | janeth.burbano@omtech.net | TULCAN # 803 Y AV. 9 DE OCTUBRE EDIF. EL CONTEMPORANEO PISO 6 |

**Tabla 3. Organizaciones que prestan servicios similares**
**Elaborada por: Autores**

# Capítulo 3

## 3.1 Inversión

### 3.1.1Infraestructura requerida.

#### 3.1.1.1 Diseño de las oficinas

El propósito del Diseño de la Oficina es modelar las instalaciones e infraestructura que se requiere para operar el Ecuador Computer Emergency Response Team, a continuación un posible esquema de las instalaciones de nuestra organización.

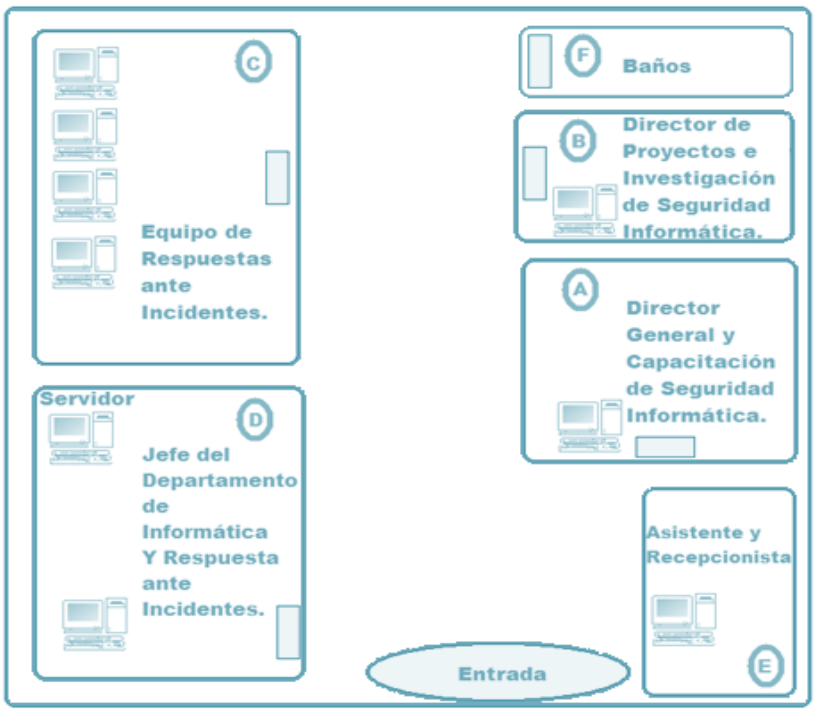


**Gráfico 5. Diseño de oficina**
**Elaborada por: Autores**

Esta Organización contara con dos oficinas, dos salas o centros de cómputo, un baño y en la entrada se encontrara la Asistente-Recepcionista encargada de la atención al cliente y de brindar información respectiva de la Organización. Cada oficina se equipara de los elementos esenciales tales como escritorios, sillas y equipos de informática.

Las salas o centros de cómputos tendrán los muebles básicos para el trabajo diario de cinco personas, contara con un Servidor e implementos para el manejo de la Red, encargados de mantener la integridad y disponibilidad en los activos informáticos de ECCERT. La recepción será dotada con su escritorio, silla y respectivos activos informáticos para atención al cliente y soporte al Director General.

#### 3.1.1.2 Descripción del Equipamiento

En el cuadro que se aprecia a continuación de desglosan los diferentes tipos de activos informáticos e inmuebles que se necesitan para llevar a cabo el proyecto.

| EQUIPOS | CANTIDAD |
|---|---|
| Muebles de Oficina | 8 |
| Computadoras | 7 |
| Router | 1 |
| Switches | 2 |
| Infocus | 1 |
| Impresora Multifunción | 1 |
| Teléfonos | 5 |

**Tabla 4. Descripción del Equipamiento**
**Elaborada por: Autores**

A continuación, se explicará detalladamente los elementos que se usaran para el equipamiento de las oficinas de ECCERT.

- **Muebles (escritorios y sillones):** Los muebles serán destinados para los Directores, Jefe, Equipo y Asistente, en total se utilizarán: 4 escritorios con sillas ,1 mesa larga para el soporte de las computadoras del Equipo de Respuestas ante incidente con sus respectivas sillas y dos sillas para recepción.
- **Computadoras:** Es la herramienta mecánica indispensable para el desarrollo del trabajo diario, 9 computadoras de manera inicial las cuales serán usadas para cada uno de los integrantes del personal.
- **Infocus:** Equipo muy necesario para charlas y reuniones que se realicen dentro de la organización, ya que facilitara el desarrollo de las mismas.
- **Impresoras Multifunción:** Equipo muy necesario que será utilizado para las impresiones y para escanear o fotocopiar los documentos importantes.
- **Teléfono:** Equipos de telecomunicación que facilitaran la comunicación interna y externa de la Organización.

### 3.1.2Esquema de red

En el gráfico 6 se desea mostrar una posible distribución de la red que se desea implantar en la organización.

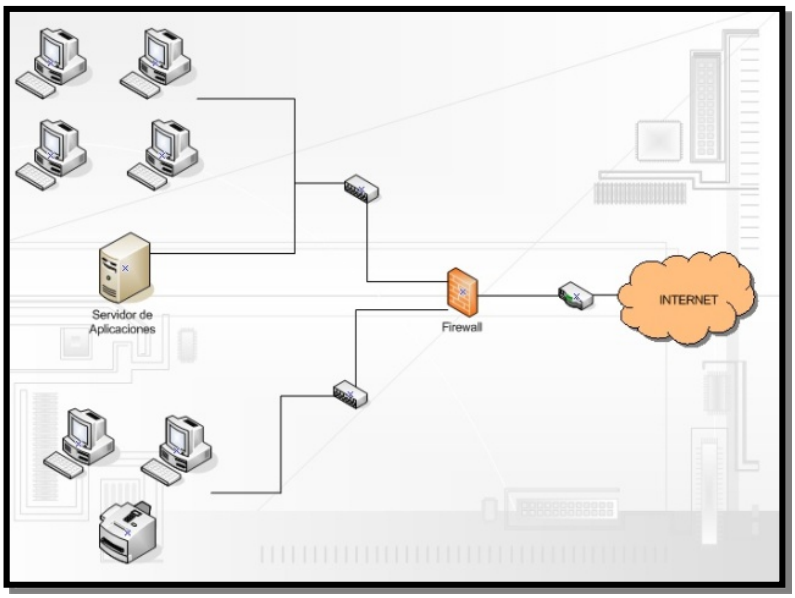


**Gráfico 6. Diseño de red**
**Elaborada por: Autores**

Teniendo en cuenta la disposición física de los distintos departamentos y los requerimientos de tráfico se decidió desarrollar una serie de redes departamentales, en este caso serán implementadas por medio de VLANS, de tal forma que cada departamento cuente con su propia red, esto permitirá que el diseño de la red sea escalable y con mayor beneficios para el equipo de trabajo.[6]

Se utilizará software libre para reducir costos y poder llevar un mayor control en cuanto a las seguridades y accesos a los dispositivos.

[6] Manual de Gestión de Incidentes de Seguridad Informática

#### 3.1.2.1 Características de la red

- Red básica segura
- No posee redundancia de servidores
- Dos segmentos de red
- Acceso a internet mínimo de 2Mbps
- Incluye distribución por capas

### 3.1.3Ubicación

Para escoger la localización de la Organización hemos considerado 3 sectores de la Ciudad de Guayaquil: Zona Centro, Norte y Sur.

Se evaluaron algunos factores para escoger la Zona en donde se localizara ECCERT, los cuales son considerados de alta prioridad para la ubicación de la Organización.

Analizando que nuestra Organización se basa netamente en ofrecer servicios, la localización debería tender a dar facilidad de acceso y cercanía a nuestros potenciales clientes de insumos.

A continuación, será detallado cada uno de los factores utilizados en el método cualitativo por puntos.

**Servicios Básicos.-** Para el correcto desempeño en las funciones de una empresa se necesitara siempre de los servicios básicos, tales como: Servicio de Internet, electricidad, agua y teléfono ya que son de vital importancia para poder brindar las condiciones necesarias básicas para que el Equipo realice de manera optima su trabajo, servicios que se muestran en la tabla a continuación.

| SERVICIOS BÁSICOS |
| --- |
| Internet |
| Energía Eléctrica |
| Agua Potable |
| Teléfono |

**Tabla 5. Servicios básicos**
**Elaborada por: Autores**

**Cercanía al Sector de Mayor Movimiento Transaccional.-** En el estudio realizado para ubicación de ECCERT pudimos encontrar una Sector en la cual sus activos de información son considerados de cuantiosa valía, que es el Sector de Mayor Movimiento Transaccional en Guayaquil, para el cual usaremos sus siglas para referirnos al mismo "SMME", en Guayaquil podemos encontrar movimiento económico en todos sus rincones, pero consideramos que el SMMT será el lugar donde se encuentren la mayor cantidad de bancos, entidades que sin sus activos de información no existirían y donde se realice de mayor manera el comercio de activos de información, ya que son entes que invierten en activos informáticos y seguridad de los mismos para la continuidad de operaciones diarias.

**Costo de Alquiler.-** El Factor costo de alquiler lo hemos tomado en cuenta ya a que es un egreso que debe ser controlado debido a los gastos que se realizaran. El costo que tendrá el alquiler de oficinas podrá variar de acuerdo a la Zona que se escogerá para la ubicación de ECCERT.

**Rutas de Acceso.-** El Factor rutas de acceso a ECCERT evalúa la localización, los medios de comunicación y transporte disponibles, al ser una Organización que ofrece servicios, se busca ayudar a la misma al estar cerca de los clientes y motivar su interés, facilitar el acceso al EQUIPO a la hora de dirigirse a laborar sin incurrir en gastos altos de transportación.

**Proveedores y Suministros.-** Este Factor nos ayuda a darnos cuenta si los insumos que necesitan para el correcto funcionamiento de ECCERT están siendo los necesarios para desarrollarse con facilidad, es de suma importancia tener esta variable presente, debido a que al tener a los proveedores cerca, se ahorra tiempo y recursos en el caso que se los necesite por alguna emergencia.

Después del análisis de cada una de las variables nombradas anteriormente, hemos decidido utilizar el método de los factores ponderados, ya que éste método permitirá de manera práctica y sencilla la identificación de los costos difíciles de evaluar que están relacionados con la localización de las instalaciones de ECCERT. En la tabla 6 a continuación, se muestran los valores tomados para realizar el método de los factores ponderados antes indicados.

| METODO CUALITATIVO POR PUNTOS | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | Zona Centro | | Zona Norte | | Zona Sur | |
| Factor | Peso | Califica. | Pondera. | Califica. | Pondera. | Califica. | Pondera. |
| Servicios Básicos | 15% | 10 | 1,5 | 7 | 1,05 | 8 | 1,2 |
| Cercano al SMMT | 20% | 9 | 1,8 | 7 | 1,4 | 6 | 1,2 |
| Costo Alquiler | 25% | 6 | 1,5 | 5 | 1,25 | 8 | 2 |
| Rutas de acceso | 25% | 8 | 2,25 | 7 | 1,75 | 7 | 1,75 |
| Proveedores y suministros | 15% | 8 | 1,2 | 8 | 1,2 | 8 | 1,05 |
| **TOTAL** | **100%** | | **8,25** | | **6,65** | | **7,2** |

**Tabla 6. Tabla de Localización - Método Cualitativo por Puntos**
**Elaborada por: Autores**

### 3.1.4Personal solicitado.

#### 3.1.4.1 Perfiles

**Director General y Capacitación de Seguridad Informática.**

- Se requiere de profesional con título universitario en Ingeniería en Ciencias Computacionales, especializado en alguna de las diferentes ramas del Área.
- Experiencia mínima de 3 años en Administración y Gerencia de Redes.
- Mínimo 25 años de edad.
- Alto conocimiento en ámbito de Seguridad de Redes Informáticas.
- Experiencia en Capacitación.
- Capacidad de análisis y buena capacidad de comunicación.
- Capacidad de liderazgo.

- Dominar 100% el idioma inglés escrito y oral.
- Se requiere persona con dotes de mando, con capacidad de planificación como de capacidad de análisis y síntesis.
- Persona responsable, perseverante, con capacidad de análisis, comprometido.

**Director de Proyectos e Investigación de Seguridad Informática.**

- Se requiere de profesional con título universitario en Ingeniería en Ciencias Computacionales, Sistemas o especializado en alguna de las diferentes ramas del Área.
- Experiencia mínima de 3 años en Administración y Gerencia de Redes.
- Mínimo 25 años de edad.
- Alto conocimiento en ámbito de Seguridad de Redes Informáticas.
- Se requiere persona con dotes de mando, con capacidad de planificación, análisis y síntesis.
- Persona responsable, perseverante, y comprometido con el proyecto.
- Capacidad de liderazgo.
- Dominar 100% el idioma inglés escrito y oral.

