



Maestría en

CIBERSEGURIDAD

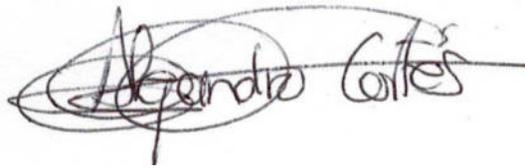
Proyecto previo a la obtención del título de Magíster en Ciberseguridad

AUTOR: Ing. Darwin Fabrissio Vargas Lara
Ing. Daniel Fernando Quinatoa Guerra
Ing. Ricardo Javier Bravo Sandoval
Ing. Andrés Alejandro Bravo Sandoval
Lic. Juan Pablo Vega Guillén
TUTOR: Ing. Alejandro Cortés López

Elaboración de un plan para la creación de la Asociación de Especialistas en Ciberseguridad del Ecuador “AECIE”.

APROBACIÓN DEL TUTOR

Yo, **Alejandro Cortés**, certifico que conozco a los autores del presente trabajo siendo los responsables exclusivos tanto de su originalidad y autenticidad, como de su contenido.

A handwritten signature in black ink that reads "Alejandro Cortés". The signature is written in a cursive style with a horizontal line extending to the right.

Alejandro Cortés
DIRECTOR DE TESIS

CERTIFICACIÓN DE AUTORÍA

Yo, **DARWIN FABRISSIO VARGAS LARA**, declaro bajo juramento que el trabajo aquí descrito es de mi autoría; que no ha sido presentado anteriormente para ningún grado o calificación profesional y que se ha consultado la bibliografía detallada.

Cedo mis derechos de propiedad intelectual a la Universidad Internacional del Ecuador, para que sea publicado y divulgado en Internet, según lo establecido en la Ley de Propiedad Intelectual, su reglamento y demás disposiciones legales.



Firmado electrónicamente por:

**DARWIN
FABRISSIO
VARGAS LARA**

.....

ING. DARWIN FABRISSIO VARGAS LARA

CERTIFICACIÓN DE AUTORÍA

Yo, **DANIEL FERNANDO QUINATOA GUERRA**, declaro bajo juramento que el trabajo aquí descrito es de mi autoría; que no ha sido presentado anteriormente para ningún grado o calificación profesional y que se ha consultado la bibliografía detallada.

Cedo mis derechos de propiedad intelectual a la Universidad Internacional del Ecuador, para que sea publicado y divulgado en Internet, según lo establecido en la Ley de Propiedad Intelectual, su reglamento y demás disposiciones legales.



Firmado electrónicamente por:
**DANIEL FERNANDO
QUINATOA GUERRA**

.....
ING. DANIEL FERNANDO QUINATOA GUERRA

CERTIFICACIÓN DE AUTORÍA

Yo, **RICARDO JAVIER BRAVO SANDOVAL**, declaro bajo juramento que el trabajo aquí descrito es de mi autoría; que no ha sido presentado anteriormente para ningún grado o calificación profesional y que se ha consultado la bibliografía detallada.

Cedo mis derechos de propiedad intelectual a la Universidad Internacional del Ecuador, para que sea publicado y divulgado en Internet, según lo establecido en la Ley de Propiedad Intelectual, su reglamento y demás disposiciones legales.



Firmado electrónicamente por:
**RICARDO JAVIER
BRAVO SANDOVAL**

.....

ING. RICARDO JAVIER BRAVO SANDOVAL

CERTIFICACIÓN DE AUTORÍA

Yo, **ANDRÉS ALEJANDRO BRAVO SANDOVAL**, declaro bajo juramento que el trabajo aquí descrito es de mi autoría; que no ha sido presentado anteriormente para ningún grado o calificación profesional y que se ha consultado la bibliografía detallada.

Cedo mis derechos de propiedad intelectual a la Universidad Internacional del Ecuador, para que sea publicado y divulgado en Internet, según lo establecido en la Ley de Propiedad Intelectual, su reglamento y demás disposiciones legales.



Firmado electrónicamente por:
**ANDRES ALEJANDRO
BRAVO SANDOVAL**

.....

ING. ANDRÉS ALEJANDRO BRAVO SANDOVAL

CERTIFICACIÓN DE AUTORÍA

Yo, **JUAN PABLO VEGA GUILLÉN**, declaro bajo juramento que el trabajo aquí descrito es de mi autoría; que no ha sido presentado anteriormente para ningún grado o calificación profesional y que se ha consultado la bibliografía detallada.

Cedo mis derechos de propiedad intelectual a la Universidad Internacional del Ecuador, para que sea publicado y divulgado en Internet, según lo establecido en la Ley de Propiedad Intelectual, su reglamento y demás disposiciones legales.



Firmado electrónicamente por:
**JUAN PABLO
VEGA**

.....

LIC. JUAN PABLO VEGA GUILLÉN

DEDICATORIA

Desde que tengo uso de razón, en mi vida siempre existió una persona que guio mi camino y logro transformar mi vida, alguien a quien siempre quise igualar, teniendo en cuenta que la vara era muy alta, y que hasta el final de sus días me cuidó como al primero de sus hijos, te dedico a ti Fico hermano mío este trabajo y esta maestría, ya que, debido a tu repentina partida, el refugiarme en los libros, fue lo único que pudo por momentos sacar de mi cabeza el saber que nunca más te volveré a ver.



Firmado electrónicamente por:
**DARWIN
FABRISSIO
VARGAS LARA**

.....

ING. DARWIN FABRISSIO VARGAS LARA

DEDICATORIA

El presente trabajo está dedicado a mis padres quienes me enseñaron que el mejor conocimiento que una persona puede tener es el adquirido por sí mismo. También se lo dedico a mi esposa Alicia y mis queridos hijos, Paulo y Doménica, quienes son mi motor y mis fuerzas para seguir cada día.

También dedico a todas las personas especiales que me acompañaron en esta etapa y que contribuyeron a mi formación tanto a nivel profesional como personal.



Firmado electrónicamente por:
**DANIEL FERNANDO
QUINATOA GUERRA**

.....

ING. DANIEL FERNANDO QUINATOA GUERRA

DEDICATORIA

A Dios quien me ha brindado la fortaleza, la salud y la vida para continuar con mis sueños.

Al motor de mi vida mi hijo Kevin Joel quien es mi inspiración más grande en todas mis metas para seguir avanzando y cumplir los sueños que me he trasado en mi vida, y darle así el ejemplo de cualquier sueño es posible con el sacrificio y dedicación necesaria.

A mis amados padres Maria y Luis quienes con su ejemplo me han enseñado que, con esfuerzo, perseverancia y dedicación se puede lograr las metas, por más duras estas sean.

Finalmente quiero dedicar esta tesis a mi gran amigo y guía Fabrissio, por extender su mano en momentos difíciles y por haberme motivado a tener este sueño, el tiempo avanza y nunca se detiene al ayer no existe solo el presente para forjar un futuro prometedor.



Firmado electrónicamente por:
**RICARDO JAVIER
BRAVO SANDOVAL**

.....

ING. RICARDO JAVIER BRAVO SANDOVAL

DEDICATORIA

La Presente Dedicatoria está dirigida primeramente a Dios, por haberme dado la capacidad de la razón, en la toma de mis decisiones, a mis padres Rosa Sandoval y Luis Bravo, que sin el apoyo incondicional de ellos, no estaría en donde me encuentro ahora, gracias a las enseñanzas y modales que me inculcaron desde pequeño me han formado para ser un hombre de bien, y encaminar mi futuro, a mis hermanos Diana y Ricardo, que gracias al apoyo incondicional que tenemos entre hermanos me ha permitido conseguir ciertos logros que me los eh propuesto.

A mi hermano que siempre ha estado junto a mí y brindándome su apoyo, muchas veces poniéndose en el papel de padre.



Firmado electrónicamente por:
**ANDRES ALEJANDRO
BRAVO SANDOVAL**

.....
ING. ANDRÉS ALEJANDRO BRAVO SANDOVAL

DEDICATORIA

Esta maestría y tesis quiero dedicar a mi papito Jorge y a mi mamita Paty, quienes con su amor incondicional y apoyo constante en las diferentes etapas de mi vida han hecho de mi un hombre de bien, además a mi hermano Jorge David quien fue pilar fundamental y un ángel para mí y mi familia, ahora ya se encuentra en un lugar mejor con la bendición de Dios.

A mi bella esposa Paola, mi hermosa hija Doménica y mi risueño hijo Leonardo por ser mi motor principal para cada amanecer ser un mejor esposo, un mejor padre, un mejor hijo y un mejor ser humano.



Firmado electrónicamente por:

**JUAN PABLO
VEGA**

.....

LIC. JUAN PABLO VEGA GUILLÉN

AGRADECIMIENTO

A mi amada Esposa, a mis hijos, por su infinito amor y paciencia en esta temporada tan difícil que hemos pasado, ya que gracias a ustedes he podido lograr culminar con éxito esta etapa de mi vida. Agradezco a mi familia por siempre motivarme a crecer profesionalmente y como ser humano, a mis compañeros y amigos por esas jornadas de estudio, a mis maestros por todos los conocimientos por ellos impartidos sin ningún egoísmo, y a la Universidad Internacional del Ecuador por apostar a este tipo de carreras que hacen que los profesionales en esta rama demos un paso hacia la excelencia.



.....

ING. DARWIN FABRISSIO VARGAS LARA

AGRADECIMIENTO

A Dios, que en este año me fortaleció en los momentos más difíciles de esta exigente, pero gratificante profesión, y que me permitió, bajo sus bendiciones, tener salud y disfrutar de los frutos de mi arduo trabajo.

A mis padres y hermanos, que me han apoyado y ayudado en cada paso que doy en esta vida.

A mis amigos de la vida, que me motivaron a seguir esta Maestría.



Firmado electrónicamente por:
**DANIEL FERNANDO
QUINATOA GUERRA**

.....

ING. DANIEL FERNANDO QUINATOA GUERRA

AGRADECIMIENTO

A mi hijo quien es mi motivo principal de seguir avanzando por cumplir metas y mejorar en la parte espiritual, personal, profesional y así pueda ver un ejemplo de que todo es posible, con esfuerzo, tiempo y dedicación.

A mi madre, quien siempre ha estado allí para darme el aliento necesario para seguir avanzando, con su apoyo incondicional ha sido posible alcanzar cada uno de los sueños que he puesto en mi camino, mi padre con su fortaleza que a pesar de las circunstancias que existan se puede cumplir los objetivos planteados.

A mis amigos quienes, con su iniciativa de iniciar este proceso, puedo estar en estas instancias de culminar este gran paso a nivel educativo y profesional.



Firmado electrónicamente por:
**RICARDO JAVIER
BRAVO SANDOVAL**

.....
ING. RICARDO JAVIER BRAVO SANDOVAL

AGRADECIMIENTO

En primer lugar doy infinitamente gracias a Dios, por haberme dado fuerza y valor para culminar esta etapa de mi vida.

Agradezco también la confianza y el apoyo brindado por parte de mi madre, que sin duda alguna en el trayecto de mi vida me ha demostrado su amor, corrigiendo mis faltas y celebrando mis triunfos.

A mi hermano, que con sus consejos me ha ayudado a afrontar los retos que se me han presentado a lo largo de mi vida.

A mi padre, que siempre lo he sentido presente en mi vida. Y sé que está orgulloso de la persona en la cual me he convertido.



Firmado electrónicamente por:
**ANDRES ALEJANDRO
BRAVO SANDOVAL**

.....

ING. ANDRÉS ALEJANDRO BRAVO SANDOVAL

AGRADECIMIENTO

Agradezco a papito Dios por darme la fortaleza y la bendición de poder culminar y alcanzar nuevas metas con salud y en unión, a mis Padres quienes fueron mis primeros maestros de vida, a mi bella esposa Paola por su apoyo y amor incondicional durante el proceso de mi maestría. Además, agradecer a mi Universidad Internacional del Ecuador, a sus excelentes docentes y tutores quienes con su profesionalismo y calidez humana han logrado en mi ser un mejor profesional y como olvidar a mis compañeros por su valiosa amistad y apoyo incondicional.



Firmado electrónicamente por:
**JUAN PABLO
VEGA**

.....

LIC. JUAN PABLO VEGA GUILLÉN

RESUMEN

Con el avance de las telecomunicaciones, la informática y la globalización, la cantidad de delitos informáticos han aumentado en proporción exponencial, tema que no es indiferente en el día a día de los seres humanos ya que la mayor parte de los mismos manejan un smartphone o computador, y tomando en cuenta que estamos en un proceso postpandemia en el cual la virtualidad jugó un papel muy importante para que la mayoría de empresas sigan a flote, generó un mayor tráfico en los servicios de internet y telecomunicaciones, siendo un mercado muy apetecido para los ciberdelincuentes, es así, que la necesidad de optar por servicios en los cuales las empresas puedan sentirse tranquilas que su información está correctamente resguardada y que se tiene un plan de respuesta en caso de algún imprevisto, la seguridad informática se ha convertido en el punto de lanza de las áreas de TI de todas las organizaciones. No todas las empresas optaron por invertir en ciberseguridad y fueron víctimas de los ciberdelincuentes; y para, generar un correcto plan de protección se tiene la obligación de analizar e identificar en que se falló para llegar a este punto.

PALABRAS CLAVE

Ciberseguridad, ciberdelincuencia, informática forense, AECIE, estrategia nacional, delito, víctima, usuarios, cibernéticos, ciberespacio, seguridad, análisis, vulnerabilidades, pen test, peritos forenses, normativa legal, información, Internet, sistemas, redes, desarrollo, diseño, plan, comunicación, incidentes, TI, necesidades, calidad, recursos, gestión, web, empresa.

ABSTRACT

With the advancement of telecommunications, information technology and globalization, the number of computer crimes has increased exponentially, an issue that is not indifferent in the day to day of human beings since most of them handle a smartphone or computer, and taking into account that we are in a post-pandemic process in which virtuality played a very important role for most companies to stay afloat, it generated more traffic in internet and telecommunications services, being a very desirable market for cybercriminals, it is thus, that the need to opt for services in which companies can feel calm that their information is properly protected and that there is a response plan in case of any unforeseen event, computer security has become the point spearhead of the IT areas of all organizations. Not all companies chose to invest in cybersecurity and fell victim to cybercriminals; and in order to generate a correct protection plan, it is necessary to analyze and identify what went wrong to reach this point.

KEY WORDS

Cybersecurity, cybercrime, computer forensics, AECIE, national strategy, crime, victim, users, cyberspace, security, analysis, vulnerabilities, pent test, forensic experts, legal regulations, information, Internet, systems, networks, development, design, plan, communication, incidents, IT, needs, quality, resources, management, web, company.