**Jefe del Departamento de Informática Y Respuesta ante Incidentes.**

- Se requiere de profesional con título universitario en Ingeniería en Ciencias Computacionales, Sistemas o especializado en alguna de las diferentes ramas del Área.
- Mínimo 23 años de edad.
- Mínimo 3 años de experiencia a nivel Gerencia de Departamento de Informática.

- Dominio de redes de datos y voz, administración de proyectos, administración de insumos de computo, soporte técnico, instalaciones de redes.
- Capacidad de liderazgo, creativo, escrupuloso, pro-activo y enfocado a resultados.
- Dominar 100% el idioma inglés escrito y oral.
- Buenas relaciones interpersonales.
- Se requiere de una persona líder con capacidad de gestión y capacidad resolutiva.
- Persona extrovertida, pro-activo y responsable.

**Asistente de Dirección General / Contable.**

- Se requiere profesional con título universitario de CPA, Ingeniería Comercial o Auditoria.
- Experiencia mínima de 3 años en Gerencia de Departamento Financiero o como Contador.
- Mínimo 25 años de edad.
- Se requiere persona con dotes de mando, con capacidad de planificación como de capacidad de análisis y síntesis.
- Alto conocimiento de contabilidad y finanzas.
- Persona responsable, perseverante, con capacidad de análisis, comprometido.

**Equipo de Respuestas ante Incidentes.**

- Se requiere de profesional con título universitario en Ingeniería en Ciencias Computacionales, Sistemas o especializado en alguna de las diferentes ramas del Área.
- Economía o Ingeniería Comercial.

- Mínimo 3 años de experiencia.
- habilidad de comunicación
- Capacidad de liderazgo, creativo, escrupuloso, pro-activo y enfocado a resultados.
- Dominar 100% el idioma inglés escrito y oral.

#### 3.1.4.2 Características

Se considera que entre las características fundamentales que debe reunir el personal, especialmente los que tendrán contacto directo con el cliente, se encuentren las siguientes:

- Buena salud física y mental.
- Ética profesional y cortesía.
- Estabilidad de comportamiento y acción y ser ejemplo a imitar.
- Confianza en sí mismo.
- Eficiencia y Eficacia personal, dinamismo
- Integridad (cualidad que engendra confianza).
- Independencia.
- Competencia intelectual.
- Juicio correcto (ser capaz de juzgar con objetividad).
- Elevada capacidad de análisis o de resolución de problemas.
- Orientación hacia el aspecto humano de los problemas.
- Capacidad para ganarse la confianza y el respeto del personal de la organización cliente.
- Capacidad para obtener la participación del cliente en la solución de los problemas.
- Capacidad para transmitir sus conocimientos al personal de la organización cliente.

- Capacidad para despersonalizar los problemas y enseñar a atacar sus causas y no a las personas.
- Capacidad superior a la medida para comunicar y persuadir.
- Madurez psicológica.

#### 3.1.4.3 Capacitaciones al personal

La capacitación del personal es una de la inversiones más significativas a nivel de calidad de Organización, a más de la selección del personal idóneo para cumplir las funciones encomendadas, debido a que ECCERT es una Organización que va a prestar a servicios a Nivel Nacional, siempre necesitara de personal con conocimientos tantos tecnológicos como de seguridad informática de actualizados.
Es así que, un porcentaje de los ingresos obtenidos a partir del funcionamiento del primer semestre de ECCERT será designado a la Capacitación del Personal.

El valor porcentual dedicado a la Capacitación de Personal será debidamente sustentado tomando en cuenta las variables de ingresos y egresos en el momento actual de ECCERT, revisando su Financiamiento y aplicándolo de tal manera que no afecte en sus normales operaciones proyectadas al siguiente semestre.

## 3.2 Financiamiento del CERT

El Plan de Financiamiento ha sido desarrollado en función de todos y cada uno de los servicios que CERT va a ofrecer a la comunidad informática las cifras y cantidades son estimaciones y proyecciones analizadas con el objetivo de cubrir con el propósito de viabilidad en el largo plazo.

El punto de vista de viabilidad y la continuidad de las operaciones, debe ser tratado con mucho cuidado, para no perder la proporción de la realidad y tender a exagerar con valores inalcanzables y nada factibles en la implementación del proyecto.

Por el lado de la Factibilidad hay que tomar en cuenta la importancia de la misma, ya que es considerada la parte medular a la hora de la toma de decisiones para invertir en el proyecto, desde el punto de vista de los socios.

Es importante mencionar previo al análisis cuantitativo que existen algunos elementos para establecer el Plan Financiero, mencionando algunos de ellos son:

- Inversión requerida
- Rentabilidad esperada, y
- Proyecciones en años.

### 3.2.1Política de Financiamiento:

Hemos detallado cada una las necesidades y requerimientos para la creación de ECCERT. De una manera cualitativa es decir describiendo necesidades, requerimientos pero es necesario establecer las cantidades y los precios para el establecimiento de la empresa, así como el financiamiento para la puesta en marcha del proyecto.

Como primera opción tenemos la factibilidad de préstamos para proyectos de la Corporación Financiera Nacional, se puede observar en el grafico No. 8 Por la cantidad de $ 15,000.00 como lo muestra la tabla de la amortización, con una tasa del 10,5%(tasa mínima bancaria) y con 24 pagos mensuales de $ 695.64 (Anexo No.8) Para ver más detalles ver tabla de amortización en los anexos.

Además del préstamo a la CFN, contamos con una aportación de los socios de ECCERT. De $ 5.904,00 lo cual suma al total de lo requerido para empezar nuestro Proyecto.

### 3.2.2Inversión Requerida:

La inversión requerida antes de la puesta en marcha debe tomarse en cuenta valores requeridos para poder invertir, desde el punto de vista de lo tangible o intangible de estos valores. Estas cifras pueden agruparse en la siguiente clasificación: capital de trabajo, activos fijos y costos.

**Capital de trabajo**: Es el dinero que se necesita para producir, básicamente se trata del monto necesario en caja para solventar los requerimientos de circulante mientras se realizan los cobros de recuperación. El detalle se encuentra en el anexo No.5

La inversión en capital de trabajo es una inversión en activos corrientes: efectivo inicial, inventario, cuentas por cobrar e inventario, que permita operar durante un ciclo productivo, dicha inversión debe garantizar la disponibilidad de recursos para cubrir costos de operación durante el tiempo requerido para la recuperación del efectivo.

Otro elemento clave en el análisis de inversión en capital de trabajo, es el monto de suministros (el objetivo del proyecto es contar con los equipos y recursos necesarios para poder brindar todos los servicios y productos de ECCERT, así como también tener a disposición el equipo humano requerido).

### 3.2.3Gastos de constitución.

En la tabla siguiente, podemos visualizar los costos de varios puntos que se deben cumplir para constituir la organización.

| COSTOS DE CONSTITUCIÓN DE LA COMPAÑÍA | |
|---|---|
| **DESCRIPCION** | **COSTO** |
| Inscripción de la Compañía en la Superintendencia | $ 25,00 |
| Registro de el titulo y eslogan en IEPI | $ 220,00 |
| Permiso de cuerpo de Bomberos | $ 30,00 |
| Permiso de Tasa de Habilitación | $ 10,00 |
| Permiso municipal uso de suelo | $ 25,00 |
| Gastos de Constitución de la Empresa | $ 250,00 |
| RUC | $ 0,00 |
| Honorarios Abogado(Trámites Legales) | $ 350,00 |
| | |
| **TOTAL** | **$ 910,00** |

**Tabla 7. Tabla de Gastos de Constitución**
**Elaborada por: Autores**

Por último, tenemos la inversión en activos diferidos, que se dan de los gastos operativos determinado en función del tiempo requerido para empezar el proyecto, gastos de constitución. (Ver anexo No. 4)

| | |
|---|---|
| **TOTAL DE INVERSIONES FIJAS** | $ 15.145,00 |

ECCERT. Tendrá una inversión inicial de **$ 20,904.00** dólares, la cual cubre con todos los requerimientos necesarios para empezar nuestro proyecto, incluso esta cifra respalda hechos o problemas imprevistos, que puedan suscitarse en el transcurso del proyecto. Esta inversión inicial se estima se recuperable en un promedio no mayor a 2 años, ya que hemos estimado un promedio muy interesante de membrecías anuales, los que respaldan la factibilidad del proyecto. Siendo además atractiva y rentable para algunos inversionistas que nos ayudarán a solventar el proyecto. Para un mejor análisis ver anexo No. 4

### 3.2.4Porcentaje de la inversión total.

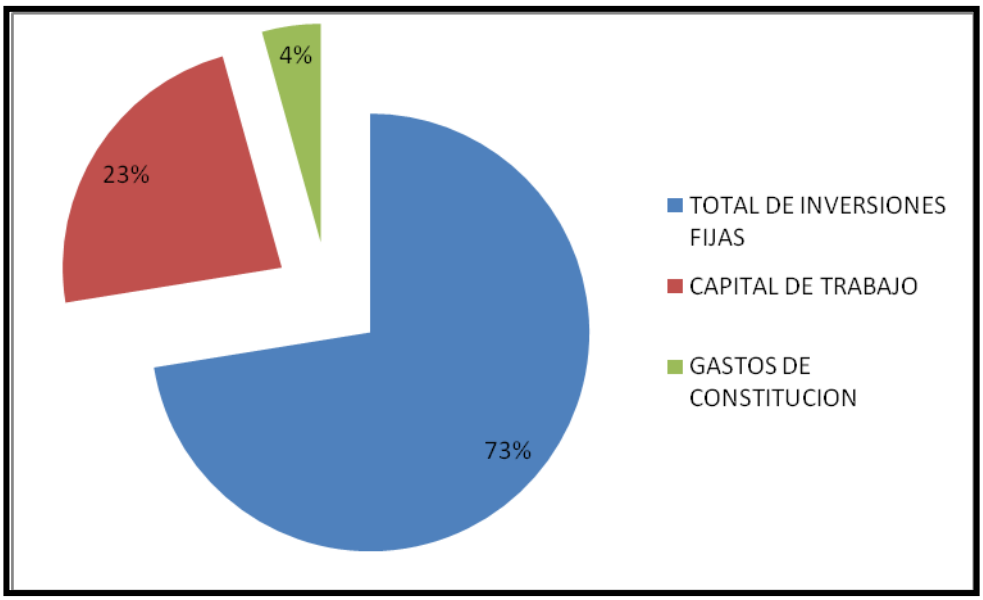


**Gráfico 7. Distribución de la inversión**
**Elaborado por: Autores del proyecto**

Analizando nuestro grafico, tenemos un 73% que constituye el total de activos o inversiones fijas, el 23% corresponde al capital de trabajo y por ultimo un 4 % que constituye el total de gastos de constitución.

## 3.3 Ingresos.

Previo a la determinación de los ingresos que percibimos por los servicios que ofrecemos tanto mensual como anualmente, realizaremos un estudio previo al análisis de la demanda, que se obtuvo como resultado de las encuestas ya anteriormente expuestas.

Por el lado de ingresos por servicios (ver anexo 7) que vamos a cobrar observamos que estos van a variar con respecto al tipo de servicio, los cuales hemos clasificado en cuatro de paquetes y membrecías que son: Membrecía Anual, Membrecía PLATINUM, Membrecía SILVER, Membrecía GOLD.

Estos cuatro tipos de membrecías tienen un costo diferente, es decir para Membrecía Anual, el precio base será trescientos dólares, los de tipo Membrecía PLATINUM se encontrarán precios de 2000 Dólares, la Membrecía SILVER tiene una precio de dos mil dólares y la Membrecía GOLD se encuentra en el valor de tres mil dólares.

Cabe indicar que estas membrecías son anuales es decir que cada uno de los servicios brindados es por el año contratado.

### 3.3.1 Proyección de Ingresos y Egresos

Hemos decidido proyectar el ingreso a cinco años, para poder determinar el margen de ganancias que recibiremos por los servicios a realizar anualmente.

Analizando las cifras en la tabla 8, llegamos a la conclusión de que el proyecto será exitoso, dado que en cada año el margen de ganancias se incrementa, lo cual será atractivo incluso para los accionistas.

| DESCRIPCION | COSTO ( $) | CANTIDAD DE CLIENTES | INGRESOS |
|---|---|---|---|
| **Membrecía anual**<br>Envío mensuales de estadísticas | 360,00 | 90 | 32.400,00 |
| **Membrecía PLATINUM**<br>Envío mensuales de estadísticas<br>(capacitación 2 veces al año)<br>Máximo 20 personas | 2.000,00 | 12 | 24.000,00 |
| **Membrecía SILVER**<br>Envío mensuales de estadísticas<br>Auditoria Informática | 2.000,00 | 12 | 24.000,00 |
| **Membrecía GOLD**<br>Envío mensuales de estadísticas<br>(capacitación 2 veces al año)<br>Máximo 20 personas<br>Incluye Auditoria Informática | 3.000,00 | 12 | 36.000,00 |
| | **TOTAL INGRESOS ANUALES POR MEMBRESIAS** | | **116.400,00** |

| DESCRIPCION | COSTO ( $) | CANTIDAD DE CLIENTES | INGRESOS |
|---|---|---|---|
| ANALISIS FORENSE | 1.000,00 | 12 | 12.000,00 |
| ESCANEO DE VULNERABILIDADES | 2.000,00 | 12 | 24.000,00 |
| SEGUIMIENTO DE INCIDENTES | 1.000,00 | 12 | 12.000,00 |
| CONSULTORIA DE SEGURIDAD | 3.000,00 | 12 | 36.000,00 |
| CAPACITACIONES ( 20 personas) | 2.000,00 | 6 | 12.000,00 |
| | **TOTAL INGRESOS ANUALES POR SERVICIOS** | | **96.000,00** |

| | |
|---|---|
| **TOTAL INGRESOS ANUALES CERT** | **212.400,00** |

**Tabla 8. Tabla de proyección de Ingresos**.
**Elaborada por: Autores**

### 3.3.2 Estimación de costos de ECCERT.

Se realizó en la tabla 9 la estimación de costos mensuales que tendría la organización, a continuación se detallan los valores estimados y un análisis de los mismos.

| ESTIMACION DE COSTOS | PROYECCION MENSUAL |
|---|---|
| SUELDOS | $ 3.300,00 |
| ALQUILER DE OFICINA | $ 600,00 |
| SERVICIOS BASICOS | $ 100,00 |
| TELEFONIA FIJA | $ 80,00 |
| TELEFONIA CELULAR | $ 250,00 |
| 1024X512 INTERNET CORPORATIVO | $ 99,00 |
| PUBLICIDAD | $ 300,00 |
| SUMINISTROS | $ 100,00 |
| HOSTING WEB PAGE | $ 20,00 |
| **TOTAL DE COSTOS FIJOS** | **$ 4.849,00** |

**Tabla 9. Tabla de estimación de costos**
**Elaborada por: Autores**

Luego de este análisis, debemos tener los costos resultantes del consumo de servicios básicos como Internet, llamadas telefónicas, en el área Administrativa (oficina) proyectados en el año, entre ellos están luz, agua, etc.

También tomamos en cuenta los **Gastos de Arrendamiento**, necesarios para la oficina de ECCERT, un área de ciento cincuenta metros cuadrados para que el personal pueda realizar sus funciones diarias y cuente con sus respectivos departamentos.

Alquilaremos una oficina, en el sector centro de la ciudad, un sector estratégico, debido a que se encuentra cerca a empresas grandes, un área de ciento cincuenta metros cuadrados que incluye dos baños, dos garajes y guardianía, con un costo de $600 mensuales.

Otro gasto de significativa importancia son los sueldos y salarios a cancelar al equipo de trabajo teniendo la siguiente distribución de los mismos: Teniendo como el mínimo $300 y el máximo $800, consideramos un presupuesto de $ 3,300.00 para pagos mensuales y $ 39,600.00 anualmente, los salarios forman parte de la distribución que tenemos que destinar para el total de gastos.

Además hemos estimado la cantidad óptima y eficiente de número de trabajadores que maximizan la utilidad de nuestra empresa concluyendo que hemos destinado un total de siete personas (recordando que nuestra empresa contará con 3 departamentos).

El último de los egresos de los que también entra en este análisis está el de gastos operativos, administrativo, Entre los valores de mayor importancia está la creación de una página Web, la publicidad en revistas.

### 3.3.3 Herramientas del análisis financiero.

Para realizar el análisis Financiero en nuestro proyecto nos valdremos de algunas herramientas muy útiles a la hora de determinar algunas dificultades Financieras, estas herramientas son los Estados Financieros, ya que la información contable que estos presentan ayudará a comprender la situación y la posición presente y futura de ECCERT como empresa. Claro está que este problema no será lo único que los Estados Financieros nos ayudarán a resolver, sino también nos permitirá tomar decisiones oportunas en nuevas adquisiciones, inversiones y estrategias factibles o rentables a favor de la empresa.

Los Elemento a tomar en consideración de entre las herramientas de los Estados Financieros mencionados, anteriormente son el Flujo de Efectivo y El Estado de Pérdidas y Ganancias.

**Valor actual neto (VAN)**

Conceptualizando brevemente el VAN o Valor actual Neto es el valor de los Flujos de Efectivo esperados menos la inversión Inicial del Proyecto.

Por lo que en el caso particular de ECCERT, fue calculado con la suma de los Flujos Anuales, un valor de $246,166.58 por concepto del VAN.

Este valor nos indica que para el primer año aproximadamente, se recuperará el total de la inversión inicial, lo cual es altamente positivo, ya que los accionistas podrán recuperar su inversión en un corto plazo y también obtendrán una buena utilidad.

**TIR**

Esta tasa consiste en evaluar el proyecto en función de una única tasa de rendimiento o la tasa de interés más alta que un inversionista pagaría sin perder su inversión. En resumidas cuentas esta tasa de descuento hace que el valor presente neto de un flujo de caja sea igual a cero.

La TIR obtenida en el flujo de caja para la realización del Proyecto de eventos es de 11.29%**.**

**CALCULO DEL TIR Y VAN**

| | PERÍODO | Año 0 | Año 1 | Año 2 |
|---|---|---|---|---|
| a) | **Costo** | | | |
| | Inventario | | | |
| | Activo Fijo | | | |
| | Diferidos | | | |
| | Capital de Trabajo | 19.000,00 | | |
| | Total de Inversión | 19.000,00 | | |
| b) | **Beneficios Netos** | | | |
| | Utilidad Neta | | 217.404,51 | 94.727,80 |
| | (+) Amortización | | 7.652,05 | 8.347,69 |
| | (+) Valor de salvamento | | | |
| c) | **Flujo Neto** | **-19.000,00** | **225.056,57** | **103.075,50** |
| | **TIR** | 11,29 | | |
| | **VAN** | 246.166,58 | | |
| | VAFE | | | |

**Tabla 10. Tabla calculo TIR y VAN**
**Elaborada por: Autores**

Después de mostrar los Estados Financieros, y las herramientas de sensibilidad, podemos concluir que el proyecto en cuestión, es económicamente viable y factible.

Esta conclusión, está respaldada en los datos obtenidos en el análisis financiero del último capítulo presentado. Teniendo como ejemplo, un VAN positivo del $246,166.58., y una TIR del 11.29%, dado esto podemos concluir que:

- La inversión requerida para ECCERT no es muy elevada con lo cual no hay pérdida de dinero por lo que los inversionistas podrán recuperar en un corto plazo su inversión (2 años).
- El estudio económico y financiero del proyecto, basado en un criterio conservador orienta a ventajas y posibilidades de llevar a cabo las actividades del negocio, logrando obtener resultados de exitosos por altos valores de retornos obtenidos al mínimo esperado fundamentado en un monto positivo del valor actual neto del proyecto (VAN).

Por otro lado, también podemos concluir, gracias al Estudio de Mercado que:

- El resultado de la investigación nos dio a conocer que existe un amplio mercado al cual dirigirnos, ya que la mayoría de empresas que hay en nuestra ciudad utiliza mucho la tecnología, para los cuales siempre necesitarán a alguien que les proporcione asesoramiento y ayuda en la capacitación en el área de tecnologías de Información.

Existe una demanda insatisfecha para la cual es necesaria la creación de este tipo de empresas encaminadas a la realización en asesoramiento, capacitación en el área tecnológica sobre todo en seguridad informática empresarial, que brinden un servicio de calidad enfocados a cubrir las necesidades e intereses del mercado.

A continuación procedemos a dar ciertas recomendaciones que consideramos son importantes a tomar en cuenta para la futura ejecución del proyecto.

- Para alcanzar los resultados proyectados, es necesario que se apliquen estrategias agresivas para las venta (el primer año) con el objetivo de captar a los clientes potenciales, pues son estás las determinantes para que el negocio continúe y crezcan los volúmenes de venta.
- Para que la empresa consiga mantenerse líder en el mercado, se recomienda la actualización y restauración del equipamiento y la infraestructura física, para de esta manera no sentirse amenazada por la competencia.
- Trabajar con una política basada en la satisfacción total de nuestros empleados y trabajadores; y mantener un ambiente de armonía en el trabajo diario, contando con la información y experiencia del giro del negocio, pueda crear competencia.

Dado que en el negocio existen periodos de estacionalidad o de recesión como temporadas en las cuales no es rentable el giro del negocio; se analiza tener cautela en el manejo de los Estados Financieros, ya que por ejemplo existen meses con ingreso nulos.

## 3.4 Difusión

Al ser nuevos en el mercado, es necesario llegar a los posibles clientes mediante unas estrategias de difusión, en las que nuestros servicios tienen que llegar a ser reconocidos.

### 3.4.1 Elaboración del Portal web

El Portal Web será la herramienta de comunicación entre la Organización y la comunidad interesada en conocer las nuevas y diferentes formas de ataques y vulnerabilidades presentadas en las diferentes aplicaciones, sistemas operativos y software en general. En el gráfico 8 a continuación, mostramos una pantalla del portal web que utilizaría la organización.[7]


**Gráfico 8. Portal Web**
**Elaborado por: Autores del proyecto**

El usuario podrá registrarse y así poder acceder a varios servicios que ofrece el portal, como son las alertas generales, el foro de discusiones y una serie de encuestas que se realizarán a menudo para evaluar los conocimientos de la comunidad.

[7] El portal será ubicado en byethost.com para realizar pruebas

Los avisos generales o noticias estarán disponibles para todos los visitantes de la página, los cuales los podrán leer y luego proceder a registrarse o ingresar para profundizar en detalles de la información, tal y como se muestra en el siguiente gráfico de las alertas en el portal web.

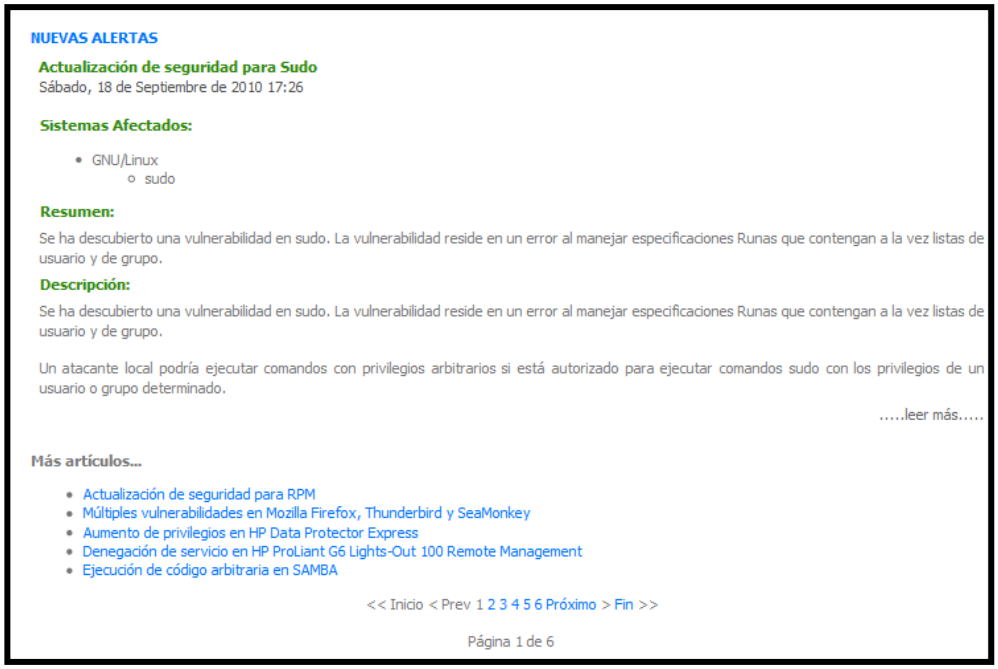


**Gráfico 9. Alertas del Portal Web**
**Elaborado por: Autores del proyecto**

El Portal Web constara con la información necesaria para que los agentes interesados puedan conocer los diferentes servicios que prestara el Equipo en los diferentes campos de la Seguridad Informática, las variadas formas de protección a nuestros equipos, para de esta manera crear conciencia e interés sobre los activos informáticos de nuestros potenciales clientes.