TABLA DE CONTENIDOS**Tabla de contenido**

CAPÍTULO 1	6
Introducción	6
Caso de estudio/Problema de investigación	8
Definición del problema.....	8
Objetivos	8
CAPÍTULO 2	10
Metodología	10
Método Inductivo.....	10
Método Analítico.	10
Desarrollo.....	11
Proceso de la creación de la asociación	11
Requisitos para constituir una asociación en el Ecuador	17
Conformación de la asociación	18
Organigrama de la directiva.....	18
CAPÍTULO 3	20
Plan de Concientización	20
Introducción	20
Objetivo.....	20
Alcance.....	20
Fases del Plan.....	21
Fases de Diseño.....	21
Planificación.....	22
Tareas de la etapa de planificación	22
Capacitar	22
Sensibilizar.....	22
Entregar.....	22
Fase de desarrollo.....	22
Realizar copias de seguridad.....	23

Fase de implementación.....	27
Fase de Mejoramiento.....	27
Objetivos de la Mejora.....	28
Directorio de Software Forense	30
Adquisición física:	31
Adquisición del sistema de ficheros.....	31
Adquisición lógica.	32
Caine	32
Wireshark	37
Para qué sirve Wireshark	38
Ventajas y desventajas de Wireshark.....	40
Desventaja:	40
Uso práctico y sencillo de Wireshark	40
Paladin Forense Suite.....	41
Kit Passware Forense	45
Crowdresponse:.....	46
Ejecución de análisis YARA.....	46
Recopilación de información adicional.....	49
Ventajas de los módulos de CrowdResponse:	49
Exiftool:	52
Para qué sirve ExifTool.....	53
Características de ExifTool.....	53
Ventajas de uso de ExifTool	53
Desventajas de uso de ExifTool.....	54
Autopsy	54
Ventajas de usar Autopsy:.....	56
CAPÍTULO 4.....	57
CONCLUSIONES	57
REFERENCIAS.....	59
APÉNDICES.....	62

LISTA DE TABLAS

Tabla 1	Trámites para formar la Asociación.....	17
Tabla 2	Plan de Capacitación y Sensibilización	26

LISTA DE FIGURAS

Figura 1	Portal Para el Proceso Gestión de la Creación de la Asociación.....	13
Figura 2	Datos del Solicitantes en el Formulario de Trámite de Creación de la Asociación	14
Figura 3	Validador del Formulario de Trámite de Creación de la Asociación.....	14
Figura 4	Datos del Trámite Para el Formulario de Trámite de Creación de la Asociación	15
Figura 5	Aceptación de Responsabilidad Para Continuar con el Formulario de Trámite de Creación de la Asociación	15
Figura 6	Datos del Trámite en el Formulario de Trámite de Creación de la Asociación	16
Figura 7	Organigrama de la Directiva de la Asociación “AECIE”	18
Figura 8	Fases del Plan de Concientización	21
Figura 9	Proceso de búsqueda URL.....	41
Figura 10	Regla que Identifica Textos y Expresiones Regulares	46
Figura 11	Ejecución de Script en base a Parámetros de Texto y Salida XML	47
Figura 12	Detección de Firma YARA en un Archivo y Proceso Denominado trksrv.exe	47
Figura 13	Golpe de Firma YARA en msinit.exe	49
Figura 14	Comandos Para Generar Informes Formato XML	51
Figura 15	Resultado de Informe Sobre Procesos Sospechosos	51
Figura 16	#Dirlist Módulo que Proporciona Detalles Para el Archivo Identificado por YARA	52

LISTA DE APÉNDICES

Apéndice A Modelo de Estatuto de la Asociación Sin Fines de Lucro 62

Apéndice B Formulario de Acceso a la Biblioteca Técnica..... 87

CAPÍTULO 1

Introducción

Con vertiginoso avance de la tecnología, tanto en el ámbito profesional informático, telecomunicaciones y en el ámbito del Internet de las cosas (IoT), ha despertado que ciertos grupos criminales monetice estos servicios y plataformas de forma ilícita para obtener ganancias. Por otro lado, el mundo actual ha adoptado la virtualidad como una herramienta del diario vivir, debido a la pandemia del COVID-19, la cual obligo a la mayoría de los usuarios a aumentar los accesos a la red, es por esto que los ciberdelitos están en aumento en el Ecuador, representando del total de todos los delitos un porcentaje que sigue en crecimiento.

Revisando las estadísticas, emitidas por la Fiscalía General del Estado (FGE), desde el inicio de la pandemia del COVID-19, la cantidad de ciberdelitos denunciados se han duplicado, ya que el ciberdelito también se está volviendo más sofisticado, complejo y organizado, considerado que el cibercrimen ataca principalmente a las transacciones, por lo que atiende a una tendencia global.

Cabe indicar que, de la literatura existente referente a seguridad cibernética, está claro que los usuarios son el eslabón más débil y vulnerable dentro de la estructura organizacional informática y son los más propensos a convertirse en víctimas del delito cibernético, debido a la baja alfabetización digital y la falta de la concientización sobre ciber seguridad. Tomando en cuenta que, las víctimas de los ciberdelitos normalmente no tienen conciencia del riesgo que representa en sus activos las brechas de seguridad, en función del desconocimiento y falta de confianza de emitir una denuncia sobre esta forma de acciones ilícitas, ya que a menudo la reputación de la Función Judicial no es del agrado de los usuarios, debido a su limitada capacidad y la lentitud en su respuesta ante estas investigaciones y enjuiciamientos.

Como resultado, los delitos cibernéticos a menudo no se denuncian debido a todos estos factores. De manera similar, los datos del ministerio de gobierno muestran que el fraude informático, el robo de identidad y las filtraciones de datos personales son los delitos cibernéticos más comunes que afectan a los ecuatorianos. La pornografía infantil ocupa el primer lugar entre los delitos relacionados con el contenido. La definición legal de delito cibernético en el marco legal actual puede considerarse obsoleta, lo que indica margen de mejora.

Sin embargo, el Ecuador se encuentra actualmente en proceso de adherirse al Convenio de Budapest sobre la Relevancia y Situación del Delito Cibernético, por lo que se esfuerza por mejorar su capacidad para combatir el delito cibernético a través de la cooperación internacional, fortaleciendo las técnicas de investigación y cooperación interinstitucionales. El proceso de adhesión requiere la aplicación de las disposiciones del tratado en el derecho interno del Ecuador, ya que es miembro de La Comunidad de Policías de América “AMERIPOL” y la Organización Internacional de Policía Criminal “INTERPOL”, con acceso a intercambio de información de manera útil y oportuna.

Como dato de interés se conoce que la Unidad Nacional de Ciberdelitos, que se encuentra bajo la estructura orgánica de la Dirección General de Investigación de la Policía Nacional del Ecuador, lleva más de una década de operación y ha adquirido una notable especialización en el campo de la investigación digital, sin embargo carece de logística y recursos humanos que le permitan evolucionar de forma sostenible, por lo que uno de los objetivos Asociación de Especialistas en Ciberseguridad en el Ecuador “AECIE”, es brindar personal capacitado, y a su vez, capacitar al personal profesional en

Ciberseguridad ya sea en el sector público o privado siendo un vínculo entre las dos sectores.

La aplicación de la ley no puede actuar sin una base jurídica clara, por lo que deben definirse claramente las funciones y los mandatos establecidos de los diversos agentes encargados de combatir la ciberdelincuencia (Fuerzas Armadas, Policía Nacional, Fiscalía General del Estado y el Sistema Judicial). En el transcurso de los últimos años se ha evidenciado el creciente volumen e impacto causado por la ciberdelincuencia, sin embargo, la capacidad de los organismos encargados de hacer cumplir la ley y orden de este delito ha involucionado ya que no cuenta con el personal profesional calificado en ciberseguridad, ciberdefensa y la falta de asignación presupuestaría para este rubro. (MINTEL, 2022, pág. 28)

Caso de estudio/Problema de investigación

Definición del problema

Dentro del Ecuador no existe una agremiación legalmente constituida, en la cual se agrupe a los profesionales que se dedican a la ciberseguridad explícitamente a la informática forense, con este antecedente no se cuenta con una real base de datos de los profesionales que puedan dar soluciones a los problemas sugeridos en esta rama.

Objetivos

- Generar un plan que permita la conformación de una Asociación de Especialistas en Ciberseguridad en el Ecuador.
- Diseñar los servicios académicos y prácticos referente a la ciberseguridad con los cuales contarán los miembros de la Asociación de Especialistas en Ciberseguridad en el Ecuador.

- Establecer campañas que permitan la concientización de los usuarios a nivel empresarial, académico y social en temas relacionados con la ciberseguridad.

CAPÍTULO 2

Metodología

Durante el trabajo de campo realizado en la Asociación de Especialistas en Ciberseguridad del Ecuador “AECIE”, se utilizaron métodos como el inductivo y analítico, tomando como referencia ejercicios metodológicos similares los cuales fueron adaptados a la realidad del estudio. Para ello establecemos los siguientes:

Método Inductivo.

El método inductivo es muy importante en nuestra investigación, ya que se basa principalmente en la observación de las actividades que se ejecutan en la asociación, además permite el nivel de visita de usuarios que adquieren los productos y servicios de los agremiados para el cumplimiento de las políticas y regulaciones a las que se rigen como profesionales de ciberseguridad.

Método Analítico.

Así mismo el Método analítico, es muy relevante para nuestra investigación, ya que consiste en la desmembración de sus partes o elementos para observar las causas, la naturaleza y los efectos es decir el impacto económico que se genera en los diferentes servicios que la asociación. Este método nos permite conocer más sobre las principales falencias que posee la asociación, con lo cual se puede: explicar y comprender mejor el comportamiento de los usuarios de los bienes y servicios de ciberseguridad.

(GONZÁLEZ LUCAS, 2013, pág. 71)

Desarrollo

Diseño del plan para la conformación de una Asociación de Especialistas en Ciberseguridad en el Ecuador

Proceso de la creación de la asociación

Misión

Planificar y adherir los entornos públicos y privados, para el fortalecimiento informático que, a través de diferentes líneas de acción, aportarán el máximo conocimiento sobre los desafíos a la Ciberseguridad y la oportunidad de prever los posibles ataques con planes articulados a través del Comité Nacional de Ciberseguridad.

Visión

Fortalecer los métodos de implementación, ejecución de la “ESTRATEGIA NACIONAL DE CIBERSEGURIDAD DEL ECUADOR” en la consecución de sus objetivos, mediante el establecimiento de alianzas público-privadas que permitan, directa o indirectamente, dotar de una mayor protección a la sociedad ecuatoriana en el ámbito del ciberespacio.

Valores

- Integración en el “Comité Nacional de Ciberseguridad del Ecuador”.
- Transparencia y accesibilidad por todas las partes interesadas.
- Adaptabilidad y flexibilidad, que permitan la articulación a través de la “AECIE” en base a la demanda y a las necesidades identificadas.
- Participación, abierta a todos los interesados con capacidad de aportar, que cumplan los requisitos que se establezcan.

- Multidisciplinar, integrando al menos a representantes de la sociedad civil, expertos independientes, sector público y privado, mundo académico, asociaciones y entidades sin fines de lucro.
- Compromiso, responsabilidad compartida y reciprocidad.
- Priorización de sus actividades, que deberán ser transversales y estratégicas.

Atribuciones y responsabilidades de la asociación

- Brindar una asesoría técnica y legal en delitos cibernéticos
- Auditoría técnica
- Seguridad ofensiva
- Pentesting y análisis de vulnerabilidades
- Promover la formación, capacitación y concienciación
- Análisis de riesgos en infraestructura IT
- Análisis forense y servicio de laboratorio
- Plan de recuperación ante desastres "DRP"
- Promover y difundir el estudio en materia de la Ciberseguridad
- Integrar a profesionales dedicados la Seguridad de la Información

Beneficios de formar parte de la asociación

Los beneficios de los socios adherentes de la “AECIE”, son:

- Formación legal y técnica en Seguridad de la Información,
- Asesorías y Consultorías en materia de ciberseguridad
- Proceso de certificación como Peritos Forenses.
- Usos de los laboratorios de la asociación para las investigaciones forenses.

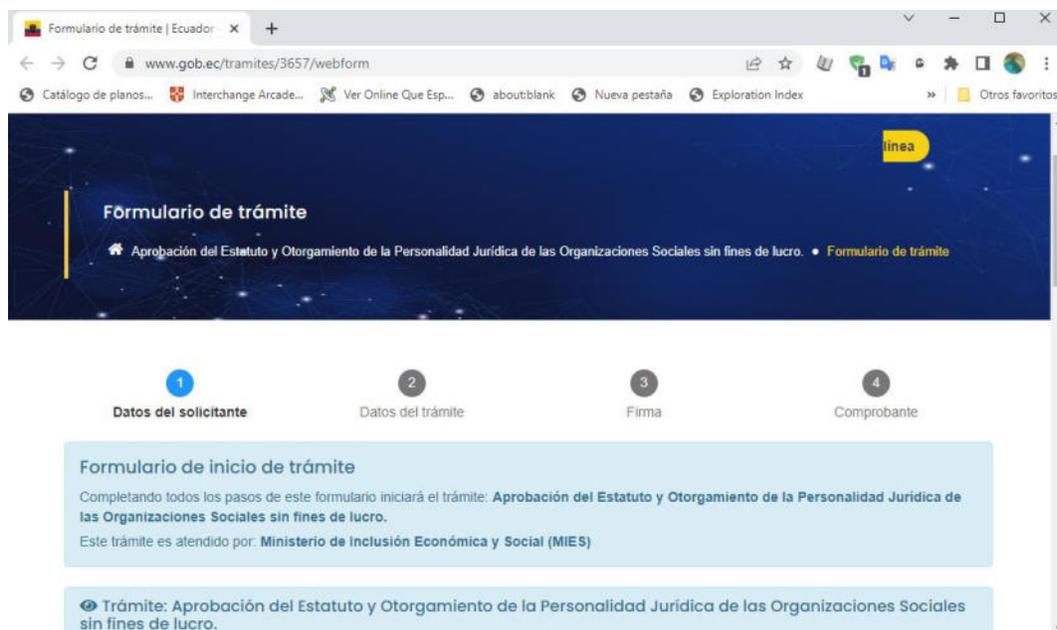
- Acceso al banco de empleo en ciberseguridad.

Proceso Técnico y Legal de la conformación de la Asociación

El primer paso se muestra en la figura 1, y corresponde a llenar el formulario de inicio de trámite, a través del portal único de tramites ciudadanos, el cual se detalla a continuación.

Figura 1

Portal Para el Proceso Gestión de la Creación de la Asociación



Nota: Fuente: (Gobierno Nacional del Ecuador , 2022)

En la figura 2 se muestra la segunda pantalla del proceso de inscripción en línea de la Asociación.

Figura 2

Datos del Solicitantes en el Formulario de Trámite de Creación de la Asociación

https://www.gob.ec/tramites/3657/webform# 80%

Formulario optimizado para Mozilla Firefox
 Estimado usuario este formulario esta optimizado su uso para Mozilla Firefox, si usted no puede realizar correctamente las acciones sugerimos utilizar este navegador para realizar su solicitud.

Tipo de identificación*

Cédula
 Pasaporte
 Registro Único del Contribuyente (RUC)

Número de Cédula*
 1710334838

Correo electrónico*
 aecieec@gmail.com

Teléfono
 0998372787

Política de términos de uso

- Confirмо que estoy autorizado a realizar este trámite y la información proporcionada es veraz y actualizada.
- Usted está de acuerdo con nuestros términos y condiciones, acepto que este sitio recoja información del usuario para poder brindar el servicio.
- Para conocer el tratamiento que damos a su información personal, revise la Política para el tratamiento de datos personales.

Acepto la política de términos de uso *

Continuar >>

NOTA: Fuente: (Gobierno Nacional del Ecuador , 2022)

En la figura 3 se muestra la tercera pantalla del proceso de inscripción en línea de la Asociación, en donde consta el validador del formulario.

Figura 3

Validador del Formulario de Trámite de Creación de la Asociación

Validador de formulario

Por favor ingrese la siguiente información, a fin de continuar con su trámite.

CEDULA

La información solicitada a continuación, es la que consta en la cédula de identidad vigente de: VARGAS LARA DARWIN FABRISIO

Estado civil*
 casado

Fecha de nacimiento*
 25 / 10 / 1978

EMAIL

Se ha enviado un código de confirmación a su correo electrónico: aecieec@gmail.com

Código de confirmación, enviado a su correo electrónico*
 03A548

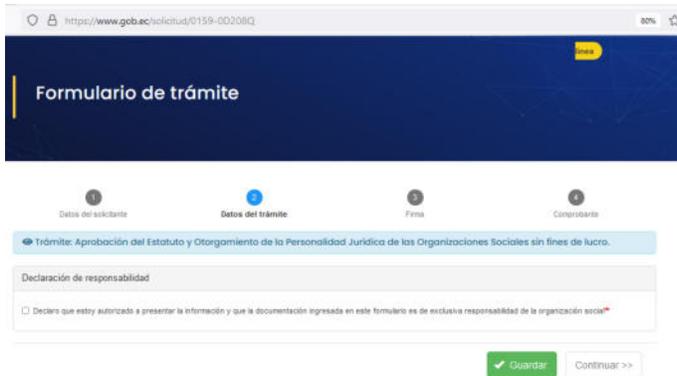
Continuar

NOTA: Fuente: (Gobierno Nacional del Ecuador , 2022)

En la figura 4 se muestra la cuarta pantalla del proceso de inscripción en línea de la Asociación, en donde consta el guardar el formulario.

Figura 4

Datos del Trámite Para el Formulario de Trámite de Creación de la Asociación



NOTA: Fuente: (Gobierno Nacional del Ecuador , 2022)

En la figura 5 se muestra la quinta pantalla del proceso de inscripción en línea de la Asociación, en donde se validan los datos del trámite.

Figura 5

Aceptación de Responsabilidad Para Continuar con el Formulario de Trámite de Creación de la Asociación



NOTA: Fuente: (Gobierno Nacional del Ecuador , 2022)

En la figura 6 se muestra la sexta pantalla del proceso de inscripción en línea de la Asociación, en donde se ingresan fecha, lugar y firma del acta general constitutiva.

Figura 6

Datos del Trámite en el Formulario de Trámite de Creación de la Asociación

Fecha y Lugar de la Firma del Acta General Constitutiva

Fecha*

Provincia*

Cantón*

Ciudad*

Dirección del lugar en que se realizó el Acta General Constitutiva*

Domicilio de la Organización Social (Dirección)*

Declaración de responsabilidad

Utilice el modelo del Estatuto publicado en la página del MIES

Sí No

Anexos / Requisitos

Acta*

Acta de la Asamblea General Constitutiva o copia certificada por el secretario provisional, suscrita por todos los miembros fundadores

No se ha seleccionado ningún archivo.

Requerimientos para subir archivo

Estatuto*

Estatuto de la organización social, certificado por el Secretario provisional

No se ha seleccionado ningún archivo.

Requerimientos para subir archivo

Acreditación de Patrimonio Social*

Declaración Juramentada Firmada por los Miembros Fundadores; o Certificación de la apertura de una cuenta de integración de Capital o apertura de una cuenta Bancaria de cualquier Instituciones Financiera (no existe montos mínimos).

No se ha seleccionado ningún archivo.

Requerimientos para subir archivo

NOTA: Fuente: (Gobierno Nacional del Ecuador , 2022)

Requisitos para constituir una asociación en el Ecuador

- Registro de la directiva de la asociación con la voluntad de 5 personas mínimo.
- Reglamento para la exclusión o inclusión de los miembros
- Estatuto de la Asociación
- Disolución y liquidación voluntaria

En la tabla 1 se expone los requisitos por trámite a realizarse, para todos los procesos de administración de una asociación sin fines de lucro.

Tabla 1

Trámites para formar la Asociación

TRAMITE	REQUISITOS
CONSTITUIR UNA CORPORACIÓN O FUNDACION	<ol style="list-style-type: none"> 1. Solicitud dirigida al/a Ministro/a 2. Acta de Asamblea General Constitutiva. suscrita por todos los fundadores (dos ejemplares) 3. Estatuto (dos ejemplares) 4. Declaración Juramentada - para acreditar patrimonio (firmada por todos los fundadores; - Presentar cuando sea solicitada
REGISTRO DE DIRECTIVA	<ol style="list-style-type: none"> 1. Solicitud dirigida al/a Ministro/a 2. Convocatoria a la Asamblea 3. Acta de la Asamblea, certificada por el Secretario
INCLUSIÓN O EXCLUSIÓN DE MIEMBROS	<ol style="list-style-type: none"> 1. Solicitud dirigida al/a Ministro/a 2. Acta de la Asamblea en la que conste la decisión de inclusión o exclusión 3. Los demás que se hubieren previsto en el estatuto
REFORMAR ESTATUTO	<ol style="list-style-type: none"> 1. Solicitud dirigida al/a Ministro/a 2. Acta de Asamblea, certificada por el Secretario, con indicación de los nombres y apellidos completos de los miembros presentes en la asamblea 3. Lista de reformas del estatuto
DISOLUCIÓN Y LIQUIDACION VOLUNTARIA	<ol style="list-style-type: none"> 1. Solicitud dirigida al/a Ministro/a 2. Convocatoria a la Asamblea General 3. Acta de la Asamblea - nombrar un liquidador y aprobar el informe 4. Informe del liquidador (existan o no bienes)

NOTA: Fuente: Tomado del (Ministerio de Inclusión Económico y Social MIES, 2017, pág. 1)

Conformación de la asociación

Al conformarse la “Asociación”, debe firmarse un acta de constitución, esta acta constitutiva, debe ser conformada por al menos cinco integrantes, con al menos las siguientes dignidades:

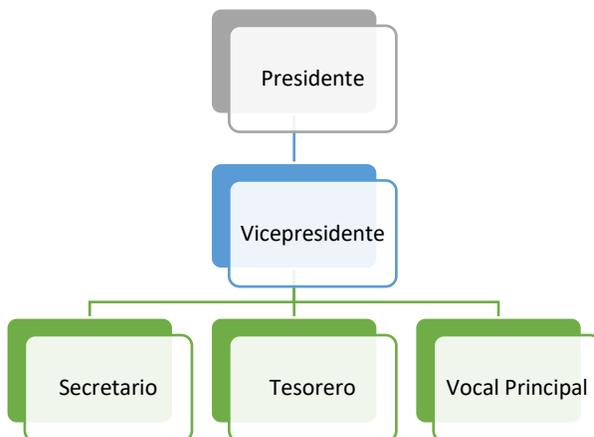
- PRESIDENTE
- VICEPRESIDENTE
- SECRETARIO
- TESORERO
- VOCAL PRINCIPAL

Organigrama de la directiva

En la figura 7, se muestra la estructura del organigrama funcional para la Asociación AECIE.

Figura 7

Organigrama de la Directiva de la Asociación “AECIE”



Para la conformación de la asociación debe existir un estatuto, el mismo que está normado acorde a las recomendaciones del Ministerio de Inclusión Económica y Social “MIES”, ya que la orientación de la AECIE, es conformar una institución o una asociación sin fines de lucro, por esto ubicamos como apéndice el modelo del estatuto por la institución gubernamental. Ver Apéndice A.

CAPÍTULO 3

Plan de Concientización

Introducción

Las tecnologías de información y comunicación se han transformado en herramientas que nos permiten optimizar recursos, tiempo y procesos para el funcionamiento de empresas, automatización edificios, aplicaciones para el hogar etc.

Con el uso de la tecnología, los usuarios se ven expuestos, a amenazas y vulnerabilidades asociadas al uso de las mismas, que pueden ocasionar brechas de seguridad para disponibilidad de los servicios, integridad y privacidad de la información que se encuentra almacenada en las diferentes aplicaciones y puedan interrumpir el correcto desempeño del negocio.

Las estadísticas de empresas consideran al recurso humano como el eslabón más débil en la cadena de seguridad de la información, ya que el primer proceso para una buena defensa es tener personal debidamente capacitado en función de la importancia del valor de la información

Objetivo

Diseñar un plan de capacitación o concientización para dar a conocer los aspectos claves referente a la importancia de la información dentro de una empresa, y que la misma es esencial para la continuidad del negocio.

Alcance

El alcance del plan de concientización sobre la importancia de la seguridad de la información es gestionar las estrategias de comunicación para capacitar a todos los miembros de la asociación.

Fases del Plan

En la figura 8, se muestra el diagrama de las fases del plan de concientización para los miembros de la asociación.

Figura 8

Fases del Plan de Concientización



Fases de Diseño

- Capacitar y sensibilizar a los miembros de la asociación
- Disminuir los incidentes de seguridad
- Establecer el alcance de los objetivos de la fase de diseño
- Guiar en el cumplimiento de las políticas de control de acceso
- Personal sensibilizado y capacitado en buenas practicas
- Realizar copias de seguridad

Planificación

En esta parte de la fase de diseño se encarga de planificar las diferentes actividades, que se llevaran a cabo dentro del plan de concientización.

Tareas de la etapa de planificación*Capacitar*

Brindar los conocimientos necesarios sobre la ciberseguridad a los usuarios en el ámbito de sus competencias que desempeñan en sus respectivas empresas, en base a un conjunto de actividades didácticas como son videos, charlas, practicas, etc.

Con los conocimientos adquiridos los usuarios podrán tener habilidades que ayuden a identificar las posibles riesgos y amenazas que puedan existir en el normal desempeño de sus activades diarias en su trabajo.

Sensibilizar

Dar a conocer acerca de la importancia sobre las buenas prácticas de la ciberseguridad, a través de la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI).

Entregar

Los conocimientos necesarios que se pueden aplicar en sus labores diarias, en función de lo aprendido en materia de ciberseguridad.

Fase de desarrollo

A continuación, se describen los principales ítems que a tener en cuenta como medidas de ciberseguridad.

Realizar copias de seguridad.

Implementar una política para la obtención de copias de seguridad, conforme a la regla 3-2-1. Para aplicar la regla de 3-2-1 en los respaldos en una empresa hay que seguir sus tres principios básicos:

- **Realizar tres copias de los datos.** Se debe realizar tres copias diferentes en distintos dispositivos o medios de almacenamiento, sean estas cintas, discos duros, etc.
- **Guardar al menos dos copias en soportes distintos.** La información de respaldo debe estar almacenada en diferentes dispositivos de almacenamiento e incluso un respaldo en la nube.
- **Una de las copias se debe mantener fuera de la empresa.** El objetivo de mantener copias externas a las instalaciones de la empresa, es apoyar al plan de contingencia para que se pueda guardar en una bodega en donde se custodie los dispositivos de almacenamiento físicos de la información respaldada, en la actualidad se ha cambiado esta forma de respaldo ya que al tener proveedores de servicios de infraestructura en la nube, de igual manera los respaldos se almacenan en la misma cuenta, al requerir un alto nivel de seguridad sin dejar al azar la integridad de la información.

Disminuir los incidentes de seguridad

- Se realizará la capacitación de diferentes tecnologías para obtener información estadística que puedan obtener las empresas asociadas.

Guiar en el cumplimiento de las políticas de acceso

Las medidas de control de accesos de la norma ISO 27001 están orientadas a controlar y monitorizar los accesos a los medios de información de acuerdo con las políticas definidas por la organización.

Requisitos para definir las reglas de control de acceso a la información, o sea los derechos y restricciones de acceso a la información.

El requisito exacto de este punto, especifica la necesidad de establecer, documentar y revisar la política de control de acceso periódicamente, lo que significa que una política documentada es obligatoria.

Los propietarios de los activos son los que deben determinar estas normas o políticas de control de acceso de acuerdo con la política de seguridad de la información y el análisis de riesgos

El principio básico para la elaboración de estas reglas es:

La asignación de la menor cantidad de privilegios posibles para llevar a cabo una tarea dentro de un sistema de información

La concesión de esos privilegios solamente por el tiempo que sea necesario para el desarrollo de las tareas

En otra forma de explicarlo, se deben asignar los permisos de acceso limitados solamente a la información necesaria para hacer un trabajo, tanto a nivel físico (accesos a instalaciones o soportes de información), como lógicos (Accesos a aplicaciones).

Aunque nos hemos referido tanto a permisos del tipo lógico como físico, este apartado solamente se refiere a los accesos a nivel lógico, aunque ambos deben ir a la par y basarse en los mismos principios.

Otro principio a tener en cuenta en la elaboración de las políticas de control de acceso es el siguiente:

El objetivo de la política de control de acceso debería ser que todo está prohibido a menos que esté expresamente permitido y no al revés

Profundicemos un poco más en todo esto para ver como aplicamos estos principios

ASIGNACION DE ROLES

Los roles dentro de un sistema de Información nos informan de lo que un usuario está autorizado a hacer dentro de un sistema y de lo que no le está permitido. (norma iso27001, 2022)

En la tabla 2 se resume el plan de capacitación y sensibilización en función de los objetivos planteados.

Tabla 2

Plan de Capacitación y Sensibilización

OBJETIVO	QUE COMUNICA	FRECUENCIA	QUIEN DEBE COMUNICAR (RESPONSABLE)	ESTRATEGIA DE COMUNICACIÓN	GRUPOS DE INTERÉS (A QUIEN COMUNICA)	
Socializar los procedimientos del proceso Gestión de Recursos Informáticos	Uso, apropiación y Actualización de los procedimientos del proceso Gestión de Recursos Informáticos	Cuando sea requerido o necesario	Funcionario asignado AECIE	Capacitación Inducción puestos de trabajo	Personal AECIE	
		Semestralmente	Funcionario asignado AECIE	Inducción Reinducción	Personal Administrativo	
Socializar información relevante relacionada con SGS y SGSI	Consejos de Seguridad	Semestralmente	Director y/o funcionario asignado AECIE	Correo Página web Redes Sociales institucionales Capacitación Inducción y Reinducción	Personal Administrativo Comunidad universitaria en general	
	Seguimiento a la mejora continua SGS y SGSI	Trimestralmente			Taller de Gestión Sistema Plan de Mejora	Alta Dirección
	Objetivos del SGS	Anual				Correo Inducción Reinducción Redes sociales Institucionales Taller de Gestión Contrato Sistema SIG
	Objetivos del SGSI					
	Manual de Políticas del SGSI					
	Política del SGS					
	Política del SGSI					
Plan del SGS - SGSI						

Capacitar y sensibilizar a los socios del AECIE en el sistema de Gestión de Seguridad de la Información.

Se dictarán capacitaciones a los funcionarios de las empresas asociadas, que permitirán dar a conocer los riesgos sobre el mal manejo de la información.

Fase de implementación

Se realizarán las actividades de sensibilización y capacitación teniendo en cuenta las siguientes estrategias de comunicación:

- Banner
- Portal web
- Redes sociales institucionales
- Correo Institucional Masivo
- Capacitación
- Inducción puestos de trabajo
- Talleres de Gestión
- Informe a la alta dirección

Fase de Mejoramiento

En esta fase es necesario establecer una comunicación bidireccional a todas las partes involucradas y tener una respuesta adecuada para conocer cómo se debe proceder.

Evaluación: Se tendrá al final de las capacitaciones una evaluación breve para conocer el nivel de aprendizaje sobre las mismas.

Objetivos de la Mejora*Calidad*

Este objetivo esta enfocado en tener una correcta gestión de la información, de manera que cumpla con los siguientes objetivos:

- No divulgar
- Destruir la misma con acceso no autorizados.

Recursos

Contar con recursos para proteger los activos de información debidamente clasificados en cada uno de los sistemas informáticos, con una correcta política de respaldos, gestión de incidentes y un plan de continuidad del negocio antes, durante y después de todo tipo de riesgo que interrumpan los servicios.

Productividad

Realizar actualizaciones de todas de las tecnologías utilizadas, para que no se dé una brecha tecnológica demasiado amplia, y estas puedan ofrecer una mejor prestación de servicios para necesidades empresariales y mejor desempeño de los usuarios.

Reducción de riesgos

Disponer e implementar un plan de continuidad de los procesos core del negocio que permitan una respuesta rápida para el control y la mitigación de posibles amenazas y riesgos que atenten al normal funcionamiento del negocio.

Capacidad

Disponer de un inventario de los servicios y activos de tecnología, así como el nivel de criticidad acorde a la clasificación de la información.

Valor

Disponer de mecanismos que permitan asegurar la confidencialidad, integridad y disponibilidad de la información, concientizando el valor real de la información dentro de una organización, empezando por la implementación de una política de acceso a los usuarios a la información más relevante acorde con las áreas a las que pertenecen.

Informar sobre las mejoras implementadas

La información de las mejoras implementadas es dada a conocer en los talleres de gestión y en apoyo en redes sociales, correos masivos.

Acción correctiva

Actuar de manera rápida y eficiente en las acciones para disminuir y eliminar la causa de los problemas, tomando como referencia los requisitos del SGSI, disponer de una bitácora técnica para solventar posibles amenazas en el futuro.

- Encontrar posibles no conformidades atadas a la estándar SGSI que generen incidente de seguridad de la información.
- Diseñar e implementar la acción correctiva necesaria.
- Contar con planes de acción de respuesta de incidentes.

Acción Preventiva

Monitorear y descubrir las posibles brechas de seguridad que pueden existir, para lo cual algunas acciones a realizarse:

- Levantar un inventario de activos informáticos.
- Clasificación de los activos informáticos
- Análisis de riesgos y vulnerabilidades
- Comunicación de los riesgos
- Diseño e implementación de un PDCA de los procedimientos de seguridad informática.

Directorio de Software Forense

Ofrecer como medio de consulta y capacitación para los miembros de la Asociación de Especialistas en Ciberseguridad del Ecuador “AECIE” un directorio de Software Forense, el mismo que con el transcurrir del tiempo debe aumentar en cantidad de aplicativos y manuales y en la actualización de las versiones de los mismos.