Será el medio de difusión principal de los servicios que ofrece ECCERT para su comunidad, los cuales se detallan y se han dividido en planes o membrecías para que puedan atractivos a quienes se encuentran interesados en adquirirlos, tal y como se muestra en el siguiente gráfico, los servicios se detallan en el portal web.


**Gráfico 10. Productos y Servicios del Portal Web**
**Elaborado por: Autores del proyecto**

Adicionalmente se puede encontrar información de lo que es ECCERT, misión y visión, sus inicios y el equipo de trabajo que lo conforma. Se encuentra llena de conceptos claves sobre seguridad informática y un poco de historia sobre lo que es CERT y seguridad de la información en general para la comunidad que recién está aprendiendo y esta escasa de conocimientos.

### 3.4.2Foros

El portal web de ECCERT contará con una herramienta foro, donde los usuarios registrados pueden participar activamente, agregar temas de interés y recibir respuestas de forma rápida no solo por los miembros del equipo CERT sino por todos los usuarios de la comunidad.

La idea del foro es dar al usuario un mayor nivel de interacción con la página, y cierta libertad para poder debatir sobre temas en los que se encuentre interesado y desee compartir con el resto de la comunidad.

Así mismo, el foro se convierte en una gran herramienta de apoyo al momento de resolver problemas en el menor tiempo posible y mantiene a la comunidad enganchada en lo que a temas de seguridad informática se refiere.

### 3.4.3Convenio con las universidades

Las universidades siempre serán un campo donde la ciencia y el conocimiento trataran de estar a la vanguardia, informados del desarrollo y auge de nuevas tecnologías, alineados con la misión de nuestra Organización, motivo por el cual ECCERT buscara formas y maneras de convenios, de esta manera se buscara optimizar los servicios y mejorar los recursos.

Los convenios manejados con universidades no solo serán de beneficio mutuo tanto como para la Organización y la Universidad interesada, sino también para la comunidad interesada en la Seguridad Informática, debido a que estos convenios ayudaran al interés de obtener tecnología segura.

### 3.4.4 Intercambio de información

El intercambio de información es uno de los pilares inteligentes mantenidos por todos los Equipos de Respuestas ante Incidentes y Emergencias a Nivel Mundial, debido a que las diferentes formas de ataques a nuestros dispositivos informáticos no solo se pueden presentar en un rincón del planeta, siendo las redes y el Internet un medio de transporte fácil podemos presenciar dichos ataques en cualquier parte del mundo.

Motivo por el cual las Organizaciones dedicadas a prestar servicios resolviendo y previniendo estos ataques informáticos, observan en el Intercambio de Información una forma de mantenerse a la vanguardia de la Seguridad Informática.

Este Intercambio de Información no solo puede presentarse a de Nivel Equipos dedicados a la tarea de la Seguridad de activos en el mundo, sino también en la comunidad interesada que recibe servicios gratuitos, que desean conocer más de estas técnicas de defensa e Intercambian Información en pro de la Seguridad Informática.

# Capítulo 4

## 4.1 Continuidad de las operaciones.

El objetivo de este proyecto es documentar todos los requerimientos iniciales para crear un CERT en Ecuador, dejar listos procedimientos a seguir al inicio de las operaciones.

Se realizó un análisis que incluyen costos reales para el inicio del proyecto, siendo el factor monetario el único inconveniente para continuar con el comienzo de las operaciones de ECCERT.

### 4.1.1 Creación de un plan integral

Lo siguiente al proyecto sería crear un plan para mantener en marcha el proyecto de crear ECCERT, este deberá ser analizado por todo el personal que integra el grupo de trabajo, el mismo que deberá asignar actividades de las cuales el personal debe estar capacitado.

## 4.2 Análisis FODA

### 4.2.1 Fortalezas

- Personal capacitado
- Actualización e investigación permanente
- Capacitación a la comunidad
- Constante comunicación con el cliente
- Respuesta inmediata a incidentes de seguridad en sistemas de información.

### 4.2.2 Oportunidades

- No existen muchas empresas que ofrecen servicios de seguridad de la información
- Formación con bases del CERT CC
- Integración al First, comunidad de CERT
- Posibilidad de alianzas con los CERT más cercanos.

### 4.2.3 Debilidades

- Poca experiencia en la constitución de una organización dentro del país.
- Pocos conocimientos con respecto a l información de las empresas de otras industrias
- No se cuenta con capital necesario para la empresa por lo que se tendrá q recurrir a un préstamo bancario u otra forma de financiamiento.

### 4.2.4 Amenazas

- Poca inversión a la seguridad de la información debido a la resistencia de empresas con pocos conocimientos del tema.
- Posible surgimiento de competencia.
- Rechazo por parte de empresas que prefieren servicios del exterior.

## 4.3 Estrategia para la continuidad del proyecto

Una vez iniciado el proyecto, su continuidad es una labor muy fuerte, para lo cual se debe crear planes de contingencia para poder mantener CERT durante el primer año, luego del cual se considera podrá sobrevivir con los recursos que genere mediante la prestación de sus servicios.

El plan de difusión es de gran importancia, ya que al poseer cierta negación a la tecnología por parte de la comunidad, llegar a ellos y transmitir el mensaje de la importancia de la seguridad informática dentro de una organización, se espera poder transmitir este mensaje mediante la participación en ferias tecnológicas o congresos.

### 4.3.1 Ferias Tecnológicas

Ser participante activo de las ferias tecnológicas que se organicen, capacitar a los expositores para que de esta forma puedan llegar a la comunidad.

CERT utilizara las ferias tecnológicas como una vía de comunicación hacia la comunidad para contribuir al desarrollo de una cultura de seguridad informática en nuestro medio.

### 4.3.2Congresos

Se espera poder ser partícipe de este tipo de eventos que se lleguen a organizar en el país, exponiendo temas de interés y casos reales en los cuales se pueda transmitir un buen mensaje a la comunidad.

Se tiene planificado realizar congresos semestrales, contando con el respaldo de las Universidades y ORGs involucradas en el tema de seguridad Informática y que han visto en CERT la oportunidad mediante la cual se logre actualizar a las personas con respecto a las nuevas tendencias de seguridad informática.

Los congresos de CERT son una iniciativa donde se presentan y discuten temas sobre seguridad informática, un área de alto interés para el desarrollo de la industria, organizaciones públicas y las empresas en un mundo globalizado altamente interconectado por la red de redes: Internet. El comercio y los negocios basados en las tecnologías de la información y comunicaciones deben necesariamente abordar con seriedad el tema de la seguridad de la información para asegurar su éxito futuro. CONGRESO CERT ofrece la oportunidad de conocer en esta área el estado de arte de la ciencia y la tecnología, como también para identificar los problemas y mostrar soluciones técnicas.

Este congreso está orientado a personas que desear conocer sobre las nuevas tendencias en lo que respecta a la seguridad informática y las vulnerabilidades que hoy en día existen en la nueva era de la comunicación.

En la tabla 11 que se muestra a continuación, se indican varios posibles temas de los congresos planificados.

| | |
|---|---|
|  | **CONGRESOS DE SEGURIDAD INFORMATICA ECCERT 2011** |
| **PROGRAMA DE LAS TEMATICAS A TRATAR** | |
| **ENERO** | 1er. Congreso de Seguridad Informática. |
| | Entre los diversos temas que se tratarán en este congreso destacan:<br>• Hacking, cracking, Ingeniería inversa, debugging, hooking, fuzzing, exploiting.<br>• Herramientas o técnicas defensivas y ofensivas punteras.<br>• Seguridad en "la nube", seguridad y hacking en entornos virtuales, productos y servicios en "la nube"<br>• Ciencia forense, investigación y técnicas anti forense.<br>• Redes, protocolos y hacking de capas 2 y 3, encapsulación. |
| **SEPTIEMBRE** | 2do. Congreso de Seguridad Informática. |
| | • Seguridad en una Infraestructura Pública de TI<br>• Seguridad en Servicios Públicos<br>• Políticas Públicas sobre Seguridad de la Información<br>• Seguridad en el Gobierno Electrónico”<br>• Seguridad en Comercio Electrónico<br>• Tecnologías de Voto Electrónico<br>• Votaciones Electrónicas y Privacidad de la Información<br>• Protocolos de Seguridad<br>• Seguridad en Redes y Comunicaciones<br>• Prevención y Detección de Intrusos<br>• Seguridad en la Web<br>• Modelos de Gestión de la Seguridad de Información<br>• Seguridad en Sistemas de Información<br>• Auditoría y Seguridad |

**Tabla 11. Posibles Congresos**
**Elaborada por: Autores**

# Capítulo 5

## 5.1 Metodología de los servicios de ECCERT

Los servicios de mayor importancia que se realizan en ECCERT responderán a una serie de pasos generales identificados por el equipo de trabajo para así poder estandarizar los servicios brindados.

### 5.1.1Pasos generales de un análisis forense

#### 5.1.1.1 Identificación

- Definir funciones y responsabilidad de cada miembro del equipo
- Obtener información sobre los agentes involucrados
- Entrevista a los clientes y levantamiento de información
- Reconocimiento de la escena y la situación
- Reconocimiento de los agentes involucrados y levantamiento de información de cada uno
- Documentar toda la información obtenida

#### 5.1.1.2 Descripción del Sistema

- Levantamiento de información del sistema involucrado
- Registro de fotos de los dispositivos visibles involucrados
- Clasificación por tipo de dispositivos
- Documentar toda la información obtenida

#### 5.1.1.3 Recolección de evidencias

- No alterar los contenidos de los discos de almacenamiento
- No utilizar herramientas propias del sistema, ya que estas pueden estar alteradas
- Evidencias volátiles
- Aquellas que se perderán al apagar el equipo
- Hora del sistema y desfase horario
    - Contenido de la memoria
    - Procesos en ejecución:
- Usuarios conectados
- Configuración de red
    - Direcciones IP, tabla de rutas, cache arp, etc
    - Conexiones activas, puertos abiertos
- Hacer checksum de todo, para evitar alteraciones
- Evidencias no volátiles
    - Aquellas que permanecerán tras apagar el equipo
    - Copiarlas al equipo de análisis
- No utilizar programas del sistema para hacer la copia
- Montar los sistemas de ficheros en modo escritura.
- Revisión y copias de logs.

#### 5.1.1.4 Análisis

- Reconstruir la secuencia de comandos ejecutados
- Analizar adecuadamente los programas en entornos seguros
- Analizar archivos normales
- Analizar archivos temporales
- Analizar archivos ocultos
- Analizar archivos borrados

#### 5.1.1.5 Informe

- Documentado
- Reproducible
- Resultados verificables
- Independiente
- Del investigador
- De las herramientas empleadas
- De la metodología

### 5.1.2Modelo para realizar análisis forense

El gráfico siguiente muestra el procedimiento a seguir para realizar análisis forense.

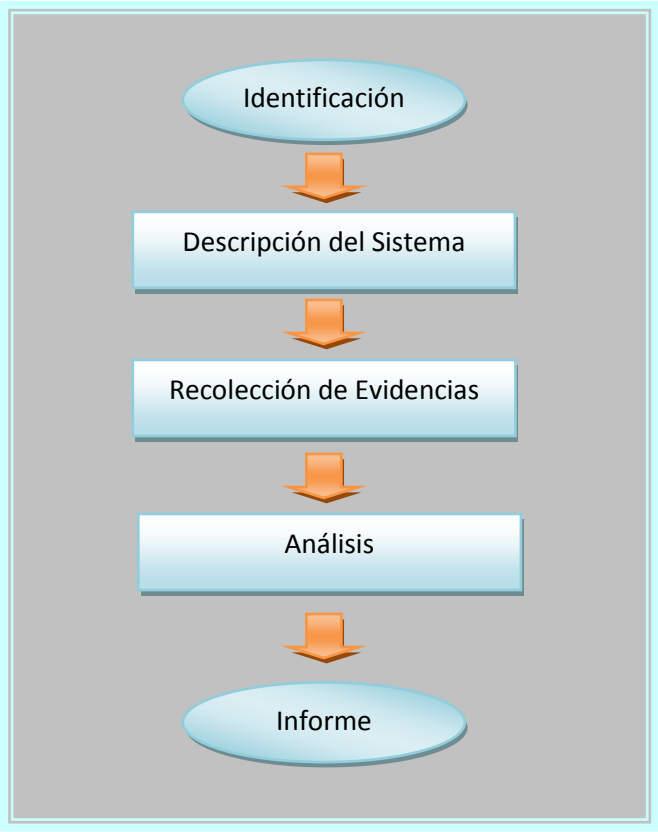


**Gráfico 11. Procedimiento de Análisis Forense**
**Elaborado por: Autores del proyecto**

### 5.1.3 Resumen de escáner de red y servidor web

A continuación se presentan los escaneos a realizar en una revisión de red y servidor web.