Desarrollo del directorio Forense

Este directorio se va a publicar para el uso de los miembros de la “AECIE” con las herramientas para el análisis forense, haciendo referencia a las fases de adquisición y análisis de las evidencias, para lo cual vemos como necesidad contar con una gran variedad de abanico de herramientas, técnicas y métodos, así como el conocimiento necesario para poder elegir la utilización de la herramienta más adecuada.

En el directorio se van a ofrecer tips profesionales con las cuales se podrá enfocar el correcto uso de las mismas, ya que algunas de las herramientas requieren de un conocimiento más profundo.

En este caso se ha creado un repositorio digital en donde los miembros de AECIE, en el cual podrán acceder a un sin número de herramientas que constantemente se actualizarán, tanto en manuales como en imágenes para ser montados en entornos virtuales.

Para lo cual se ha publicado la versión 1.0 del directorio, en el cual los miembros pueden acceder a consultar los aplicativos y manuales.

URL de ingreso <http://34.86.255.61>

Para el ingreso a la URL donde se encuentre el repositorio digital, se debe realizar una solicitud de acceso. Ver Apéndice B.

Desde nuestra perspectiva agrupamos y como primer proceso de investigación nos enfocaremos en las herramientas forenses de “Adquisición de información”, agrupando en 3 métodos distintos de extracción de evidencias:

- Adquisición física
- Adquisición del sistema de ficheros
- Adquisición lógica.

Adquisición física:

En general este es el método líder. El cual implica en realizar una copia idéntica del medio de almacenamiento original, con el objetivo de preservar todas las pruebas posibles. La ventaja de este método es que nos da la posibilidad de buscar elementos eliminados. Su principal desventaja es el grado de dificultad en comparación con otros métodos, así como la cantidad de tiempo requerido para completar esta adquisición.

Adquisición del sistema de ficheros

La forma en la que se hace la copia de los ficheros almacenados en el dispositivo es mediante la utilización de herramientas propietarias del fabricante, su forma de acceso y trabajo es a través del terminal bash del ordenador. La ventaja de este proceso en relación con el anterior es el grado de complejidad, mientras que su desventaja sería no permitir su acceso a una gran cantidad de información.

Adquisición lógica.

Mediante la ejecución de este método nos permite ver todos los archivos en un sistema de ficheros, el cual no incluye particiones ocultas o ficheros eliminados. En función del tipo de análisis forense que se esté trabajando, este método puede ser suficiente, ya que es un método de menor complejidad en la adquisición de evidencia lógica. Para lograr esto, se utilizan los componentes integrados del sistema operativo, para realizar una copia de ficheros de este. Cabe indicar que cuando se eliminan estos ficheros, a nivel lógico se etiquetan como disponible para sobre escribirlos, por lo que aún están disponibles temporalmente y, por lo tanto, se pueden recuperar.

Para elegir el método adecuado en la recolección de evidencia durante el análisis forense se debe tener en consideración los siguientes aspectos:

- Nivel de minuciosidad requerido
- Limitación de tiempo para completar el proceso
- Tipo de información necesaria como volátil, previamente eliminada y de aplicaciones de terceros.

Una vez definida la versión 1.0 del directorio digital procedemos a listar los aplicativos forenses a continuación:

Caine

El proyecto Computer Aided Investigative Environment “CAINE”, es una distribución GNU/Linux en modo LiveCD creada por Giancarlo Giustini como un proyecto de Informática Forense (Forense Digital) para el Centro de Investigación en Seguridad (CRIS), con el apoyo de la Universidad de Modena y Reggio Emilia.

Como novedad, CAINE ofrece una nueva interfaz de usuario, para todas las herramientas incluidas dentro del proyecto. Además, presenta nuevas funcionalidades importantes que tienen como objetivo que varias herramientas forenses trabajen bajo el mismo esquema, entendiendo que una interfaz gráfica de usuario unificada es más amigable para los investigadores forenses, ya que es una guía en la adquisición y el análisis de evidencia digital, brindando un proceso continuo durante el proceso de documentación y generación de informes y resultados.

Características principales

Esta distribución nos ofrece un entorno Linux completo, integrando todas las herramientas disponibles en una GUI amigable y fácil de usar desde el primer momento. Todo en lo que consiste esta distribución es de código abierto, tanto la parte de gestión como todas las herramientas disponibles.

Adicional, esta distribución está diseñada para funcionar sin problemas en todo tipo de computadoras, tanto BIOS Legacy como UEFI, ejecutándolo incluso en equipos con el arranque seguro habilitado, tomando en cuenta que el único requisito para utilizar las nuevas versiones de esta herramienta es que el procesador sea de 64 bits, ya que no existe disponible una imagen x86.

El proyecto CAINE ofrece al usuario las siguientes actualizaciones importantes:

- Fácil interoperabilidad durante todo el análisis (Recolección, Preservación, Análisis y Reportes)
- GUI amigable e intuitivo de usar
- Como sistema base el proyecto CAINE está en Ubuntu, esto implica una instalación fácil y adaptación a nuestro entorno de trabajo
- Los reportes se generan de forma no automatizada.

Esta distribución cuenta con herramientas que nos permiten analizar desde redes, discos duros, tarjetas de memoria hasta bases de datos, ya que es compatible con los estándares principales de comunicación y además soporta sistemas de archivos, como EXT2, EXT3, FAT, FAT32, NTFS, HFS y exFAT. De igual manera se puede auditar sistemas basados en Windows a través de la memoria RAM, ya que podemos volcar datos estos con el formato RAW.

Cabe indicar que en esta distribución de Linux nos podemos encontrar con programas conocidos, tales como un terminal bash y navegador Firefox.

Algunas de las herramientas más relevantes que podemos listar del proyecto CAINE se detallan a continuación:

- **AtomicParsley:** es un programa de línea de comandos liviano para leer, analizar y configurar metadatos en archivos MPEG-4, en particular, metadatos de estilo iTunes.
- **AutoMacTc:** “Automated Mac Forensic Triage Collector” Software diseñado para auditar equipos en entornos macOS.
- **Autopsy:** Interfaz gráfica para The Sleuth Kit, una herramienta imprescindible para el investigador forense.
- **Bkhive:** Es una herramienta que se utiliza para la extracción de la clave del sistema de Windows, la cual es utilizada para cifrar los valores hash de las contraseñas de los usuarios.
- **Bitlocker:** Contiene un plugin, el cual permite acceder a las particiones cifradas con el software de Microsoft.
- **Cryptcat:** Es una herramienta que utiliza el cifrado twofish para mantener la confidencialidad del tráfico entre el cliente y el servidor. Además, nos permite leer y/o inyectar datos en conexiones TCP o UDP.

- **DCfldd:** Es una herramienta mejorada de GNU dd con funciones útiles para análisis forense y seguridad.
- **Dvdesastre:** Es una herramienta que almacena datos en CD/DVD/BD (medios admitidos) de manera que se pueden recuperar por completo incluso después de que se hayan producido algunos errores de lectura.
- **Firmwalker:** Es un script que nos permite buscar sistemas de archivos de firmware con información de contraseñas, archivos de configuración y scripts.
- **FKLook:** Es un script se puede usar para buscar una palabra clave en muchos archivos y copia solo los archivos que tienen una palabra clave coincidente en un directorio separado de su elección.
- **Fsstat:** Nos permite conocer y monitorear las operaciones del sistema de archivos por tipo de sistema de archivos y por punto de montaje con la información de cualquier imagen u objeto de almacenamiento.
- **Geany:** Es un editor de texto potente, estable y ligero para programadores, que proporciona una gran mayoría de funciones útiles.
- **HDSentinel:** Es una herramienta de monitoreo y análisis de SSD y HDD de múltiples sistemas operativos. Su objetivo es encontrar, probar, diagnosticar y reparar problemas de unidades de disco duro, informar y mostrar el estado de SSD y HDD, degradaciones de rendimiento y fallas.
- **Log2timeline:** Es una herramienta para la creación automática de un informe de los registros encontrados como sospechosos sobre una línea de tiempo.
- **Md5deep:** Es una herramienta que nos permite comprobar la integridad de los algoritmos de hash MD5, SHA-1, SHA-256, Tiger, de cualquier fichero o directorio.

- **Offset_Brute_Force:** Es un script de Shell que analiza los discos por fuerza bruta, buscando una partición oculta la cual intentará montarla.
- **PhotoRec:** Es una herramienta que permite recuperar archivos a través de la metadata y pie de página de los tipos de archivos que se encuentra en el espacio no asignado.
- **RegRipper:** Programa diseñado para extraer y mostrar información específica ubicada en los archivos de la sección del registro y complejas bases de datos.
- **Rifiuti:** Es una herramienta de análisis forense de papelera de reciclaje.
- **SQLJuicer:** Es una herramienta basada en Perl que enumera las transacciones CRUD de la base de datos, analizando las entidades de registro de transacciones de SQL Server.
- **TestDisk:** Es una herramienta que permite recuperar particiones de almacenamiento de datos perdidas y/o hacer que los discos que no arrancan puedan volver a arrancar cuando existe un problema causado por software defectuoso, como ciertos tipos de virus o errores humanos como borrar accidentalmente la tabla de particiones.
- **Tinfoleak:** Es una herramienta de código abierto dentro de las disciplinas OSINT (Open Source Intelligence) y SOCMINT (Social Media Intelligence), que automatiza la extracción de información en Twitter y facilita el análisis posterior para la generación de inteligencia.
- **Wireshark:** Es una de las herramientas más importante y ampliamente utilizada en el mundo, la cual nos permite ver lo que sucede en la red con un nivel microscópico ya que nos permite capturar y analizar la información que viaja por la red.

Todos los programas podemos lanzarlos desde el propio menú de aplicaciones, por lo que no tenemos por qué memorizar sus nombres, ya que se encuentran correctamente clasificados y ordenados en función de su finalidad.

Wireshark

Gerald Combs en el año de 1997, ante la necesidad de una herramienta para buscar problemas en la red de una herramienta para analizar y encontrar conocimiento sobre lo que pase en la red empezó a diseñar Ethereal (nombre con el que nació originalmente en la web). El proyecto Wireshark) como una solución a estos problemas y otorgar una herramienta que cumpla este propósito.

Este desarrollo en la época en la que inicio era bastante costoso y tenía muchos problemas los mismos que en año de 1998 fueron subsanados a través de la versión 0.2.0. Esta versión seguía siendo inestable, por lo que se les comenzaron a agregar parches que prácticamente subsanaban errores de código y de componentes básicos, con todas estas decisiones el proyecto volvió a tomar un rumbo muy prometedor.

Gilbert Ramírez encontró potencial en esta idea, la cual la visualizo como ganadora y se sumó al proyecto, agregando un disector de bajo nivel (una extensión que permite que el programa principal desensamble un paquete de datos basado en ciertos argumentos y propiedades).

Guy Harris en su búsqueda de una mejor herramienta que el limitado tcpview, por lo que comenzó a parchear y proporcionar más analizadores para Ethereal.

Richard Sharpe, que estaba investigando más en los protocolos de TCP/IP, observo un gran potencial y un futuro promisorio en este proyecto y realizó estudios para analizar la compatibilidad con los otros protocolos. Demostrando que eran fáciles de agregar, entonces, comenzó a ofrecer más analizadores a profundidad (disector), parches y complementos.

Este proyecto contaba con muchos colaboradores los mismos que investigaban y exploraban los protocolos que no eran compatibles con Wireshark, por lo que el crecimiento del

proyecto alcanzó etapas para las cuales no se estaba preparado. Su objetivo fue clonar un disector que ya se encontraba en el mercado, con esto el equipo tenía más acceso al código y por ende mayor control del conocimiento.

Wireshark finalmente lanzó la versión 1.0 después de muchos años de desarrollo, se consideró esta versión completa con las características necesarias para su lanzamiento, que se hizo en una pomposa fiesta llamada Sharkfest, en la cual sus creadores ofrecieron una brillante conferencia. La versión 2.0 fue lanzada en el 2015 con una nueva interfaz de usuario.

Luego de repasar la historia de Wireshark podemos sin duda alguna decir que en la actualidad es un software muy conocido y de mucha utilidad para los administradores de sistemas, jefes de infraestructura, analistas de redes y profesionales de ciberseguridad que se encargan del ámbito de las telecomunicaciones y redes.

No es una coincidencia que la mayoría de profesionales que se dedican a la ciberseguridad consideren que es el software líder en el mundo de las telecomunicaciones desde su promulgación, que el progreso alcanzado por este paquete es el que ha permitido de la mayoría de problemas, ya que permite su análisis en tiempo real y también mediante la importación de archivos web que contienen estos paquetes de datos.

Para qué sirve Wireshark

Dentro de todas las aplicaciones de Wireshark sirve para lo siguiente:

- Maneja la pérdida de paquetes
- Incidentes de latencia y actividad maliciosa en la red
- Solicitudes HTTP.
- Proporciona herramientas y comandos para filtrar y analizar el tráfico de la red.
- Los administradores de sistemas y redes lo utilizan para detectar dispositivos no

autorizados que sueltan paquetes

- Problemas de latencia de máquinas no autorizadas
- Enrutamiento del tráfico de red en todo el mundo
- Filtrado de malware en intentos de piratería en la organización.

El analizador de red tiene una poderosa herramienta la misma que para ser utilizada necesita que quien lo hace tenga profundos conocimientos de redes y telecomunicaciones. Esto quiere decir que el comprender cómo funciona el protocolo HTTP y el TCP/IP, en especial su pila, lo analizan y comprenden las cabeceras de los paquetes, que normalmente van atados a su metadata, el enrutamiento y su entrelazado, y a su vez el control de puertos y la asignación dinámica de direcciones IP (DHCP).

Otras características que se pueden listar son las siguientes:

- Rastrear paquetes de flujo TCP,
- Informe de todo lo relacionado con los protocolos TCP/IP
- Uso de filtros personalizados de todo el flujo de comunicación.
- Extracción y exportación de paquetes
- Emisión de informe de estadísticas de todos los paquetes capturados, se incluye un

resumen con la siguiente información:

- ✓ Los puntos finales
 - ✓ Protocolos Jerarquizados
 - ✓ Conversaciones
 - ✓ Diagrama de flujo de toda la comunicación.
- Análisis informativo tomando como referencia MAC ADDRESS, red, y otros.
 - Reconfiguración de paquetes.

- Terminal de Linux llamada TShark similar al terminal de Linux.

Ventajas y desventajas de Wireshark

Ya que Wireshark es considerado como un analizador de paquetes y redes poderoso, podríamos decir que siempre van a ser más las ventajas que las desventajas, con esta premisa podemos concluir que es uno de los aplicativos más usados y conocidos.

Ventajas:

- Cuenta con soporte de “*Brute Analysis*”.
- Colaboración de la comunidad para incluir mejoras, manuales y documentación.
- Colaboración de la comunidad para disminuir el tiempo y la calidad de los cambios basándose en la necesidad de especificidad de los paquetes.

Desventaja:

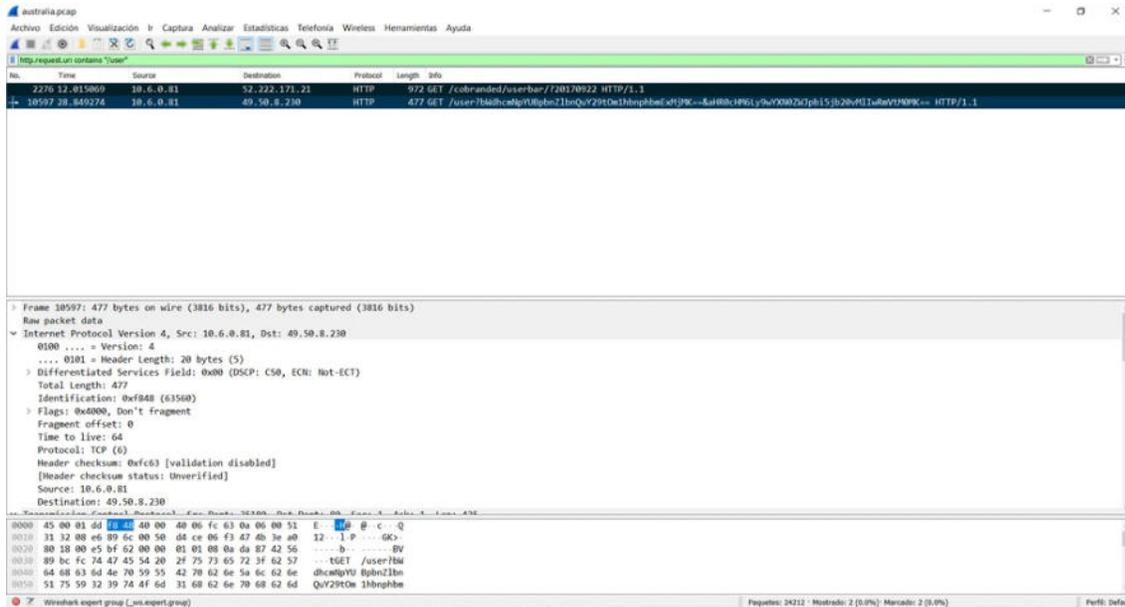
- La única desventaja que podríamos traer a colación es que la persona que use Wireshark debe conocimientos profundos sobre los protocolos de red y su pila stack.