- Escaneo de Vulnerabilidades en PC.
- Escaneo de puertos en la PC.
- Con los datos obtenidos, completar una tabla que indique, dirección IP del host, puertos TCP y UDP disponibles y riesgos de seguridad detectadas.
- Escaneo de Vulnerabilidades de servidor Web
- Realizar un escaneo de las vulnerabilidades de dos servidores WEB.
- Analizar los puertos comprendidos entre el 15 y el 85, donde se realice una detección de Sistema Operativo.
- Con los datos obtenidos se completará una tabla donde se indique, el servidor WEB, puertos disponibles, Sistema Operativo utilizado, y riesgos de seguridad.

### 5.1.4 Resumen de una consultoría

En el desempeño del trabajo de consultoría pueden estar implícitas algunas, varias o todas las tareas siguientes, de las cuales la primera se menciona constituye una etapa inicial prácticamente obligada de cualquier otra:

- Iniciación, preparativos o preparación inicial.
- Diagnóstico, que puede permitir la identificación del estado de las cosas.

- Estudios especiales, que pueden implicar desde encuestas sobre las opiniones de los consumidores en cuanto a la calidad de los productos, investigaciones sobre la demanda perspectiva, hasta los estudios técnicos – económicos sobre inversiones para el desarrollo.
- Elaboración de soluciones, que debe constituir un paso superior al estudio de un programa, al brindar las soluciones concretas a estos, por ejemplo una de distribución de los equipos de la fábrica.
- Ayudar en la aplicación de soluciones, lo que implica una efectiva ayuda a interpretar y tomar medidas concretas para que se implanten las soluciones.
- Asesorar que consiste en dar consejo o dictaminar, y que es una de las tareas de la que consultor alguno se evade, pues debe responder cuando se le pregunta sobre los asuntos en relación con los que han solicitado sus servicios, dando criterios.

### 5.1.5Modelo para realizar consultoría

El gráfico siguiente muestra el procedimiento a seguir para realizar una consultoría.

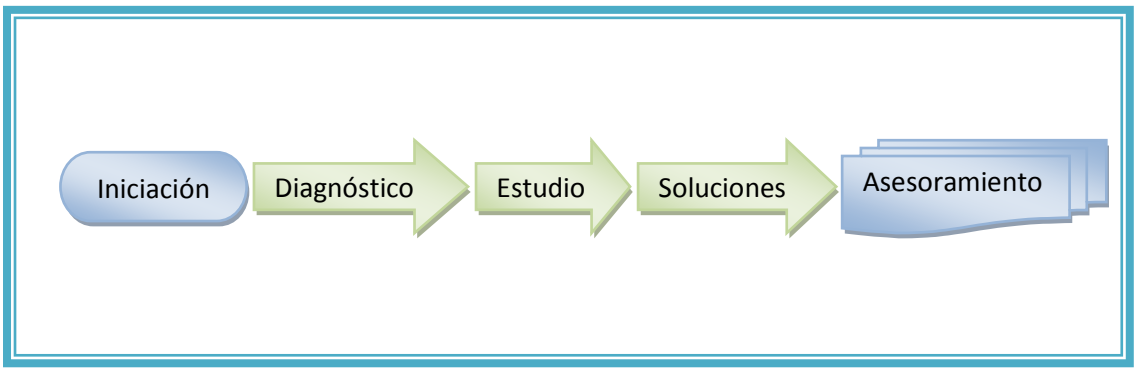


**Gráfico 12. Procedimiento de Consultoría**
**Elaborado por: Autores del proyecto**

### 5.1.6 Aplicación de la metodología en casos reales

Para la resolución de casos es necesario saber ciertos conceptos relacionados a los delitos informáticos y las condiciones legales establecidas en la legislación ecuatoriana, los cuales se detallan a continuación.

#### 5.1.6.1 Delito informático

Se entiende por delitos informáticos como todas aquellas conductas ilícitas susceptibles de ser sancionadas por el derecho penal, que hacen uso indebido de cualquier medio Informático.

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

#### 5.1.6.2 Tipos delitos informáticos

- Fraudes:- Delitos de estafa a través de la maniobra de datos o programas para la obtención de un lucro ilícito (caballos de troya, falsificaciones, etc.).
- Sabotaje informático:- Daños mediante la destrucción o modificación de datos, programas o documentos electrónicos contenidos en redes o sistemas informáticos (bombas lógicas, virus informáticos, malware, ataques de negación de servicio, etc.).
- Espionaje informático:- Divulgación no autorizada de datos reservados

- Pornografía Infantil:- Inducción, promoción, producción, venta, distribución facilitamiento de prostitución, cuando se utilizan menores con fines de exhibicionistas o pornográficos.
- Infracciones de Propiedad Intelectual:- Copia o reproducción no autorizada de programas informáticos de protección legal.

#### 5.1.6.3 Leyes establecidas en la legislación ecuatoriana.

Para que todo lo realizado en la informática forense sea exitoso, es necesario que se tengan regulaciones jurídicas que penalicen a los atacantes y que pueda sentenciárseles por los crímenes cometidos. Cada país necesita reconocer el valor de la información de sus habitantes y poder protegerlos mediante leyes. De manera que los crímenes informáticos no queden impunes.

En la legislación del Ecuador bajo el contexto de que la información es un bien jurídico a proteger, se mantienen leyes y decretos que establecen apartados y especificaciones acorde con la importancia de las tecnologías, tales como:

- Ley Orgánica de Transparencia y Acceso a la Información Pública.
- Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos.
- Ley de Propiedad Intelectual.
- Ley Especial de Telecomunicaciones.
- Ley de Control Constitucional (Reglamento Habeas Data).

Ecuador ha dado sus primero pasos con respecto a las leyes existentes, en las que se contemplan especificaciones de la información y la informática, lo que se considera un avance importante ante el desarrollo tecnológico que se ha tenido en los últimos años en el país, sin embargo es evidente que aún falta mucho por legislar, para asegurar que no queden en la impunidad los actos que se comentan relacionados con las tecnologías.

#### 5.1.6.4 Casos de seguimientos de delitos informáticos

**Caso:** Rastreo de correo electrónico

**Descripción:** Recepción de correos intimidatorios y ofensivos, enviados desde una cuenta desconocida, se inicia seguimiento para detectar el autor del correo electrónico.

**Desarrollo del caso**: La criminalística del delito telemático, especialmente del que es cometido mediante el uso del correo electrónico, se fundamenta primordialmente en el análisis de las cabeceras del e-mail, al objeto de determinar la IP de origen del mensaje. Pero tan importante como la expresión del crimen son los móviles que llevan a él: los casos de amenazas no acostumbran a darse entre personas desconocidas.

En el momento de presentar una denuncia, los investigadores acostumbran a interrogar a la víctima sobre posibles sospechosos, a fin de determinar el posible móvil del delito. El texto de la amenaza también puede ser objeto de un exhaustivo análisis: la sintaxis, la tipografía, e incluso los errores ortográficos pueden ayudar a cotejar la identidad del autor.

Las sentencias judiciales en delitos telemáticos no se fundamentan exclusivamente en la prueba informática, sino en un cúmulo de indicios que los investigadores recogen con infinita paciencia. Tras la cobardía de un amenazante anónimo siempre se esconden pasiones humanas.

Podemos establecer un paralelismo entre el denominado 'computer forensics' y la ciencia forense clásica. En ambos casos se analiza el cuerpo del delito: en un caso, computadores; en el otro, cadáveres.

Este tipo de rastreo legal del correo electrónico es similar al trabajo detectivesco convencional. Al verificar cada uno de los puntos por donde pasó el correo electrónico, el rastreador trabaja paso a paso para regresar hacia la computadora de donde se originó el correo y, con suerte, hacia al autor. Para ver cómo trabaja este proceso, caminaremos por las etapas básicas que sigue un investigador cuando tiene que enfrentar una incursión hecha por el correo electrónico.

Encabezamientos (headers). Mayormente, el rastreo del correo electrónico externo se inicia con la información que encabeza el mensaje electrónico enviado por la Internet. El encabezamiento de un mensaje es el texto de la parte superior de un mensaje electrónico que viaja a través de la Internet. Contiene el origen del mensaje en la línea "From" (De), mientras que en las líneas "Received" (recibidas), el encabezamiento enumera todos los puntos por los cuales pasó el mensaje durante su viaje, al igual que la fecha y hora.

El encabezamiento del mensaje proporciona un rastro, que puede verificarse, de los lugares por donde ha pasado un mensaje electrónico. Encontrar a la persona que envió el mensaje es asunto de recorrer el rastro en sentido inverso, punto por punto, y reunir la evidencia de que el mensaje pasó por cada punto.

Consideremos como muestra un mensaje electrónico recibido por una compañía, el cual muestra en el encabezamiento cuatro puntos de detención entre el remitente y el receptor. Dos de ellos, los pasos tres y cuatro, se encuentran dentro del sistema de correo electrónico de la compañía y aparecerán en los registros internos de mensajes electrónicos de la compañía si es que se está registrando esa información.

Si los segundos dos puntos corresponden a denominaciones electrónicas desconocidas fuera de la red informática de la empresa, los investigadores pueden apelar a algunas herramientas de investigación. Servicios que buscan en las bases de datos de los registradores que anotan a los usuarios en línea y sus direcciones IP (Protocolo de Internet), que son identificadores numéricos de las computadoras de una red informática, equivalentes virtuales a una dirección domiciliaria. Esto les da a los investigadores un lugar por donde empezar a rastrear el mensaje.

Si el domicilio de la persona remitente no es falso, encontrar a la persona detrás de la computadora se convierte en un asunto de averiguar quién empleó la máquina en el momento en que se remitió el mensaje. Por ejemplo, en el caso en el que una persona envió una amenaza de bomba a una compañía a través de una cuenta comercial de correo electrónico de la computadora de una biblioteca, los investigadores rastrearan el correo electrónico hasta la computadora de la biblioteca y posteriormente pudieron determinar quién había usado la computadora, al revisar los registros de usuarios.

**Falsificación:** Pero rara vez es tan fácil el seguimiento forense. Algunos sistemas de correo electrónico eliminan el encabezamiento del mensaje antes de entregarlo al receptor o esconden el encabezamiento del mensaje dentro del programa de correo electrónico. En otros casos, se falsifica la línea "From" del encabezamiento. Las herramientas que pueden ayudar a rastrear los pasos intermedios del mensaje no pueden determinar la dirección real si es que se ha insertado información falsa, ni pueden identificar quién ha robado la cuenta de otro o usado información domiciliaria falsa, de tal modo que cada vez que un remitente falsea una dirección, estas herramientas son de uso limitado.

La línea "From" puede ser adulterada de varias formas. Estas incluyen el engaño ("spoofing"), reenvío, retransmisión, robo de cuentas y creación de cuentas falsas.

**Engaño:** Se llama "engaño" el hacer que un correo electrónico parezca provenir de alguien (o de algún lugar) diferente del verdadero remitente. Para hacer esto, el que envía el mensaje utiliza un programa que está fácilmente disponible en la Internet, para cortar su dirección IP y reemplazarla con la dirección de otra persona. Afortunadamente, este truco no crea una barrera impenetrable para los investigadores, porque la primera computadora que recibe el mensaje "engañoso" registra la verdadera dirección IP del equipo que envía el mensaje, como un asunto de protocolo, aun cuando el IP falsificado esté en el encabezamiento. Esto le da al investigador forense una forma de encontrar el equipo real y luego empezar a rastrear al individuo que lo usó.

**Reenvío (Remailing).** Otra forma de sacar del camino a los investigadores, es enviar el correo electrónico a una computadora que retira la dirección IP del remitente y lo vuelve a enviar con la dirección IP de la computadora que hace el reenvío. La única manera de averiguar quién remitió el correo electrónico es tener acceso a los registros de la computadora que reenvió el mensaje. Pero como el diseño de las computadoras que reenvían las hace anónimas, normalmente no registran los mensajes electrónicos que han pasado a través de ellas.

Es difícil identificar a los remitentes que han empleado computadoras que reenvían mensajes, a menos que hayan cometido un error. Una de esas equivocaciones puede estar en el contenido que envían. Un análisis del mensaje o documento adjunto, por ejemplo, puede dar indicios sobre la identidad del remitente. La información que el programa encaja en los propios documentos también puede dar pistas sobre la identidad del sistema y de la computadora de donde vino el mensaje.