Uso práctico y sencillo de Wireshark

Con este ejemplo se puede observar que en la interfaz se puede realizar búsquedas utilizando GET con la finalidad de obtener únicamente los paquetes que nos interesan y desechar lo que no aporta.

Se puede hacer una búsqueda en definido protocolo utilizando los métodos ya sea GET, POST y usando el operador “and” para unir y concatenar las búsquedas utilizando más parámetros, ya que estos paquetes pueden contener una ruta determinada como la de “user”

Podemos encontrar algo más preciso al buscar en la url contenga “/user” en la url, como se muestra en la figura 9, lo que quiere decir que a pesar de que puede ser más preciso no necesariamente puede funcionar.

Figura 9*Proceso de búsqueda URL*

Para este ejemplo podemos decir que al final se tratará en un fichero pcap, en el cual vamos a hacer búsquedas diseccionando los paquetes, la información de sus archivos raw dependerá de la búsqueda ya que también no se podrá encontrar nada. Se concluye que este tipo de análisis son muy extensos ya que la red contiene bastante información y si no se tiene una pista clara de donde puede provenir lo que estamos buscando entraremos en análisis más exhaustivo.

Paladin Forensic Suite.

Paladín está basada en Ubuntu, y fue desarrollada gracias al trabajo incasable de Manoj Kumar y el equipo de Forensic Digital proporcionada como cortesía por SUMURI. La pieza central de estas herramientas es la caja de herramientas de PALADIN. PALADIN Toolbox ha combinado y simplificado múltiples tareas forenses en una GUI (interfaz gráfica de usuario) fácil de usar que requiere una capacitación mínima y no requiere que los usuarios utilicen la línea de comandos

El "motor" que hace funcionar PALADIN Toolbox es una combinación de aplicaciones que los examinadores e investigadores forenses han utilizado durante años y han resistido el escrutinio de muchos tribunales de justicia.

Una de las principales funciones de PALADIN además de las herramientas forenses es la de clonación de discos o crear imágenes en local o a través de red, hacer dos clonaciones de forma simultánea y utilizando formatos en los que se incluyen:

- AFF
- Apple Disk Image (.dmg)
- EWF2 (.Ex01)
- Expert Witness (.E01)
- RAW (.dd)
- SMART
- Virtual Disk Format (.vmdk)

Dentro de las principales funciones tenemos:

- Arranca la mayoría de las PC y las Mac Intel en un entorno sólido desde el punto de vista forense.
- Admite los formatos de imagen forense más populares: .E01, Ex01, RAW (.dd), SMART, AFF, VHD y VMDK.
- Posibilidad de clonar dispositivos.
- Capacidad para convertir de una imagen forense a otra, incluido el formato VMDK.
- Capacidad para crear una imagen maestra y una de archivo o dos formatos de imagen diferentes al mismo tiempo.
- Capacidad de montaje e imagen a través de una red.

- Disk Manager le permite visualizar e identificar fácilmente las unidades adjuntas y sus particiones.
- Capacidad para formatear como ExFAT, HFS+, EXT4, FAT32 y NTFS.
- Controle el montaje, la limpieza (esterilización) y el triturado con un solo clic. Capacidad de capturar y crear una imagen del espacio no asignado y el espacio libre en un archivo para tallar.
- Registro automático que se puede guardar en cualquier dispositivo. Clasificación integrada que puede buscar por nombre de archivo, palabras clave o tipos MIME (firmas de archivo).
- Más de 100 herramientas y aplicaciones forenses de código abierto pre compiladas en el Baúl de herramientas forenses.
- Compatibilidad con Bitlocker para Windows Vista, 7, 8, 8.1 y 10 particiones cifradas.

Diferencias entre versiones (PALADIN LTS vs. EDGE)

Hay tres versiones de PALADIN:

- PALADIN LTS (arquitectura de 64 bits)
- PALADIN EDGE 64 (arquitectura de 64 bits)
- PALADIN EDGE 32 (arquitectura de 32 bits)

PALADIN LTS es arquitectura de 64 bits y se basa en la versión LTS (soporte a largo plazo) más actual de Ubuntu. LTS permite una distribución más estable Además de la caja de herramientas de PALADIN, esta versión de PALADIN incluye herramientas y aplicaciones forenses de código abierto pre compiladas.

PALADIN EDGE incluye PALADIN Toolbox, pero no incluye ninguna herramienta ni aplicación forense de código abierto pre compilada adicional.

Al eliminar las herramientas pre compiladas adicionales, esta distribución es más pequeña y se inicia más rápido. Además, las ediciones de PALADIN EDGE se compilan con kernels de Linux más nuevos que tienden a admitir hardware más nuevo.

PALADIN EDGE está disponible en arquitectura de 32 y 64 bits.

Tanto PALADIN como PALADIN EDGE tienen tres modos que se pueden seleccionar desde la pantalla de bienvenida:

- Sesión en vivo - Modo forense
- Sesión en Vivo - Servicios Remotos SUMURI
- Sesión en vivo - Modo no forense

Modo forense con redes desactivado, Arrancando a Modo Forense PALADIN no monta unidades internas, medios adjuntos y/o archivos de intercambio.

Una vez iniciado, el montaje de dispositivos es controlado por PALADIN Toolbox.

El usuario puede utilizar PALADIN Toolbox y cualquier herramienta forense precompilada para completar las tareas.

PALADIN Toolbox

El proyecto PALADIN fue concebido por Steve Whalen en 2006 debido a la necesidad de tener una solución fácil de usar, de bajo costo o sin costo alguno, para obtener imágenes y obtener una vista previa de las computadoras. Este fue lanzado como "Raptor" en 2007. Whalen abandonó "Raptor" en 2010 cuando se fundó SUMURI y se lanzó PALADIN. Desde 2010, la caja de herramientas de PALADIN se ha reescrito por completo para tener en cuenta los cambios en la tecnología y continúa actualizándose. PALADIN Toolbox ha combinado y simplificado múltiples tareas forenses en una GUI (interfaz gráfica de usuario) fácil de usar

Kit Passware Forense

Kit Passware Forense, Es la solución completa de descubrimiento de evidencia electrónica cifrada que informa y descifra todos los elementos protegidos con contraseña en una computadora, tiene la capacidad de recuperar contraseñas de más de 300 tipos de archivos, dentro de su capacidad tiene la de descifrar y recuperar contraseñas de imágenes de disco tales como Apple DMG, bitlocker, DELL, FileVault2, Symatex entre otras.

Dentro sus funciones, además de descifrar equipos de cómputo permite el análisis forense móvil para extraer y descifrar datos de dispositivos móviles Android e iOS, y recuperar datos de iPhone de dispositivos deshabilitados.

La función de detección inteligente y análisis de complejidad detecta todos los archivos y las imágenes del disco duro e informa el tipo de cifrado y la complejidad del cifrado, analiza las imágenes de memoria en vivo, archivos de hibernación y extraer claves de cifrado.

VENTAJAS DE LA HERRAMIENTA

Una de las principales ventajas del Passware Kit Forensic en comparación con otras aplicaciones similares como ClamAV/ClamWin, Free Word ExcelPassword, Hashkill, UnrarExtract, cRARk, es que permite ejecutar múltiples acciones bajo un mismo entorno y una misma plataforma. Otra de las ventajas sobresaliente del Passware Kit Forensic es que permite descifrar contraseñas a través de métodos de diccionario y fuerza bruta utilizando aceleración de GPU y computación distribuida para Windows, Linux y servicios en la nube como Amazon EC2, así como Password Exchange el cual proporciona acceso a la lista de contraseñas encontradas por los usuarios de Passware Kit en todo el mundo, ofreciéndose como un diccionario avanzado para mejorar las posibilidades de encontrar contraseñas seguras.

Crowdresponse:

CrowdResponse es una herramienta Open Source diseñada por Robin Keir de CrowdStrike, en el cual el objetivo de CrowdResponse es proporcionar una solución ligera para que los analistas forenses realicen la detección de firmas y la recopilación de datos de clasificación. Es compatible con todas las distribuciones de Windows hasta Windows Server 2012 y está basado en la línea de comandos Command-line Interface (CLI).

La primera versión está enfocada en la detección de firmas, con un potente motor de escaneo denominado YARA.

Ejecución de análisis YARA

Yet Another Regex Analyzer (YARA), se ha convertido en una de las principales herramientas para describir y detectar malware. Para realizar una búsqueda con YARA se utilizan reglas que consisten en una serie de cadenas unidas por una condición booleana, la búsqueda con texto, distinción entre mayúsculas y minúsculas y expresiones regulares, combinación de estas opciones permite la construcción de pruebas complicadas para limitar los falsos positivos.

Como ejemplo, a través de la figura 10 se muestra una regla YARA, la cual permite identificar textos y expresiones.

Figura 10

Regla que Identifica Textos y Expresiones Regulares

```
script.yara
C:\Users> rcar > OneDrive > Escritorio > script.yara
1 rule CrowdStrike_Shmoon_DroppedFile
2 { meta:
3 description = "Rule to detect Shmoon malware."
4 strings:
5 $testn123 = "test123" wide
6 $testn456 = "test456" wide
7 $testn789 = "test789" wide
8 $testdomain = "testdomain.com" wide
9 $pingcmd = "ping -n 30 127.0.0.1 >nul" wide
10 condition:
11 (any of ($testn*) or $pingcmd) and $testdomain
12 }
```

Realizando el análisis del malware destructivo Shamoon detección mediante CrowdResponse, utilizando una regla de YARA en particular identifica el malware. Después de pegar la regla en el archivo config.txt de CrowdResponse (también puede apuntar a una carpeta o URL que contenga reglas), ejecutamos la siguiente línea de comandos como se observa en la figura 11.

Figura 11

Ejecución de Script en base a Parámetros de Texto y Salida XML

```
C:\Users > ricar > OneDrive > Escritorio > scriptyara > ...
1
2 <!--StartFragment--><strong>CrowdResponse -v -i config.txt -o "%ip% %nm% %tm%.xml"</strong><!--EndFragment-->
```

Creamos una VM (Máquina Virtual) y la infectamos de Shamoon, al realizar el análisis del sistema infectado devolvió la salida de la Figura 12.

Figura 12

Detección de Firma YARA en un Archivo y Proceso Denominado trksrv.exe

```
C:\WINDOWS\system32\cmd.exe
Scanning file "C:\WINDOWS\system32\USER32.dll"
Scanning file "C:\WINDOWS\system32\GDI32.dll"
Scanning file "C:\WINDOWS\system32\MSCTF.dll"
Scanning file "C:\WINDOWS\system32\MSUTB.dll"
Scanning file "C:\WINDOWS\system32\IMM32.DLL"
Scanning file "C:\WINDOWS\system32\uxtheme.dll"
Scanning file "C:\WINDOWS\system32\apphelp.dll"
Scanning file "C:\WINDOWS\system32\msctfime.ime"
Scanning file "C:\WINDOWS\system32\ole32.dll"
Scanning file "C:\WINDOWS\system32\shlwapi.dll"
Scanning file "C:\WINDOWS\system32\USERENV.dll"
Scanning file "C:\WINDOWS\system32\trksrv.exe"
"CrowdStrike_Shamoon_DroppedFile": TRUE
Scanning PID 788 (trksrv.exe)
"CrowdStrike_Shamoon_DroppedFile": TRUE
Scanning file "C:\WINDOWS\system32\ntdll.dll"
Scanning file "C:\WINDOWS\system32\kernel32.dll"
Scanning file "C:\WINDOWS\system32\NETAPI32.dll"
Scanning file "C:\WINDOWS\system32\msvcrt.dll"
Scanning file "C:\WINDOWS\system32\ADVAPI32.dll"
Scanning file "C:\WINDOWS\system32\RPCRT4.dll"
Scanning file "C:\WINDOWS\system32\Secur32.dll"
Scanning file "C:\WINDOWS\system32\WS2_32.dll"
Scanning file "C:\WINDOWS\system32\WS2HELP.dll"
Scanning file "C:\WINDOWS\system32\USER32.dll"
```

Recibimos dos alertas para el mismo archivo: `trksrv.exe`. El primero es el resultado de búsqueda de YARA para el archivo ubicado en la carpeta `C:\Windows\system32`. La segunda alerta es el resultado del escaneo de memoria, identificando dentro del ID de proceso 788. Este es un punto clave: el módulo CrowdResponse YARA facilita el escaneo de archivos y procesos en la memoria. Específicamente, el plugin `@yara` puede:

- Analizar todos los procesos en ejecución
- Analizar archivos binarios de imágenes en disco
- Analizar archivos DLL cargados
- Analizar archivos y carpetas arbitrarios
- Limitar el escaneo por expresión regular
- Descargar reglas desde una URL y usar máscaras de reglas para limitar las selecciones

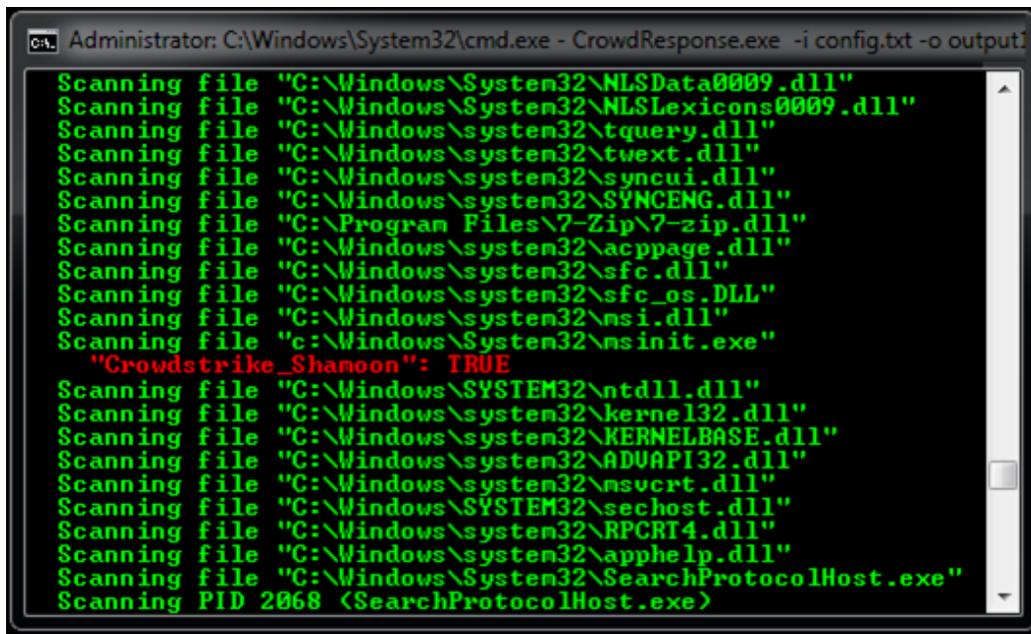
Shamoon es famoso por inutilizar a sus víctimas. La carga útil consiste en un limpiador que procede a sobrescribir los perfiles de usuario, los directorios del sistema y, en última instancia, el MBR del disco. Puedes ver varios de los objetivos del limpiaparabrisas en esta próxima regla YARA.