**Retransmisión (Relaying):** Una tercera forma en que alguien puede esconder el origen de un mensaje electrónico es hacer que el servidor de correos de otra persona se encargue de enviar el mensaje. Un servidor de correos apropiadamente configurado sólo tramitará la correspondencia de su propio sistema y no retransmitirá mensajes de direcciones IP originados fuera de su red informática. Pero si el servidor de correo no está configurado correctamente, se hace vulnerable al mal uso. Por ejemplo, los remitentes de propaganda comercial no autorizada (spammers) podrían crear un mensaje electrónico para un gran número de receptores y después canalizar el mensaje a través del servidor de correos de una compañía que no sospecha lo que sucede. El remitente lo usa como un punto de retransmisión, y el dueño del servidor podría no saber nunca que allí ha estado el que envió los mensajes electrónicos. El remitente luego desaparece antes de que alguien empiece a entrar en

sospechas. Esto no es sólo un robo de servicios, sino también una potencial denegación de ellos si el volumen de correo electrónico enviado a través del servidor lo hace fallar, negando el acceso de la compañía a su propio correo o servicio.

**Robo de cuentas de correo electrónico:** Un cuarto medio de cubrir las huellas electrónicas es obtener el acceso a la clave y a la cuenta de correo electrónico de otra persona. Algunas de las formas más comunes de conseguir el acceso son el "shoulder-surfing" (observar por encima del hombro de otro mientras ingresa su clave y ID) o husmeando (“sniffing”) una red (observar todo el tráfico de una red e interceptar los IDs y claves de los usuarios). Una vez que un pirata informático posee una clave y un ID legítimos, toda la red está comprometida. Cuando los investigadores descubren la actividad ilegal e intentan encontrar a la persona que está detrás de ella, serán conducidos a la víctima inocente cuya cuenta ha sido secuestrada. Sin embargo, para determinar quien habría secuestrado la computadora, los investigadores necesitarían otras maneras para probar quién era el usuario al momento de producirse el delito. Las terminales públicas pueden tener una hoja de registro de ingreso o una cámara de vigilancia, lo que puede adelantar la investigación.

**Cuentas falsas de correo gratuito:** Otra táctica usada por los criminales es asegurarse que el rastro se diluirá cuando el investigador pase del mundo electrónico al real. En este caso, el remitente no esconde el origen del mensaje electrónico en términos de la computadora desde la cual se envió. Sin embargo, llegar a esa computadora durante la investigación no revelará nada sobre la verdadera identidad del delincuente porque esa persona habrá dado una identidad y domicilio falsos cuando abrió la cuenta.

Es difícil capturar a alguien que ha hecho esto porque la compañía de correo electrónico nunca sabe quién abrió la cuenta falsa. Los que se dedican a la pornografía usan este truco con frecuencia.

**El registro:** En la mayoría de los casos, el rastreo forense del correo electrónico se apoya en los registros de las computadoras. Un registro de computadora es la anotación de cada mensaje de correo electrónico que pasa por una computadora de una red informática. Idealmente, los investigadores prueban que un correo electrónico viajó a través de una máquina, localizando el número de identificación del mensaje en un registro de transacciones de correo, junto con la fecha y hora en que se registró la dirección. Lamentablemente, esta situación ideal no es típica. Los problemas se presentan cuando no existen registros. Los límites legales y los problemas de jurisdicción internacional pueden también crear serios desafíos para los investigadores que están tratando de seguir el rastro del correo electrónico.

**Ausencia de registros:** El mayor desafío que enfrenta un investigador es el proveedor de servicios de Internet (ISP) que no lleva registro de los mensajes electrónicos. Los ISP más pequeños no conectan las funciones de registro de sus computadoras, sea porque tienen personal inadecuadamente entrenado o porque no desean la responsabilidad de brindar información sobre sus clientes. Algunos ISP mantienen sólo datos parciales, como las anotaciones de registros (log-ins) o las transferencias FTP (protocolo de transferencia de archivos) hacia y desde la máquina. Esto puede dificultar la labor del investigador porque no hay suficiente información para dar el siguiente paso.

**Límites de la ley:** Aun cuando los ISP llevan suficientes registros, varían en su interés por ayudar a los investigadores. Algunos fácilmente proporcionan los registros de las computadoras para ayudar en la investigación, mientras que otros se rehúsan a entregar los registros si no existe una orden o citación judicial. (Tienen la legítima preocupación de ser llevados ante la justicia por violar los derechos de privacidad de los usuarios).

Para el investigador privado que no tiene el respaldo de la ley, conseguir una orden judicial puede ser difícil o imposible. Para superar este impedimento a su avance, los investigadores pueden trabajar con organizaciones policíacas cuando investigan un delito para su compañía o un cliente. Si los oficiales de policía toman contacto con el ISP y le informan que cierto usuario está siendo investigado, el ISP está obligado por ley a preservar cualquier información que habría normalmente registrado o reunido, dando tiempo a los investigadores para buscar la autoridad legal para obtener la información pertinente. Sin embargo, los ISP no están obligados a incrementar sus actividades de seguimiento. Consecuentemente, si no estaban llevando un registro, no están obligados a empezar a hacerlo.

**Incidentes internacionales:** Rastrear a través de jurisdicciones internacionales a los intrusos de computadoras y de correos electrónicos, puede ser realmente difícil. En muchos casos, uno tiene que contar con el respaldo de un agregado jurídico y del Departamento de Estado, así como el apoyo de los organismos policiales del país. Si la pista conduce a una computadora ubicada en un país que no desea ayudar, muy poco se puede hacer. Los investigadores podrían dirigir su atención a una computadora específica en ese país. Pero no hay forma de comprobar si la computadora fue víctima de un pirata informático o específicamente quién envió el mensaje electrónico.

**Búsquedas dentro de la organización:** Si el problema se origina en las propias computadoras de la compañía, la búsqueda es más fácil, al menos en el sentido de que la compañía tiene acceso físico al equipo así como el derecho legal de efectuar una búsqueda del contenido (suponiendo que están en aplicación los avisos de registro y/o los convenios con los usuarios, mediante los cuales el usuario acepta el control sobre el sistema y concuerda en que el sistema sólo es para uso oficial). Esto supone, por supuesto, que la compañía tiene en aplicación buenos procedimientos y políticas. Por ejemplo, se debe asegurar que los servidores de correo estén configurados apropiadamente para anotar las transacciones del correo electrónico y que se consigan copias de respaldo de esas anotaciones con regular frecuencia.

Una vez que se han encontrado las computadoras involucradas, el equipo de análisis obtiene copias exactas (llamadas “copias imagen”) de los discos duros. Cualquier análisis de una porción de un medio de información debe hacerse siempre en una copia imagen para evitar que se altere la evidencia original. Luego, el equipo efectúa una revisión completa de estos registros. Buscan fragmentos de archivos o partes de cualquiera de los mensajes electrónicos que contengan referencias específicas al mensaje ofensivo. Por ejemplo, si el usuario estaba empleando el servicio público de correo electrónico Hotmail, los investigadores comprobarán la copia imagen del cache de la Internet del buscador (browser), que muestra dónde ha estado en línea el usuario. Ella contendrá las copias de los mensajes electrónicos creados o enviados o recibidos vía Hotmail. Si el usuario ha vaciado el cache o de otra manera ha eliminado un mensaje electrónico, los investigadores generalmente pueden usar los programas utilitarios para restaurar elementos eliminados para lograr recuperar esta información.

Los investigadores también pueden realizar un análisis de nodos de red, un examen de todos los registros de la computadora, que pueden ayudar a determinar la ruta que siguió un mensaje electrónico o un pirata informático. Por ejemplo, los servidores Web y FTP mantienen registros de todos los pedidos hechos al servidor y disponen de herramientas automatizadas para comparar los registros y juntar los patrones de información o de semejanzas.

Cuanta mayor sea la rapidez en la presentación de una denuncia, mayores posibilidades existirán de que las compañías involucradas conserven los datos que permitan dar con el responsable de la amenaza, y mayores las posibilidades de encontrar documentación en el ordenador de las personas que puedan ser detenidas. Al igual que ocurre en el mundo físico, también en el mundo digital el tiempo acaba por borrar todas las huellas.

## CONCLUSIONES

1. Luego de realizado los análisis para el diseño y operación del primer CERT en Ecuador llegamos a la conclusión de la importancia que tendría esta organización en nuestro país, al estar en crecimiento tecnológico debe haber un referente en gestión de la seguridad de la información que sea de ayuda a las organizaciones locales a mantenerse informadas sobre nuevas vulnerabilidades, a realizar conciencia sobre el manejo de la información e incentivar a la capacitación y creación de políticas para el personal, y a las organizaciones internacionales proporcionando información y ayuda en la resolución de posibles casos de incidentes de seguridad de la información.

2. Al ser una nueva propuesta en el mercado, ofrecer servicios de seguridad de la información, podría crear barreras y causar dificultades llegar hasta quienes serían el cliente final, aquellas organizaciones que requieran de los servicios.

3. Sin embargo, ser nuevos también tiene su beneficio, realizando los planes mostrados en el documento presente nos llevara a ser conocidos rápidamente, y así cumplir uno de los objetivos principales de convertirnos en referentes de seguridad informática.

4. El costo del proyecto es elevado, se presenta como un negocio de mediano riesgo tomando como una ventaja un periodo de recuperación de 2 años aproximadamente.

5. El estudio realizado muestra ser un proyecto viable, y de gran importancia para las organizaciones por los servicios que se ofrece que ayudan a mejorar los procesos internos de la organización, lo que indica sería un proyecto exitoso considerando los puntos citados en la investigación realizada.

## RECOMENDACIONES

1. La realización de este proyecto nos ha permitido obtener conocimientos el poco valor que se le da debido a la falta de conocimientos de tener nuestra información expuesta y la importancia que tiene la seguridad de la información en el desarrollo tecnológico de las organizaciones de nuestro país.

2. Tanto las grandes organizaciones como las pequeñas deben brindar mayor atención a los activos de información que poseen, el lugar donde se encuentra almacenado, los cuidados que se le dan a los equipos y el personal a cargo, ya que la información es un capital de mucho valor para las organizaciones y por lo tanto se deben tomar las medidas necesarias de seguridad para mantenerla a salvo.

3. Entre las principales medidas a tomar priorizamos la adquisición de conocimientos o consultoría a personas especializadas que puedan ayudar en la gestión del almacenamiento de la información y verificar que esta se encuentre almacenada en un lugar seguro, invertir en capacitaciones al personal y dar a conocer lo importante que es para la organización mantener seguro los activos de información, establecer políticas de seguridad y hacer seguimientos para verificar que estas se cumplan.

4. Finalmente hacemos el llamado de atención a las entidades educativas para que se haga conciencia sobre el manejo de la información en general, de esta forma buscamos mejorar en el futuro y formar profesionales conscientes y honestos, ya que la información siempre estará disponible para el personal que labora dentro de las empresas; y por parte de las organizaciones capacitar a su personal para tener consciencia en cuanto a la manipulación de la información se refiere.

## ANEXOS

| DESCRIPCIÓN DEL EQUIPAMIENTO | | | |
|---|---|---|---|
| **EQUIPOS** | **CANTIDAD** | **VALOR UNITARIO** | **VALOR TOTAL** |
| Computadoras | 7 | $ 780,00 | $ 5.460,00 |
| Servidor de aplicaciones | 1 | $ 1.200,00 | $ 1.200,00 |
| Router | 1 | $ 800,00 | $ 800,00 |
| Switches | 2 | $ 400,00 | $ 800,00 |
| Infocus | 1 | $ 790,00 | $ 790,00 |
| Impresora Multifunción | 1 | $ 300,00 | $ 300,00 |
| Teléfonos | 8 | $ 45 | $ 360,00 |
| | | **TOTAL** | **$ 9.710,00** |

**Anexo 1. Descripción del Equipamiento de EC-CERT**
**Elaborado por: Autores del proyecto**

| COSTOS DE CONSTITUCIÓN DE LA COMPAÑÍA | |
|---|---|
| **DESCRIPCION** | **COSTO** |
| Inscripción de la Compañía en la Superintendencia | $ 25,00 |
| Registro de el titulo y eslogan en IEPI | $ 220,00 |
| Permiso de cuerpo de Bomberos | $ 30,00 |
| Permiso de Tasa de Habilitación | $ 10,00 |
| Permiso municipal uso de suelo | $ 25,00 |
| Gastos de Constitución de la Empresa | $ 250,00 |
| RUC | $ 0,00 |
| Honorarios Abogado(Trámites Legales) | $ 350,00 |
| **TOTAL** | **$ 910,00** |