Shamoon destruye el sistema operativo y normalmente solo detectaría esta firma en un sistema donde algo impidió que el malware se ejecutara con éxito.

En la figura 13, vemos esta regla para un archivo denominado *msinit.exe*.

Figura 13

Golpe de Firma YARA en msinit.exe



```
Administrator: C:\Windows\System32\cmd.exe - CrowdResponse.exe -i config.txt -o output
Scanning file "C:\Windows\System32\NLSData0009.dll"
Scanning file "C:\Windows\System32\NLSLexicons0009.dll"
Scanning file "C:\Windows\system32\tquery.dll"
Scanning file "C:\Windows\system32\twext.dll"
Scanning file "C:\Windows\system32\syncui.dll"
Scanning file "C:\Windows\system32\SYNCENG.dll"
Scanning file "C:\Program Files\7-Zip\7-zip.dll"
Scanning file "C:\Windows\system32\acppage.dll"
Scanning file "C:\Windows\system32\sfc.dll"
Scanning file "C:\Windows\system32\sfc_os.DLL"
Scanning file "C:\Windows\system32\nsi.dll"
Scanning file "c:\Windows\System32\msinit.exe"
"Crowdstrike_Shamoon": TRUE
Scanning file "C:\Windows\SYSTEM32\ntdll.dll"
Scanning file "C:\Windows\system32\kernel32.dll"
Scanning file "C:\Windows\system32\KERNELBASE.dll"
Scanning file "C:\Windows\system32\ADVAPI32.dll"
Scanning file "C:\Windows\system32\USER32.dll"
Scanning file "C:\Windows\SYSTEM32\sechost.dll"
Scanning file "C:\Windows\system32\RPCRT4.dll"
Scanning file "C:\Windows\system32\apphelp.dll"
Scanning file "C:\Windows\System32\SearchProtocolHost.exe"
Scanning PID 2068 (SearchProtocolHost.exe)
```

Recopilación de información adicional

Una vez que haya detectado coincidencias de firmas en un sistema determinado, el siguiente paso es verificar esos resultados. Los módulos de CrowdResponse *#pslist* y *#dirlist* proporcionan información detallada sobre los archivos y procesos en ejecución de un sistema.

Ventajas de los módulos de CrowdResponse:

#pslist

- Enumerar todos los procesos
- Recopilar datos de encabezado PE
- Verificar firmas digitales
- Binario de imagen hash
- Proporcionar línea de comandos

- Mostrar archivos DLL cargados
- Identificar importaciones/exportaciones
- Detectar inyección de código

#dirlist

- Lista de archivos recursiva con máscaras regex y límites de recursión
- Verificar firmas digitales
- Cómputo de hashes MD5/SHA256 (compatible con hash rápido)
- Recopilar información de recursos
- Recopilación de marcas de tiempo (Información estándar)

CRconvert

CrowdResponse devuelve la salida en formato XML, lo que facilita su manipulación en cualquier forma que desee. Dependiendo del número de sistemas y módulos empleados, puede devolver una buena cantidad de datos. Los tres primeros módulos lanzados (#yara, #pslist y #dirlist) tienen 40 opciones de salida diferentes y casi 100 puntos de datos posibles. CRConvert crea informes CSV y HTML a partir de esta salida. Como ejemplo en la figura 14, el siguiente comando convierte la salida XML nativa en una serie de informes HTML:

Figura 14

Comandos Para Generar Informes Formato XML

```

<> script.yara
C: > Users > ricar > OneDrive > Escritorio > <> script.yara > ...
1
2 CRconvert -v -h -f <filename>.xml
    
```

En este ejemplo, aparecen dos archivos y un proceso en el sistema JIMMY278F golpeó dos reglas YARA diferentes. Mirando la figura 15 en la cual se muestra el informe de CrowdResponse #pslist proporciona más información sobre el proceso sospechoso, incluido PID, tamaño binario, línea de comandos, hilos inyectados, información de PE, etc.

Figura 15

Resultado de Informe Sobre Procesos Sospechosos

Module: pslist

system	pid	name	size	companyname	filedescription
JIMMY278F	0	*System Idle Process	0		
JIMMY278F	4	*System	0		
JIMMY278F	252	CAWINDOWS\system32\smss.exe	75264	Microsoft Corporation	Windows NT Session Manager
JIMMY278F	300	CAWINDOWS\system32\csrss.exe	6144	Microsoft Corporation	Client Server Runtime Process
JIMMY278F	324	CAWINDOWS\system32\winlogon.exe	945152	Microsoft Corporation	Windows NT Logon Application
JIMMY278F	2884	CAWINDOWS\SysWOW64\ctfmon.exe	15360	Microsoft Corporation	CTF Loader
JIMMY278F	2744	CAWINDOWS\system32\trksrv.exe	532992	Microsoft Corporation	Distributed Link Tracking Serve
JIMMY278F	1096	CAWINDOWS\explorer.exe	1364480	Microsoft Corporation	Windows Explorer
JIMMY278F	2884	CAWINDOWS\system32\ctfmon.exe	20000	Microsoft Corporation	CTF Loader

Finalmente, podemos usar el informe #dirlist para obtener más información sobre los archivos identificados a través de los escaneos YARA. Aquí podemos ver el tamaño del archivo, las marcas de tiempo, la verificación de firma digital, los hashes y más. La información proporcionada por #dirlist, como se muestra en la figura 16, debe ser más que suficiente para

validar las detecciones de las firmas YARA y determinar si es necesario adquirir memoria o imágenes de disco del sistema.

Figura 16

#Dirlist Módulo que Proporciona Detalles Para el Archivo Identificado por YARA

name	size	created	accessed	modified
C:\WINDOWS\system32\msieftp.dll	377856	2007-02-18T13:00:00Z	2014-02-26T00:05:59Z	2007-02-18T13:00:00Z
C:\WINDOWS\system32\msiexec.exe	124928	2008-05-22T03:45:46Z	2014-02-26T00:05:59Z	2008-05-22T03:45:46Z
C:\WINDOWS\system32\msihnd.dll	503296	2010-09-17T18:16:22Z	2014-02-26T00:05:59Z	2010-09-17T18:16:22Z
C:\WINDOWS\system32\msimg32.dll	6656	2007-02-18T13:00:00Z	2014-02-26T00:17:04Z	2007-02-18T13:00:00Z
C:\WINDOWS\system32\msimg.dll	2560	2008-05-22T03:45:46Z	2014-02-26T00:05:59Z	2008-05-22T03:45:46Z
C:\WINDOWS\system32\MSIMTF.dll	389632	2007-02-18T13:00:00Z	2014-02-26T00:16:56Z	2007-02-18T13:00:00Z
C:\WINDOWS\system32\msinit.exe	227840	2014-02-26T00:04:02Z	2014-02-26T00:06:20Z	2014-02-25T21:44:17Z
C:\WINDOWS\system32\msisip.dll	24064	2008-05-22T03:45:46Z	2014-02-26T00:05:59Z	2008-05-22T03:45:46Z
C:\WINDOWS\system32\mslbui.dll	36864	2007-02-18T13:00:00Z	2014-02-26T00:05:59Z	2007-02-18T13:00:00Z
C:\WINDOWS\system32\msls31.dll	223232	2009-03-08T09:25:42Z	2014-02-26T00:05:59Z	2009-03-08T09:25:42Z
C:\WINDOWS\system32\msobjx.dll	46080	2007-02-18T13:00:00Z	2014-02-26T00:05:59Z	2007-02-18T13:00:00Z
C:\WINDOWS\system32\msoeacct.dll	357888	2014-01-17T02:34:18Z	2014-02-26T00:05:59Z	2007-02-18T13:00:00Z
C:\WINDOWS\system32\msort2.dll	163328	2014-01-17T02:34:18Z	2014-02-26T00:05:59Z	2007-02-18T13:00:00Z

Exiftool:

Exchangeable Image File “EXIF” son datos que brindan información muy minuciosa y precisa sobre archivos digitales (imagen, audio y video).

Es decir, nos lleva a una vigilancia y búsqueda de datos por lo que debemos saber cómo acceder a ellos con la finalidad de recabar información valiosa para una investigación forense:

- Pueden ayudar a situar un evento o una persona en el tiempo y el espacio
- Conocer la cámara o el teléfono con el que se ha capturado una imagen fotográfica.

Borrar los propios datos:

- Como investigador forense se debe mantener la información personal lo más oculta posible y evitar dejar huellas que puedan comprometer el caso de investigación.

Para qué sirve ExifTool

ExifTool es un programa de código abierto el cual permite leer y operar metadatos de archivos digitales (imagen, audio y video).

Gracias a esta herramienta conocemos algunos de los metadatos que de un archivo tipo vídeo podríamos extraer:

- La hora y la fecha en la que se ha grabado.
- La marca y el modelo del dispositivo que se ha usado.
- Los parámetros de exposición.
- La ubicación geográfica (en el caso de que se haya grabado con la función de GPS activo).

Características de ExifTool

Posee un sinnúmero de características esta herramienta, exponemos algunas de ellas:

- Potente, rápido, flexible y personalizable
- Lee y escribe notas del creador de muchas cámaras digitales
- Copia metainformación entre archivos (incluso archivos de diferentes formatos)
- Crea un archivo de salida de texto para cada archivo de imagen
- Salidas avanzadas de volcado hexadecimal detallado y basadas en HTML

Ventajas de uso de ExifTool

Existen un sinnúmero de herramientas para conocer los datos EXIF, sin embargo, ExifTool posee estas grandes ventajas:

- Lectura de todos los metadatos del archivo, en los que se incluyen los datos específicos de los fabricantes de las cámaras digitales, de la misma manera con los archivos de audio y video.

- Soporte a través de una comunidad en la red, proporcionando actualizaciones y mejoras frecuentes, dentro de estos sitios se pueden encontrar guías y manuales actualizados.

Desventajas de uso de ExifTool

- La característica principal de esta herramienta es que funciona mediante órdenes por comandos de código abierto.
- GUI corresponde al acrónimo de Graphic User Interface y es la misma herramienta ExifTool pero con una interfaz gráfica.
- Sistemas operativos que soporta a través de una interfaz GUI son Windows y para MacOS.

Al final se tratará en un fichero pcap, de hacer muchas búsquedas y rebuscar entre los paquetes, sus raw y demás información hasta obtener alguna incidencia o quizás no porque no la haya. Pero al final será un trabajo arduo, ya que un análisis de red contiene muchísima información y no es fácil de detectar, salvo que tengamos indicios claros, de dónde puede provenir cualquier actividad maliciosa o fuera de lugar en nuestra red.

Autopsy

El proyecto de Autopsy Forensic es una herramienta de análisis forense. Y puede analizar sistemas de ficheros Linux y Windows. Es utilizado por la policía, militares e investigadores forenses que revisar lo que sucedió en un computador, dispositivo móvil o almacenamiento.

Autopsy es un proyecto Open Source, siendo compatible sobre las diferentes distribuciones de Windows y Linux. Ya que está basado en lenguaje de hipertexto, la conexión es muy sencilla ya que solo requerimos de un navegador HTML. Proporciona una interfaz amigable similar a un

gestor de ficheros y se puede observar en detalle la información sobre las estructuras de sistema de ficheros y datos borrados.

Ya que Microsoft Windows es el sistema operativo más utilizado y el proyecto Autopsy funciona nativamente en Windows es la solución forense más conocida.

Tipos de Análisis

- Análisis post-mortem (dead analysis) cuando un sistema de análisis dedicado es sospechoso se diseña un análisis para examinar los datos de un sistema. Para lo cual Autopsy normalmente se corre en un laboratorio o en un ambiente controlado. Cabe indicar que Autopsy soporta los formatos Advanced Forensic Format (AFF), Expert Witness y Raw.
- Análisis en vivo (live analysis) se ejecutan desde un CD en un entorno no controlado y ocurre cuando el sistema a ser analizado está en ejecución. Este método se utiliza ante la respuesta a un incidente o mientras el incidente de seguridad está siendo confirmado. Una vez confirmado, el análisis posterior sería un dead análisis (análisis post-mortem).

Características

- *Análisis de Archivos LNK*: Para identificar atajos para acceder a los Documentos analizados.
- *Análisis de Línea de Tiempo*: Muestra todos los eventos para identificar las actividades realizadas a través de una interfaz gráfica de línea de tiempo.
- *Análisis de Registro*: Para identificar los hechos o acceder a documentos utilizando Register Ripper.
- *Artefactos web*: Con la finalidad de identificar la actividad del usuario, a partir de la actividad web realizadas por el usuario utilizando navegadores comunes.

- *Keyword Search*: Prepara unos módulos para buscar menciones de archivos con términos específicos y también buscar aquellas expresiones regulares, patrones para la extracción de Texto.

Ventajas de usar Autopsy:

- *Fácil de usar*: la instalación es muy fácil y hay *wizards* disponibles para guiar en cada paso.
- *Flexible*: a través de la comunidad se ha desarrollado varios módulos que son de acceso público. Algunos de estos son los siguientes:
 - ✓ Filtrado hash: indicadores mencionados para reconocer archivos malos y archivos buenos.
 - ✓ Búsqueda por palabra clave: para buscar archivos, se utiliza una búsqueda por palabra clave indexada.
 - ✓ Artefactos web: extrae el historial del archivo de registro, los marcadores en el archivo y las cookies de varios navegadores web.
 - ✓ Data Carving: recupere archivos dañados al usar PhotoRec.
 - ✓ Multimedia: introduzca archivos EXIF de videos e imágenes.
 - ✓ Indicadores de compromiso: se utilizan para escanear usando STIX (lenguaje estructurado para amenazas cibernéticas).
- *Rápido*: Rápido significa que ejecuta todas las funciones de fondo lateralmente utilizando numerosas instancias y proporciona resultados tan pronto como se calculan.
- *Rentable*: Autopsy es un programa de código abierto.

CAPÍTULO 4

CONCLUSIONES

Partiendo de la Problemática del caso se obtienen las siguientes conclusiones.

- En la actualidad el uso diario de la tecnología en la cotidianidad de las actividades que son realizadas por parte de los sectores empresariales, sociales, educación, salud, etc., se ven expuestos a ataques perpetuados o dirigidos por cibercriminales, es por ello que se ha visto la necesidad de que la sociedad en general del Ecuador disponga de una entidad que le permita acceder a una base de datos de los profesionales en el campo de la ciberseguridad y ciencias forenses, las cuales podrán asesorarlos, capacitarlos y entre otros servicios que brindará la Entidad.
- La Asociación al disponer de alianzas publicas privadas, podrá garantizar una asesoría oportuna, eficiente, a la sociedad en general con el fin, de proteger su información en el ciberespacio.
- La Asociación se encargará de coordinar campañas de concientización a la sociedad en general sobre temas relacionados en ciberseguridad.
- Con la conformación de la AECIE, se ofrecerá a los profesionales ecuatorianos de ciberseguridad, la posibilidad de acceder a un proceso de capacitación continua y actualización de conocimientos ya que los tiempos de evolución de tecnología cada vez son más rápidos.
- Considerando que la Asociación dispone de una biblioteca de manuales y guías de uso, de las diferentes herramientas forenses esta deberá ser actualizada periódicamente.

- Con la creación de asociación se debe gestionar convenios y alianzas a nivel nacional e internacional con los diferentes organismos rectores y académicos en materia de la ciberseguridad.
- El llevar un registro de todos los profesionales dedicados a la rama de la ciberseguridad ofrece la opción de que en un futuro se pueda generar una bolsa de trabajo y asesoría en la contratación en este tipo de profesionales.
- Con el tiempo la asociación debe gestionar alianzas estratégicas con fabricantes de software y hardware con la finalidad de abaratar costo.
- Como siguiente paso la asociación procederá con la implementación de un laboratorio técnico especializado en ciberseguridad para uso de sus miembros.
- Actualmente se conoce que el exceso de confianza, la divulgación de información personal en las diferentes redes sociales que existen actualmente son las raíces y orígenes que motivan a cometer espionaje informático llevando esto a cometer delitos informáticos, es así, que durante la navegación en el ciberespacio nuestro propósito es defendernos y para lograr esto primero debemos aprender a atacar con la finalidad de conocer nuestro enemigo y sus vulnerabilidades.