**Anexo 2. Costos de constitución de la compañía**
**Elaborado por: Autores del proyecto**

| DESCRIPCIÓN DE MOBILIARIO DE OFICINA | | | |
|---|---|---|---|
| **DESCRIPCION** | **CANTIDAD** | **VALOR UNITARIO** | **TOTAL** |
| Sillones Ejecutivos | 2 | $ 200,00 | $ 400,00 |
| Sillas de Trabajo | 12 | $ 30,00 | $ 360,00 |
| Basurero metálico | 6 | $ 15,00 | $ 90,00 |
| Archivadores aéreos | 5 | $ 65,00 | $ 325,00 |
| Archivadores verticales | 4 | $ 90,00 | $ 360,00 |
| Muebles de recepción | 2 | $ 400,00 | $ 800,00 |
| Archivador tipo vitrina | 1 | $ 200,00 | $ 200,00 |
| Papelera metálica | 4 | $ 25,00 | $ 100,00 |
| Escritorios ejecutivos | 2 | $ 150,00 | $ 300,00 |
| Escritorios en L con cajonera | 1 | $ 150,00 | $ 150,00 |
| Mesa para reuniones | 1 | $ 150,00 | $ 150,00 |
| Aire acondicionado 24 BTU | 1 | $ 700,00 | $ 700,00 |
| | | **TOTAL** | **$ 3.935,00** |

**Anexo 3. Descripción de mobiliario de oficina de EC-CERT**
**Elaborado por: Autores del proyecto**

| INVERSION TOTAL DEL PROYECTO EC-CERT | |
|---|---|
| **INVERSIONES FIJAS** | **MONTO** |
| EQUIPOS DE OFICINA | $ 9.710,00 |
| MUEBLES DE OFICINA | $ 3.935,00 |
| INSTALACION DE OFICINA | $ 1.500,00 |
| **TOTAL DE INVERSIONES FIJAS** | $ 15.145,00 |
| **CAPITAL DE TRABAJO** | $ 4.849,00 |
| **GASTOS DE CONSTITUCION** | $ 910,00 |
| **TOTAL** | **$ 20.904,00** |

**Anexo 4. Inversión total del proyecto EC-CERT**
**Elaborado por: Autores del proyecto**

| COSTOS FIJOS EC-CERT | | |
|---|---|---|
| | **PROYECCION MENSUAL** | **PROYECCION ANUAL** |
| SUELDOS | $ 3.300,00 | $ 39.600,00 |
| ALQUILER DE OFICINA | $ 600,00 | $ 7.200,00 |
| SERVICIOS BASICOS | $ 100,00 | $ 1.200,00 |
| TELEFONIA FIJA | $ 80,00 | $ 960,00 |
| TELEFONIA CELULAR | $ 250,00 | $ 3.000,00 |
| 1024X512 INTERNET CORPORATIVO | $ 99,00 | $ 1.188,00 |
| PUBLICIDAD | $ 300,00 | $ 3.600,00 |
| SUMINISTROS | $ 100,00 | $ 1.200,00 |
| HOSTING WEB PAGE | $ 20,00 | $ 240,00 |
| TOTAL DE COSTOS FIJOS | **$ 4.849,00** | **$ 58.188,00** |

**Anexo 5. Costos fijos EC-CERT**
**Elaborado por: Autores del proyecto**

| CAPITAL DE TRABAJO | | | |
|---|---|---|---|
| **SUELDO BASE MENSUAL** | | | |
| **Puesto** | **No** | **Base** | **Total** |
| Director General | 1 | $ 800,00 | $ 800,00 |
| Jefe del Departamento de Proyectos y Respuesta ante Incidentes | 1 | $ 600,00 | $ 600,00 |
| Asistente de Dirección General / Contable | 1 | $ 300,00 | $ 300,00 |
| Equipo de Respuestas ante Incidentes | 4 | $ 400,00 | $ 1.600,00 |
| **TOTAL** | 7 | | $ 3.300,00 |

**Anexo 6. Capital de trabajo**
**Elaborado por: Autores del proyecto**

| SERVICIOS DE EC-CERT | |
|---|---|
| **DESCRIPCIÓN** | **COSTOS** |
| ANALISIS FORENSE | $ 1.000,00 |
| ESCANEO DE VULNERABILIDADES | $ 2.000,00 |
| SEGUIMIENTO DE INCIDENTES | $ 1.000,00 |
| CONSULTORIA DE SEGURIDAD | $ 3.000,00 |
| CAPACITACIONES ( 20 personas) | $ 2.000,00 |
| **TOTAL** | $ 9.000,00 |

**Anexo 7. Servicios**
**Elaborado por: Autores del proyecto**

| AMORTIZACION DEL PRESTAMO | |
|---|---|
| Monto | $ 15.000,00 |
| Tasa de interés | 10,50% |
| Pago | $ 695,64 |
| Tiempo | 24 MESES |

| TABLA DE AMORTIZACION PRESTAMO CERT | | | | |
|---|---|---|---|---|
| **PERIODO** | **INTERESES** | **AMORTIZACION** | **PAGO** | **SALDO** |
| - | - | - | - | $ 15.000,00 |
| 1 | $ 131,25 | $ 564,39 | $ 695,64 | $ 14.435,61 |
| 2 | $ 126,31 | $ 569,33 | $ 695,64 | $ 13.866,28 |
| 3 | $ 121,33 | $ 574,31 | $ 695,64 | $ 13.291,97 |
| 4 | $ 116,30 | $ 579,34 | $ 695,64 | $ 12.712,63 |
| 5 | $ 111,24 | $ 584,41 | $ 695,64 | $ 12.128,23 |
| 6 | $ 106,12 | $ 589,52 | $ 695,64 | $ 11.538,71 |
| 7 | $ 100,96 | $ 594,68 | $ 695,64 | $ 10.944,03 |
| 8 | $ 95,76 | $ 599,88 | $ 695,64 | $ 10.344,15 |
| 9 | $ 90,51 | $ 605,13 | $ 695,64 | $ 9.739,02 |
| 10 | $ 85,22 | $ 610,42 | $ 695,64 | $ 9.128,59 |
| 11 | $ 79,88 | $ 615,77 | $ 695,64 | $ 8.512,83 |
| 12 | $ 74,49 | $ 621,15 | $ 695,64 | $ 7.891,67 |
| 13 | $ 69,05 | $ 626,59 | $ 695,64 | $ 7.265,09 |
| 14 | $ 63,57 | $ 632,07 | $ 695,64 | $ 6.633,01 |
| 15 | $ 58,04 | $ 637,60 | $ 695,64 | $ 5.995,41 |
| 16 | $ 52,46 | $ 643,18 | $ 695,64 | $ 5.352,23 |
| 17 | $ 46,83 | $ 648,81 | $ 695,64 | $ 4.703,42 |
| 18 | $ 41,15 | $ 654,49 | $ 695,64 | $ 4.048,94 |
| 19 | $ 35,43 | $ 660,21 | $ 695,64 | $ 3.388,72 |
| 20 | $ 29,65 | $ 665,99 | $ 695,64 | $ 2.722,73 |
| 21 | $ 23,82 | $ 671,82 | $ 695,64 | $ 2.050,92 |
| 22 | $ 17,95 | $ 677,70 | $ 695,64 | $ 1.373,22 |
| 23 | $ 12,02 | $ 683,63 | $ 695,64 | $ 689,59 |
| 24 | $ 6,03 | $ 689,59 | $ 695,64 | $ 0,00 |

**Anexo 8. Amortización del préstamo**
**Elaborado por: Autores del proyecto**

| Servicio de Envío de Alertas Personalizado ECCERT | |
|---|---|
| Planes Corporativos EC-CERT | |
| **DESCRIPCION** | **COSTOS** |
| **Membrecía anual** | $ 360 |
| • Envío mensuales de estadísticas | |
| Este servicio tiene como objetivo informar sobre las nuevas vulnerabilidades aparecidas en los sistemas informáticos, ofreciendo toda la información necesaria para que el administrador de sistemas pueda evaluar el riesgo y tomar las medidas necesarias. | |
| **Membrecía PLATINUM** | $ 2000 |
| • Envío mensuales de estadísticas | |
| • (capacitación al personal 2 veces al año) | |
| • Máximo 20 personas | |
| Este plan además del servicio de envío de estadísticas se enfoca, en la capacitación al personal de la empresa, para ello se analizará cuáles son sus necesidades en seguridad informática con el fin de satisfacer las expectativas actuales de seguridad | |
| **Membrecía SILVER** | $ 2000 |
| • Envío mensuales de estadísticas | |
| • Auditoria Informática | |
| Este tipo de membrecía se orienta a empresas con una gran infraestructura, En este servicio incluimos una auditoria informática que básicamente, consiste en realizar un análisis de la eficiencia de los sistemas informáticas, la verificación de los procesos y gestión de los recursos humanos e informáticos | |
| **Membrecía GOLD** | $ 3000 |
| • Envío mensuales de estadísticas | |
| • (capacitación al personal 2 veces al año) | |
| • Máximo 20 personas | |
| • Incluye Auditoria Informática | |
| La membrecía GOLD, es un paquete completo de servicios de seguridad informática, ya que comprende desde el servicio de envío de alertas, auditoria de la infraestructura informática para poder evaluar los recursos para luego crear procedimientos y procesos, finalmente preparamos la capacitación al personal de la Empresa. | |

**Anexo 9. Tipos de membrecías**
**Elaborado por: Autores del proyecto**

| UTILES DE OFICINA | |
|---|---|
| **DESCRIPCIÒN** | **CANTIDAD** |
| Hojas a4 500 | 11 |
| Carpetas | 220 |
| Clips* | 200 |
| Grapadoras | 11 |
| Perforadoras | 11 |
| Pestañas** | 200 |
| Adhesivos** | 200 |
| Marcadores* | 50 |
| Lápices* | 50 |
| Plumas* | 50 |
| Estilógrafos | 1 |
| Post-it** | 50 |
| Bandejas organizadoras | 9 |
| Sellos | 40 |
| Organizador de sellos | 9 |
| Almohadillas | 9 |
| Agendas | 10 |
| Bitácoras | 1 |

**Anexo 10. Útiles de oficina**
**Elaborado por: Autores del proyecto**

| Compañías de tecnología, afiliadas a la Cámara de Comercio de Guayaquil | |
|---|---|
| **Razón Social** | **Actividad General** |
| ANDRADE MENESES VIOLETA ELIZABETH | DESARROLLO E IMPLEMENTACION DE SOFTWARE |
| OPTIMAL SOLUTIONS OPTSOL S.A. | DESARROLLO DE SISTEMAS INFORMATICOS |
| COMEXLINK S.A. LINCOMEX | CONSULTOR Y DESARROLLADOR DE SOFTWARE Y HARDWARE |
| OPEN MIND TECHNOLOGY C.A. | CONSULTOR Y DESARROLLADOR DE SOFTWARE |
| AGROSOFT S. A. | CONSULTOR Y DESARROLLADOR DE SOFTWARE |
| THEMICROSERV S.A. | DESARROLLO DE APLICACIONES DE SOFTWARE |
| SERVICIOS PROFESIONALES CIMA-E C. LTDA. | CONSULTORIA DE SOFTWARE Y TECNOLOGIA DE INFORMACION |
| HARDCOMPUTER | SOPORTE TECNICO, COMPUTACION,VENTA DE EQUIPOS Y REDES |
| I.T.G.S. INFORMATION TECHNOLOGY GLOBAL SERVICES S.A. | SISTEMAS DE COMUNICACION ELECTRICA |
| ORGANIZACION DE SISTEMAS E INFORMATICA OS. S.A. | VENTA DE ENLACES DE INTERNET, DESARROLLO DE SOFTWARE |
| TARGETSOFT S.A. | DESARROLLO DE SOFTWARE |
| SOTICORP S.A. | DESARROLLO DE SOLUCIONES TECNOLOGICAS |
| E-TECHNOLOGY S.A. | DESARROLLO DE SOFTWARE |
| ECOSYSTEM S.A. | DESARROLLO PAGINA WEB |
| IROUTE SOLUTIONS CIA. LTDA. | ASESORIA Y DESARROLLO DE SISTEMAS Y CONSULTORIA DE NEGOCIOS. ESPECIALIDAD DE SISTEMAS DE INFORMACION GERENCIAL CON BUSINESS INTELLIGENCE. |
| MICROSOFT DEL ECUADOR S.A. | REPRESENTACION DE MICROSOFT, DESARROLLO DE SOFTWARE |