REFERENCIAS

Gobierno Nacional del Ecuador . (2022). *www.gob.ec*. Obtenido de *www.gob.ec*:
<https://www.gob.ec/articulos/tramites-linea>

GONZÁLEZ LUCAS, O. B. (2013). *repositorio.upse.edu.ec*. Obtenido de *repositorio.upse.edu.ec*:
<https://repositorio.upse.edu.ec/bitstream/46000/956/1/TESIS%20GONZALEZ%20LUCAS%20OSCAR.pdf>

Ministerio de Inclusión Económico y Social MIES. (2017). *www.inclusion.gob.ec*. Obtenido de *www.inclusion.gob.ec*:
https://www.inclusion.gob.ec/wp-content/uploads/2018/08/requisitos_-_organizaciones_sociales_.pdf

MINTEL. (2022). Estrategia Nacional de Ciberseguridad del Ecuador. Quito. Obtenido de
<https://asobanca.org.ec/wp-content/uploads/2022/08/ESTRATEGIA-NACIONAL-DE-CIBERSEGURIDAD-DEL-ECUADOR-2022481.pdf>

normaiso27001. (25 de noviembre de 2022). *A9 CONTROL DE ACCESO*. Obtenido de
<https://normaiso27001.es/a9-control-de-acceso/>

Acosta, Pastor. 2009. “Seguridad nacional y ciberdefensa”,
catedraisdefe.etsit.upm.es/wp-content/uploads/2010/07/CUADERNO-Nº-6.pdf.

Andes. 2013. “Sistema informático electoral del Ecuador sufrió ciberataque desde un país del primer mundo”,

<http://www.andes.info.ec/es/noticias/sistema-informatico-electoral-ecuador-sufrio-ciberataque-pais-primer-mundo.html>.

Cepik, Marco. 2003 “Espionagem e democracia”,

http://professor.ufrgs.br/marcocepik/files/cepik_-_2003_-_fgv_-_espionagem_e_democracia_21-apr-14_1.compressed.pdf.

CIBERSEGURIDAD (2022), PLAN DE CONCIENCIACIÓN DE SEGURIDAD
INFORMÁTICA

<https://ciberseguridad.com/normativa/espana/medidas/plan-concienciacion/>

Comisión federal de comercio (2022) Conceptos básicos sobre seguridad informática para
pequeños negocios

[https://www.ftc.gov/es/guia-para-negocios/conceptos-basicos-sobre-seguridad-
informatica-para-pequenos-negocios](https://www.ftc.gov/es/guia-para-negocios/conceptos-basicos-sobre-seguridad-informatica-para-pequenos-negocios)

Choucri, Nazli, y David Clark. 2013. “Who controls cyberspace?”.

Bulletin of Atomic Scientists 5 (69): 21-31.

Ecuador Universitario. 2012. “El contexto de la Ciberseguridad”,

<http://ecuadoruniversitario.com/ciencia-y-tecnologia/el-contexto-de-la-ciberseguridad/>.

El Comercio. 2014. “Ecuador implementará un Comando de Ciberdefensa”. 09 de septiembre,

[http://www.elcomercio.com/actualidad/ciberdefensa-ecuador-comando-fuerzasarmadas-
ministerioddefensa.html](http://www.elcomercio.com/actualidad/ciberdefensa-ecuador-comando-fuerzasarmadas-ministerioddefensa.html).

El Telégrafo. 2014. “Ecuador escala 9 puestos en ranking de aplicación de las TIC”. 25 de abril,

[http://www.eltelegrafo.com.ec/noticias/tecnologia/30/ecuador-escala-9-puestos-en-r
anking-de-aplicacion-de-las-tic](http://www.eltelegrafo.com.ec/noticias/tecnologia/30/ecuador-escala-9-puestos-en-r
anking-de-aplicacion-de-las-tic).

El Universo. 2009. “Ciberataques a sitios web de Ecuador”. 13 de mayo,

[http://www.eluniverso.com/2009/05/13/1/1431/82615AC354164A25ABE48FCDE222C4
8E.html](http://www.eluniverso.com/2009/05/13/1/1431/82615AC354164A25ABE48FCDE222C4
8E.html).

INCIBE (2022), Kit de concienciación

<https://www.incibe.es/protege-tu-empresa/kit-concienciacion>

Kaspersky (2022), Las siete principales amenazas de ciberseguridad a las que debes estar atento

<https://latam.kaspersky.com/resource-center/threats/top-7-cyberthreats>

__. 2012. “Anonymous inicio ataque a web oficiales en Ecuador”. 11 de septiembre,

<http://www.elcomercio.com/actualidad/negocios/anonymous-inicio-ataque-a-web.html>.

__. 2016. “Hackers de Rusia, China, EE.UU. y Francia dirigen ataques a Ecuador”. 29 de octubre,

<http://www.elcomercio.com/actualidad/hackers-rusia-ecuador-ciberataques-seguridad.html>.

__. 2014. “Formación militar prevé ciberdefensa”. 21 de mayo,

<http://www.eluniverso.com/noticias/2014/05/21/nota/2991356/formacion-militar-preve-ciberdefensa>.

APÉNDICES**Apéndice A** *Modelo de Estatuto de la Asociación Sin Fines de Lucro*

ESTIMADO/A USUARIO/A

Esta guía fue elaborada de acuerdo a la Constitución y la normativa legal para su utilización, a fin de orientar el proceso de aprobación del estatuto y el otorgamiento de la personalidad jurídica de una Fundación/Asociación/Corporación.

Recuerde que el ámbito de competencias del Ministerio de Inclusión Económica y Social – MIES para aprobar estatutos y otorgar personalidad jurídica a las organizaciones sociales tienen que ver con los grupos de atención prioritaria y la población que se encuentra en situación de pobreza y vulnerabilidad, promoviendo el desarrollo y cuidado durante el ciclo de vida, la movilidad social ascendente y fortaleciendo a la economía popular y solidaria a nivel nacional a través de las competencias desconcentradas en las Coordinaciones Zonales y Direcciones Distritales

Para conformar una organización se requieren mínimo 1 persona para Fundación y 5 personas para una Asociación/Corporación.

La finalidad de estas organizaciones es la búsqueda o promoción del bien común de la sociedad en todos los aspectos sociales, así como actividades relacionadas con la filantropía y beneficencia pública.

SÍRVASE LEER Y (dando click) COMPLETAR O ELEGIR LA INFORMACIÓN QUE SE SOLICITA EN LOS CAMPOS PERMITIDOS PARA SU ESCRITURA DE ACUERDO A SU INTERÉS Y VOLUNTAD DE LIBRE ASOCIACIÓN.

Recuerde que los trámites en este Portafolio de Estado no tienen costo.

AL FINALIZAR

NO IMPRIMIR ESTA PÁGINA

ESTATUTO DE LA ASOCIACIÓN

CAPITULO I

CONSTITUCIÓN, DENOMINACIÓN, ÁMBITO DE ACCIÓN, DOMICILIO, ALCANCE TERRITORIAL Y DURACIÓN

Art. 1.- CONSTITUCIÓN Y DENOMINACIÓN: Se constituye la Fundación / Asociación / Corporación: XXXXXXXX. como una organización de derecho privado sin fines de lucro, con patrimonio propio, administración autónoma; con capacidad legal para ejercer derechos y contraer obligaciones.

La Organización se regirá de conformidad con la Constitución del Estado, las disposiciones del Código Civil, por el presente Estatuto y demás disposiciones legales que sean aplicables.

Art. 2.- ÁMBITO DE ACCIÓN: La Organización tendrá como ámbito de acción: Proponer y ejecutar programas y servicios de XXXX (ámbito de trabajo, no geográfico).

Art. 3.- DOMICILIO: La Organización tendrá su domicilio en Haga clic aquí para escribir texto.
(Dirección completa)

Art. 4.- ALCANCE TERRITORIAL DE LA ORGANIZACIÓN. - La Organización cumplirá con su ámbito de acción, fines y objetivos a nivel Elija un elemento. Además, podrá operar a nivel internacional previo el cumplimiento de la normativa legal pertinente.

Art. 5.- PLAZO DE DURACIÓN La Organización tiene como plazo de duración Elija un elemento., pudiendo disolverse por las causales aquí establecidas.

CAPITULO II

FINES, OBJETIVOS Y DECLARACIÓN DE REALIZAR ACTIVADES DE VOLUNTARIADO

Art. 6.- FINES: La Organización tiene como fines: Proponer y ejecutar programas y servicios de

XXXXXXXXXXXX

Art. 7.- OBJETIVOS: La Organización tiene los siguientes objetivos: (Los que requiera la organización social de acuerdo a su realidad)

1.-

2.-

3.-

4.-

Art. 8.- DECLARACIÓN: La Organización en este acto precisa que Elija un elemento. realizará programas y/o actividades de voluntariado de acción social y desarrollo.

CAPITULO III

DE LOS MIEMBROS, CLASES DE MIEMBROS, DERECHOS Y OBLIGACIONES,
MECANISMOS DE INCLUSION Y EXCLCUSIÓN, REGIMEN DISCIPLINARIO

TÍTULO I

DE LOS MIEMBROS, CLASES DE MIEMBROS, DERECHOS Y OBLIGACIONES

Art. 9.- CLASES DE MIEMBROS. - Son miembros de la Organización:

- a) Fundadores: Las personas que suscribieron el Acta Constitutiva, tienen voz y voto;
- b) Adherentes: Los que posteriormente expresen su voluntad y soliciten por escrito su ingreso adjuntando fotocopia de su documento de identificación y otros documentos específicos de acuerdo a su composición asociativa, y fueren aceptados por la Asamblea General, tienen voz y voto; y,
- c) Honorarios: La Asamblea General podrá nombrar miembros Honorarios a las personas naturales o jurídicas que hubieren realizado actos en beneficio de la Organización para el cumplimiento de sus fines y objetivos; de igual manera podrá quitar dicha calidad si sus actos

públicos o privados son contrarios a la ley. Esta clase de miembros podrán participar con voz, pero sin voto cuando sean invitados a las sesiones de asambleas generales. Los deberes y obligaciones no aplican a esta clase de miembros.

En general, para ser miembro se requiere cumplir con los requisitos de ley y específicos de acuerdo a su composición asociativa; así como, tener capacidad jurídica o ser representado conforme la normativa legal.

Art. 10.- SUSPENSIÓN Y PÉRDIDA DE LA CALIDAD DE MIEMBRO: Se suspende la calidad de miembro por el incumplimiento de las obligaciones y demás disposiciones de este estatuto; y se pierde la calidad de miembro por:

- a) Renuncia voluntaria que se presentará por escrito ante el Presidente;
- b) Por expulsión; previo el derecho a la defensa; y,
- c) Por fallecimiento.

Art. 11.- DERECHOS DE LOS MIEMBROS. - Son derechos de los miembros fundadores y adherentes los siguientes:

- a) Elegir y ser elegido para el desempeño de dignidades en la Directiva y/o comisiones;
- b) Concurrir e intervenir con voz y voto en las deliberaciones de las Asambleas Generales;
- c) Gozar de todos los beneficios que presta la Organización y acogerse a todas las prerrogativas establecidas en este Estatuto;
- d) Demandar ante la Directiva y en última instancia a la Asamblea General, el cumplimiento de las disposiciones estatutarias y/o reglamentarias;
- e) Solicitar y obtener de la Directiva los informes relacionados con la Administración, manejo y destino de los recursos;
- f) Exigir a la Directiva y a la Asamblea General el reconocimiento de sus derechos;

- g) Formular ante la Directiva o la Asamblea General, propuestas, sugerencias y recomendaciones que crean convenientes para la consecución de los fines, objetivos y buena marcha de la Organización; y,
- h) Los demás que les corresponda conforme al Estatuto y demás disposiciones legales.

Art. 12.- OBLIGACIONES DE LOS MIEMBROS. - Son obligaciones de los miembros fundadores y adherentes las siguientes:

- a) Cumplir y hacer cumplir las disposiciones del presente Estatuto, Reglamento y las Resoluciones legalmente aprobadas por la Asamblea General y la Directiva; (su incumplimiento será falta grave);
- b) Concurrir de manera puntual a las sesiones de Asamblea General cuando fueren convocados legalmente; (su incumplimiento será falta leve);
- c) Cumplir las comisiones que se le encomendaren; (su incumplimiento será falta leve);
- d) Pagar las cuotas de ingreso, ordinarias y extraordinarias que se acuerden legalmente; (su incumplimiento será falta grave);
- e) Desempeñar con ética y responsabilidad los cargos para los que fueren elegidos, salvo caso de fuerza mayor o caso fortuito; (su incumplimiento será falta grave);
- f) Intervenir activamente en las actividades que organice o se promuevan en el seno de la Organización; (su incumplimiento será falta grave);
- g) Brindar la ayuda y colaboración necesaria para lograr el engrandecimiento y prestigio de la Organización; (su incumplimiento será falta leve);
- h) Guardar el debido respeto y consideraciones entre los miembros; (su incumplimiento será falta leve);

- i) No dañar el buen nombre de la Organización, de sus dirigentes y compañeros; (su incumplimiento será falta grave);
- j) Las demás que les corresponda conforme al Estatuto y demás disposiciones legales.

Art. 13.- Todo miembro gozará de los derechos consignados en este Estatuto, la ley y la Constitución, a menos que se encuentre suspendido de su calidad por evidente y notorio incumplimiento de sus obligaciones y demás disposiciones del estatuto y/o hubiere sido sancionado legalmente con la pérdida de su calidad.

TITULO II

MECANISMOS DE INCLUSIÓN O EXCLUSIÓN DE MIEMBROS

Art. 14.- MECANISMOS DE INCLUSIÓN: Para ser incluidos como miembros será necesario que el interesado presente al Presidente de la organización su solicitud escrita en dónde exprese su voluntad de ingresar a la organización, adjuntando fotocopia de su documento de identificación y otros documentos específicos de acuerdo a su composición asociativa, con detalle de cuáles.

La Directiva procederá a revisar, analizar y emitir criterio positivo o negativo sobre las solicitudes de ingreso de nuevos miembros, para la aceptación o negativa de la Asamblea General, quién emitirá su pronunciamiento en Asamblea General

El Presidente de la Organización notificará y solicitará a la autoridad competente el registro del ingreso/inclusión de los miembros, de forma inmediata.

Art. 15.- MECANISMOS DE EXCLUSIÓN: El miembro puede solicitar en cualquier tiempo su exclusión/retiro/salida voluntaria, para lo cual presentará su solicitud en donde exprese su voluntad con fotocopia de su documento de identificación.

El miembro podrá ser excluido por inobservar e incumplir de forma reiterada (más de dos veces en el año) decisiones de la Asamblea General, la Directiva, las estipulaciones del estatuto, la ley, la Constitución y demás disposiciones legales.

En todo momento se garantizará al miembro el debido proceso, derecho a defenderse y presentar prueba de descargo. El miembro de la Organización comparecerá ante la Asamblea General en el plazo de diez (10) días de haber sido notificado por escrito por el presidente y secretaria de la directiva con el juzgamiento para ejercer su derecho a la defensa, la que luego de escuchar los alegatos y analizar las pruebas de descargo, emitirá su fallo de última y definitiva instancia, dentro del plazo de hasta (05) días.

El Presidente de la Organización notificará y solicitará a la autoridad competente el registro de la salida/exclusión de los miembros, de forma inmediata.

TITULO III

REGIMEN DISCIPLINARIO

Art. 16.- FALTAS DISCIPLINARIAS: Existen las siguientes faltas disciplinarias:

- a) Faltas leves; y,
- b) Faltas graves.

Art. 17.- Son Faltas leves:

- a) La inasistencia injustificada a dos sesiones de la Asamblea General, de la Directiva o comisiones;
- b) La falta de puntualidad en la asistencia a las sesiones dispuestas por la Asamblea General o la Directiva;
- c) Incumplimiento o negligencia en las tareas encomendadas por la Asamblea General o la Directiva dentro de las comisiones designadas; y,

d) otras que se deriven del incumplimiento de sus obligaciones.

Art. 18.- Las faltas leves merecerán la amonestación escrita en primera instancia por la Directiva.