| | |
|---|---|
| CONCIERTO DE TECNOLOGIA CIA. LTDA. CONCIERTEC | CONSULTOR Y DESARROLLADOR DE SOFTWARE |
| ECUADIGITAL S.A. | ANALISIS, DISEÑO Y PROGRAMACION DE SISTEMAS - PROCESAMIENTO O TABULACION DE TODO TIPO DE DATOS |
| REPRESENTACIONES Y NEGOCIOS S.A. REPRESENSA | DESARROLLO DE SOFTWARE |
| SMART TECNOLOGIA S.A. SMT | ANALISIS, DISEÑO Y PROGRAMACION DE SOFTWARE |
| TFASE S.A. | DESARROLLO DE SOFTWARE Y ASESORIA EN SISTEMAS INFORMATICOS |
| RAQUEL VITALIA GARCIA SALAS | DISEÑO Y PROGRAMACION DE SISTEMAS INFORMATICOS |
| ELECTROHOME S.A | ACTIVIDADES DE INSTALACION, MANTENIMIENTO Y REPARACION DE SISTEMAS |
| ECLIPSOFT S.A. | DESARROLLO DE SOFTWARE, PRESTACION DE SERVICIO TELEFONICO E INTERNET |
| COMET GROUP S.A. COMETGROUPSA | DESARROLLO DE PAGINAS WEB Y SOFTWARE |
| INGENIERIA ELECTRONICA Y SISTEMAS INGELSISTEM CIA. LTDA. | ASESORIA TECNICA EN SISTEMAS DE COMPUTACION |
| ARTWARE S.A | COMERCIALIZACION DE SOFTWARE |
| SMARTNET S.A. | CONSULTOR Y DESARROLLADOR DE SOFTWARE |
| CHINA ECUADOR S.A. | IMPORTACION DE SOFTWARE, ASESORIA Y DESARROLLO DE PROYECTOS INFORMATICOS |
| KUO CHIN LIAO LIU << YUKO TECHNOLOGY >> | SERVICIOS Y VENTA DE COMPUTADORAS Y SOFTWARE |
| QUALITYSOFT INNOVATIVE SOLUTIONS Q.S.S CIA.LTDA. | CONSULTOR Y DESARROLLADOR DE SOFTWARE INTERNACIONAL |
| ONLY CONTROL S.A. CONONLY | SOLUCIONES DE SOFTWARE Y HARDWARE DE IDENTIFICACION DE SERES HUMANOS |
| INNOVASYSTEM ECUADOR S.A. | ASESORIA, DISEÑO, DESARROLLO, MANTENIMIENTO DE SITIOS |

| | |
|---|---|
| IMPORTADORA COMERCIAL OCHOA S.A. I.C.O. S.A. | IMPORTACION Y COMERCIALIZACION DE PRODUCTOS DE SEGURIDAD ELECTRONICA |
| AURORASI S.A. | ASESORIA EN INFORMATICA |
| DATASOLUTIONS S.A. | SERVICIOS DE ARCHIVO, ORGANIZACIÓN, DIGITALIZACIÓN, CONSERVACIÓN, CUIDADO Y DESTRUCCIÓN DE DOCUMENTOS. |
| CENTRO DE SERVICIOS INFORMATICOS S.A. CENINFOR | ANALISIS, DISEÑO Y PROGRAMACION DE SISTEMAS |
| CENTRO DE ENTRENAMIENTO CERTIFICADO DE TECNOLOGIA INFORMATICA CENTROTECNI S.A. | CAPACITACION Y CONSULTORIA |
| BISMARK S.A. | SOLUCIONES TELECOM |
| DISTRIBUCION Y ASESORIA TECNOLOGICA DYATECHNOLOGY S.A. | DISTRIBUCION DE SISTEMAS Y EQUIPOS COMPUTARIZADOS |
| MIZUR S.A. | PRODUCCION DE AUDIO Y VIDEO, DESARROLLO DE PAGINAS WEB |
| GLOBALMARMER S.A. CORPORACIÓN GLOBAL DE ASESORES | ASESORIA CONTABLE, TRIBUTARIA Y FINANCIERA - AUDITORIA EXTERNA E INTERNA. / VENTA DE SOFTWARE Y HARDWARE |
| SWITCHORM S.A. | ANALISIS, DISEÑO, PROGRAMACION, PROCESAMIENTO T¡Y TABULACION DE DATOS |
| SOLUCIONES ESPECIALIZADAS DE INGENIERIA EN TELEMATICA S.A. SESTEL | DISEÑO Y PROGRAMACION DE SISTEMAS |
| MARIO ROBERTO ORTEGA CORONEL | VENTAS AL POR MAYOR Y MENOR DE MATERIALES ELECTRICOS, PROGRAMAS DE COMPUTACION |
| PRODUCCIONES DIGITALES IMAGETECH C. LTDA. | SERVICIOS DE ELABORACION DE DISEÑO DE PAGINAS WEB |
| SOLUCIONES INFORMATICAS DEL ECUADOR SINFOEC S.A. | ASESORIA , MANTENIMIENTO Y DESARROLLO DE SOFTWARE |
| INMOBILIARIA UNICORNIO S.A. UNINMOB | ACTIVIDADES DE SERVICIOS ESPECIALIZADOS EN COMPUTACION |

| | |
|---|---|
| EXPOTECH S.A. | DESARROLLO DE SISTEMAS |
| TECHNOLOGICAL SOLUTIONS INDUSTRIES S.A. | ANALISIS, DISEÑO Y PROGRAMACION DE SISTEMAS |
| CARLOS MANUEL QUINDE ERAS | SERVICIOS DE REDES Y COMUNICACIONES |
| ALNOBEL S.A. | VENTA AL POR MAYOR DE MAQUINARIA Y EQUIPO DE OFICINA, INCLUSO PARTES Y PIEZAS |
| EIKON S.A. | DESARROLLADOR DE SOFTWARE |
| ROSADO SANCHEZ COMPANY SOLUCIONES FUTURAS S.A. | VENTA AL POR MENOR DE PROGRAMAS DE COMPUTADORA |
| DISTRIBUIDORA RENE DIRES S.A. | ELABORACION DE PROGRAMAS DE COMPUTACION Y SOFTWARE |
| TELEFIRST S.A. | DESARROLLO DE PROGRAMAS PARA COMPUTADORAS |
| VIAMATICA S.A. | COMERCIALIZACION DE SISTEMAS Y PROGRAMATICO INFORMATICO |
| ALTA TECNOLOGIA EN SOFTWARE S.A. ALTECSOFT | CONSULTOR Y DESARROLLADOR DE SOFTWARE |
| T.S.S. TECNOLOGIA SOFTWARE Y SERVICIOS S.A. | ANALISIS, DISEÑO Y PROGRAMACION DE SISTEMAS |
| TELEBAK S. A. | DIGITALIZACION DE DATOS Y VENTA DE SOLUCIONES DIGITALES |
| SISTEMAS DE EXCELENCIA SYSTEXEC S.A. | SOFTWARE / CONSULTOR Y DESARROLLADOR DE SOFTWARE |
| JOHNNY ANTONIO SEGARRA MEDINA <<SEGATECH>> | CONSULTORIA INFORMATICA |
| NOVATECH SISTEMAS DE MEJORAMIENTO CONTINUO CIA. LTDA. | CONSULTOR Y DESARROLLADOR DE SOFTWARE |
| WISE COMPUTER DECISIONS S. A. | CONSTULTOR Y DESARROLLADOR DE SOFTWARE |
| SOLUCIONES INTEGRADAS S.A. SOLINTEGRA | ACTIVADES RELACIONADAS CON EL ANALISIS CON EL ANALISIS DISEÑO Y PROGRAMACION DE SISTEMAS |
| FENIX INTERNATIONAL S.A. FINTERSA | DISEÑO Y PROGRAMACION DE SISTEMAS DE COMPUTACION |
| MICROSERVICES S.A. | SERVICIO EN SOPORTE TECNICO, REDES, COMPUTADORAS Y PERIFERICO |

| | |
|---|---|
| | CONEXO |
| NUEVOS SISTEMAS, IMPORTACIONES Y MAQUINARIAS NSIM CIA. LTDA. | COMERCIALIZACION DE SOFTWARE Y PRESTACION DE SERVICIO DE ARRENDAMIENTO DEL SOFTWARE |
| SYDFAST S.A. | CONSULTOR Y DESARROLLADOR DE SOFTWARE |
| AVP SISTEMAS S.A. | PRESTACION DE SERVICIOS DE SOFTWARE Y ANTIVIRUS |
| CORPORACION LATINOAMERICANA DE SOFTWARE SOCIEDAD ANONIMA (C.O.R.L.A.S.O.S.A.) | VENTA DE LICENCIA ORACLE, SOFTWARE Y DESARROLLO DE SOFTWARE |

**Anexo 11. Compañías de tecnología, afiliadas a la CCG**
**Elaborado por: Autores del proyecto**

| | |
|---|---|
|  | **CONGRESOS DE SEGURIDAD INFORMATICA ECCERT 2011** |
| **PROGRAMA DE LAS TEMATICAS A TRATAR** | |
| **ENERO** | 1er. Congreso de Seguridad Informática. |
| | Entre los diversos temas que se tratarán en este congreso destacan:<br>• Hacking, cracking, ingeniería inversa, debugging, hooking, fuzzing, exploiting.<br>• Herramientas o técnicas defensivas y ofensivas punteras.<br>• Seguridad en "la nube", seguridad y hacking en entornos virtuales, productos y servicios en "la nube"<br>• Ciencia forense, investigación y técnicas anti forense.<br>• Redes, protocolos y hacking de capas 2 y 3, encapsulación. |
| **SEPTIEMBRE** | 2do. Congreso de Seguridad Informática. |
| | • Seguridad en una Infraestructura Pública de TI<br>• Seguridad en Servicios Públicos<br>• Políticas Públicas sobre Seguridad de la Información<br>• Seguridad en el Gobierno Electrónico”<br>• Seguridad en Comercio Electrónico<br>• Tecnologías de Voto Electrónico<br>• Votaciones Electrónicas y Privacidad de la Información<br>• Protocolos de Seguridad<br>• Seguridad en Redes y Comunicaciones<br>• Prevención y Detección de Intrusos<br>• Seguridad en la Web<br>• Modelos de Gestión de la Seguridad de Información<br>• Seguridad en Sistemas de Información<br>• Auditoría y Seguridad |

**Anexo 12. Posibles Congresos y temas a tratar**
**Elaborado por: Autores del proyecto**

| Leyes en la Legislación del Ecuador |
| --- |
| **Ley Orgánica de Transparencia y Acceso a la Información Pública** |
| La ley establece que todas las instituciones del sector público pongan a disposición de la ciudadanía, el libre acceso a la información institucional (estructura orgánica, bases legales, regulaciones, metas, objetivos, presupuestos, resultados de auditorías, etc.), a través de sus sitios web, bajo este mismo contexto las disposiciones contenidas en la Constitución Política del Ecuador vigente. |
| **Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos** |
| La Ley contiene los principios jurídicos que regirán las transmisiones de los mensajes de datos. Se le concede pleno valor y eficacia jurídica a los mensajes de datos, tanto a su información como a su contenido general; la interpretación de la Ley y el ejercicio de la Propiedad Intelectual se rigen por la legislación ecuatoriana y por los tratados internacionales incorporados al cuerpo legal ecuatoriano. Se protege la confidencialidad de los mensajes de datos en sus diversas formas, señalando lo que se entenderá por tal concepto y su violación. |
| **Ley de Propiedad Intelectual** |
| Dar a conocer la importancia que tiene la Propiedad Intelectual en el Ecuador y su debida aplicación en los sectores económico, industrial, intelectual y de investigación, debe ser tarea no sólo del profesional del derecho, sino de los industriales y empresarios, de las instituciones públicas y privadas, de los centros superiores de estudios e inclusive del propio estado ecuatoriano. |
| **Ley Especial de Telecomunicaciones** |
| La Ley Especial de Telecomunicaciones tiene por objeto normar en el territorio nacional la instalación, operación, utilización y desarrollo de toda transmisión, emisión o recepción de signos, señales, imágenes, sonidos e información de cualquier naturaleza por hilo radioelectricidad, medios ópticos y otros sistemas electromagnéticos. |

**Anexo 13. Leyes en la Legislación del Ecuador**
**Elaborado por: Autores del proyecto**

## BIBLIOGRAFÍA


- CLCERT, Manual de Gestión de Incidentes de Seguridad Informática, www.proyectoamparo.net, Octubre del 2010
- Ec-Council , Computer Forensics - Investigation Procedures and Response, Cengage Learning, Diciembre del 2010
- Hossein Bidgoli, Handbook of information security Volume 3, California State University Bakersfield, Diciembre del 2010
- Chris Prosise - Kevin Mandia, Incident response and computer forensics, McGraw-Hill, Diciembre del 2010
- Carnegie Mellon University, Steps for Creating National CSIRTs, http://www.cert.org/cert/, Septiembre del 2010
- Forum for Incident Response and Security Teams, FIRST, http://www.first.org/, Septiembre del 2010
- Secretaría de la Función Pública de Argentina, Arcert, http://www.arcert.gov.ar/, Septiembre del 2010
- U. de Chile, Clcert, http://www.clcert.cl/, Septiembre del 2010
- Cámara de Comercio de Guayaquil, http://www.lacamara.org, Octubre del 2010
- Segu-Info, Seguridad de la información, http://www.segu-info.com.ar/, Septiembre del 2010
- Derechoecuador, Revista Judicial, http://www.derechoecuador.com, Noviembre del 2010