Art. 19.- Son Faltas graves:

- a) Reincidir por más de dos ocasiones en faltas leves; (sanción pecuniaria)
- b) Actuar en nombre de la Organización, sin la debida autorización de la Asamblea General o la Directiva; (sanción de suspensión temporal de un mes hasta tres meses)
- c) Tomar el nombre de la Organización en asuntos que no sean de su interés; (sanción de suspensión temporal de un mes hasta tres meses)
- d) Realizar actividades que afecten los intereses de la Organización o que promuevan la división entre sus miembros; (sanción de suspensión temporal de un mes hasta tres meses)
- e) Faltar de palabra o de obra a los miembros; (sanción de suspensión temporal de un mes hasta tres meses)
- f) Defraudación o malversación de los recursos de la Organización; (sanción de expulsión)
- g) Haber sido condenado a penas de privación de libertad; y, (sanción de suspensión temporal hasta que dure su interdicción)
- h) Otras que se deriven del incumplimiento de sus obligaciones.

Art. 20.- Las sanciones a las faltas graves serán las siguientes:

- a) Sanción pecuniaria (será resuelta en asamblea general o en el reglamento interno)
- b) Suspensión temporal de un mes hasta tres meses y/o hasta que dure su interdicción en caso de encontrarse privado de la libertad; (No le exime de seguir cumpliendo con sus obligaciones económicas);
- c) Destitución del cargo, en caso de ser miembro de la Directiva; y,
- d) Expulsión.

Art. 21.- El miembro de la Organización comparecerá ante la Asamblea General con su apelación en el plazo de diez (10) días de haber sido notificado por escrito por el presidente y secretaria de la directiva con la resolución del juzgamiento para ejercer su derecho.

Art. 22.- Las amonestaciones y sanciones a las faltas leves y graves en segunda y última instancia serán impuestas por la Asamblea General en el plazo de hasta cinco (5) días, luego de practicado el juzgamiento en el que se le haya dado al miembro el derecho de defensa y presentación de pruebas, la que luego de escuchar los alegatos y analizar las pruebas de descargo, emitirá su fallo de última y definitiva instancia.

CAPITULO IV

ESTRUCTURA ORGANIZACIONAL

Art. 23.- Para su funcionamiento la Organización contará con la siguiente estructura organizacional:

- a) La Asamblea General;
- b) La Directiva (Presidente, Vicepresidente, Secretario y Tesorero); y
- c) Las Comisiones.

Los cargos serán de confianza, honoríficos y ad honorem; así como la integración de las comisiones. No obstante, tendrán derecho al reembolso de los gastos de desplazamiento que hubieren de efectuar para asistir a las reuniones de los órganos de que formen parte, y de cuantos otros se les causen, en el desempeño de cualquier misión concreta que se les confíe en nombre o interés de la Organización, para el cumplimiento de sus fines y objetivos. La Asamblea General fijará el monto mínimo y máximo de los reembolsos y honorarios de ser el caso.

TÍTULO I

ATRIBUCIONES Y DEBERES DE LOS ÓRGANOS INTERNOS:

DE LA ASAMBLEA GENERAL

Art. 24.- LA ASAMBLEA GENERAL. - Es el máximo organismo de la Fundación/Asociación/Corporación, está conformada por todos los miembros fundadores y adherentes legalmente convocados, quienes tendrán derecho a un solo voto. Sus decisiones son obligatorias, siempre que no se contrapongan al presente Estatuto, la Constitución y demás leyes.

Art. 25.- ATRIBUCIONES Y DEBERES DE LA ASAMBLEA GENERAL:

- a) Aprobar el reglamento interno de la Organización y sus reformas;
- b) Aprobar las reformas al Estatuto;
- c) Aceptar o negar el ingreso de nuevos miembros, previo informe de la Directiva; y, entregar un ejemplar del estatuto y reglamento interno en caso de existir al nuevo miembro para su conocimiento. Conocer y resolver en segunda y última instancia sobre la exclusión de miembros por inobservancia a las disposiciones del estatuto, resoluciones, la ley y la constitución;
- d) Conocer y resolver en segunda y última instancia sobre las faltas leves y graves;
- e) Elegir las dignidades de la Directiva en el tiempo y la forma que se haya contemplado en el artículo 23 de este estatuto mediante votación Elija un elemento.; y en caso de renuncia o ausencia temporal o definitiva le sucederá quien establezca el presente estatuto; si no existiera disposición será elegida por la asamblea general; y, destituirlos por el incumplimiento de sus atribuciones y deberes en cualquier tiempo;
- f) Conocer los informes de cada una de las actividades que realice la Directiva;

- g) Conocer y resolver sobre el plan de actividades y el presupuesto que presente la Directiva, dentro de los primeros meses de cada año;
- h) Fijar, aprobar y modificar las cuotas de ingreso, así como las ordinarias y extraordinarias y definir su utilización;
- i) Conocer, aprobar, negar u observar el informe semestral o anual que presente la Directiva a través del Presidente sobre la ejecución de sus actividades;
- j) Solicitar a la Directiva cuanto informe estime necesario para conocer, aprobar, negar u observar sus actuaciones;
- k) Ordenar la fiscalización de los recursos económicos y financieros en cualquier momento en que así lo considere conveniente;
- l) Autorizar al Presidente y Tesorero la suscripción de actos y contratos cuyo monto exceda de remuneraciones básicas mínimas unificadas;
- m) Aprobar y resolver sobre la compra, venta, hipoteca y demás gravámenes sobre los bienes de la Organización, cuyo valor o avalúo sea igual o superior a remuneraciones básicas mínimas unificadas;
- n) Aceptar o rechazar las donaciones que se hicieren a la Organización;
- o) Resolver sobre la disolución, liquidación y el destino de sus bienes según la normativa que rige a las organizaciones sin fines de lucro.
- p) Conocer en segunda y última instancia sobre las denuncias y demás actos internos que hayan o no sido resueltos por la Directiva;
- q) Nombrar una comisión especial para que ejerza el control y supervisión sobre el funcionamiento y cumplimiento de las obligaciones estatutarias, constituyéndose como órgano de fiscalización y control interno que no forma parte de la estructura organizacional;

r) Establecer o fijar un monto de reembolso por concepto de viáticos o gastos, de ser el caso, para los miembros de la Directiva y de las comisiones, por el cumplimiento de sus actividades, siempre y cuando hayan sido justificados, será reglamentado o acordado en asamblea general; (sin perjuicio de que los cargos directivos y de las comisiones serán de confianza, honoríficos y ad honorem)

CLASES DE ASAMBLEA GENERAL, LA FORMA Y LAS EPOCAS DE CONVOCAR A LAS ASAMBLEAS GENERALES

Art. 26.- CLASES DE ASAMBLEA GENERAL. - Las Asambleas Generales puede ser de dos clases: Ordinarias o Extraordinarias.

Art. 27.- LA ASAMBLEA GENERAL ORDINARIA. - La Asamblea General Ordinaria se reunirá Haga clic aquí para escribir texto. veces al año, por convocatoria del Elija un elemento. La convocatoria se realizará con por lo menos Haga clic aquí para escribir texto. día(s) de anticipación, con señalamiento del lugar, día, hora, y el orden del día a tratar.

Art. 28.- LA ASAMBLEA GENERAL EXTRAORDINARIA. - La Asamblea General Extraordinaria se reunirá cuando el caso lo requiera, por convocatoria del Elija un elemento., debiendo convocarse con al menos Haga clic aquí para escribir texto. día(s) de anticipación, con señalamiento del lugar, día, hora y el orden del día a tratar y sólo para tratar los asuntos puntualizados en la Convocatoria.

Art. 29.- LA AUTO-CONVOCATORIA. - En el supuesto de no cumplirse con lo dispuesto en los artículos inmediatos anteriores, la organización puede convocarse (auto-convocatoria) con la firma de la mitad más uno de los miembros que la conforman, registrados ante la autoridad competente y que se encuentren al día en sus obligaciones, con señalamiento del lugar, día, hora, y el orden del día a tratar.

Art. 30.- La convocatoria se realizará por cualquier medio que justifique el conocimiento de sus miembros, prefiriendo aquella que deje constancia de su recepción, debiendo contener la fecha de emisión del documento, clase de Asamblea o reunión, dirección completa, día y hora de la reunión, el orden del día y la advertencia respecto a la falta de quórum de instalación.

QUÓRUM PARA LA INSTALACIÓN DE LAS ASAMBLEAS GENERALES Y

EL QUÓRUM DECISORIO

Art. 31.- QUÓRUM PARA LA INSTALACIÓN DE LAS ASAMBLEAS GENERALES: La Asamblea General puede instalarse con la mitad más uno de sus miembros (registrados ante la autoridad competente y que estén al día con sus obligaciones antes de tomar las decisiones). Si no existiera el quórum de instalación necesario a la hora señalada, se podrá sesionar Haga clic aquí para escribir texto. hora(s) más tarde o se realizará una segunda convocatoria y se sesionará con los miembros presentes. Este particular se hará constar en la convocatoria para su validez.

Art. 32.- Las sesiones de Asamblea General estarán presididas y dirigidas por el Presidente, en su ausencia por el Vicepresidente, y a falta de ellos por un Director de Asamblea, nombrado de entre sus miembros.

Art. 33.- QUÓRUM DECISORIO: En la Asamblea General, el quórum decisorio será por simple mayoría de votos de los presentes; en caso de empate, tendrá voto dirimente el Presidente o el Director de la Asamblea.

Art. 34.- De cada Asamblea General deberá elaborarse un acta que será leída a los presentes para su aprobación Elija un elemento.; contendrá la firma del Presidente o de quien haya presidido la Asamblea y del Secretario de la Directiva o quien haya actuado como Secretario ad-hoc.

TÍTULO II

DE LA DIRECTIVA, FORMA DE ELECCIÓN DE LAS DIGNIDADES Y DURACIÓN EN FUNCIONES, ATRIBUCIONES

Art. 35.- LA DIRECTIVA. - Es el órgano ejecutivo de la organización elegido de entre sus miembros (o no) por la Asamblea en Asamblea General Elija un elemento., (registrados ante la autoridad competente y que estén al día con sus obligaciones). Elija un elemento. y estará integrado por las siguientes dignidades:

- a) Presidente,
- b) Vicepresidente,
- c) Secretario; y,
- d) Tesorero.

Art. 36.- DURACIÓN EN FUNCIONES:

La Directiva durará Haga clic aquí para escribir texto. AÑOS, en sus funciones. El periodo de duración será expreso, colocándose la fecha de inicio (día, mes y año) y la fecha de finalización (día, mes y año).

Con por lo menos 30 días anteriores a la finalización del periodo de funciones se debe convocar y elegir la nueva directiva. En caso de no realizarse la convocatoria y la asamblea general para la elección de la nueva directiva en el tiempo aquí estipulado y la organización quedare sin directiva vigente se convocarán (auto-convocatoria) con la firma de la mitad más uno de los miembros que conforman la organización para el efecto.

Art. 37.- ALTERNABILIDAD. - Se establece la reelección consecutiva por una sola vez, luego de lo cual debe pasar por lo menos un periodo para ser electo nuevamente para la misma dignidad, acatando el principio constitucional de la alternabilidad de los dirigentes.

Art. 38.- ATRIBUCIONES Y DEBERES DE LA DIRECTIVA:

- a) Cumplir y hacer cumplir el presente Estatuto, el Reglamento Interno y las resoluciones de la Asamblea General o de la propia Directiva;
- b) Vigilar el normal funcionamiento, así como conservar en forma organizada toda la información y documentos de la organización;
- c) Elaborar el Reglamento Interno y demás instrumentos necesarios de carácter general, y someterlos a la Asamblea General para su aprobación;
- d) Formular los proyectos de reforma del Estatuto que creyere del caso y someter a la Asamblea General para su aprobación;
- e) Elaborar y poner en conocimiento por intermedio de su Presidente a la Asamblea General el presupuesto y plan anual de programas o actividades para su aprobación;
- f) Utilizar con celo y responsabilidad los fondos de la Organización, así como de sus bienes muebles e inmuebles; siempre habrá actas de entrega-recepción de todos los bienes de la organización y responderán por su mal uso o pérdida atribuida a su negligencia;
- g) Conformar comisiones que se requieran de entre los miembros, previa su aceptación y que deban cumplir actividades de carácter especial, y que tengan relación con el ámbito de acción, fines y objetivos de la Organización;
- h) Conocer y aceptar las renunciaciones voluntarias de los miembros y las exclusiones por fallecimiento; de igual manera, conocerá y resolverá en primera instancia sobre la exclusión de miembros por la inobservancia a las disposiciones del estatuto, resoluciones, la ley y la Constitución, previo el derecho al debido proceso;
- i) Conocer y resolver sobre las faltas leves y graves en primera instancia;
- j) Conocer y resolver sobre los requerimientos, denuncias y demás actos generados por los miembros o terceras personas;

- k) Adoptar resoluciones transitoriamente sobre asuntos no contemplados en este Estatuto hasta que se reúna la Asamblea General, y ratifique o revoque lo aprobado;
- l) Revisar, analizar y emitir criterio/informe positivo o negativo sobre las solicitudes de ingreso de nuevos miembros, para la aceptación o negativa de la Asamblea General;
- m) Rendir cuentas a sus miembros, a través de su Presidente, al menos una vez por año, por iniciativa propia o a petición de dos miembros de la directiva o por las dos terceras partes de los miembros de la organización. La rendición se cumplirá respecto del período de sus funciones aun cuando estas hubieren finalizado;
- n) Son responsables de sus actos frente a la misma en los términos previstos en la Constitución y demás normativa legal; y,
- o) Las demás que le correspondan conforme al Estatuto y demás disposiciones legales.

Art. 39.- La Directiva sesionará ordinariamente cada Elija un elemento. días en forma obligatoria, la convocatoria la realizará el Presidente o por dos de sus miembros con por lo menos Haga clic aquí para escribir texto. día(s) de anticipación, señalándose lugar, día, hora y orden del día a tratar; y, sesionará extraordinariamente cuando fuere necesario siguiendo el procedimiento anterior.

Art. 40.- El quórum para sesionar la Directiva y tomar decisiones válidamente será la mitad más uno de sus miembros.

De cada reunión de la Directiva deberá elaborarse un acta que será leída a los presentes para su aprobación Elija un elemento., contendrá la firma del Presidente o de quien haya presidido la reunión y del Secretario de la Directiva o quien haya actuado en su reemplazo.

Art. 41.- Las resoluciones adoptadas por la Directiva se pondrán en conocimiento de la Asamblea General; y tratándose de inclusión o exclusión de miembros se observará los tiempos y el procedimiento a seguirse.

ATRIBUCIONES DE LOS MIEMBROS DEL DIRECTORIO

Art. 42.- ATRIBUCIONES Y DEBERES DEL PRESIDENTE:

- a) Ejercer la representación legal, judicial y extrajudicial de la Organización;
- b) Actuar como tal en las sesiones de la Asamblea General y de la Directiva, con derecho a voz y voto, y, si no fuera miembro con derecho a voz (conforme el artículo 35);
- c) Presidir las sesiones ordinarias y extraordinarias de Asambleas Generales y de la Directiva.
- d) Cumplir y hacer cumplir las disposiciones estatutarias y reglamentarias; así como las resoluciones de Asambleas Generales y de la Directiva;
- e) Legalizar con su firma la correspondencia, actas y demás documentos de la Organización conjuntamente con el Secretario;
- f) Realizar y firmar conjuntamente con el Secretario, las convocatorias, el orden del día para las sesiones y las actas de las asambleas generales y de la directiva; y, revisar para firmar las actas que serán leídas a los presentes para su aprobación Elija un elemento.;
- g) Suscribir convenios, contratos o autorizar los egresos u obligaciones en los montos en que está autorizado;
- h) Supervisar y controlar el movimiento económico de tesorería;
- i) Girar y manejar la cuenta bancaria o de ahorros de la Organización, conjuntamente con el Tesorero;

j) Elaborar el informe anual de actividades y presentarlos a consideración de la Asamblea General;

Organizar conjuntamente con los integrantes de la directiva todos los actos y eventos para cumplir con los fines y objetivos de la Organización;

k) Receptar las solicitudes de ingreso de nuevos miembros, para la aceptación o negativa de la Asamblea General; y,

l) Las que le correspondan conforme al Estatuto y demás disposiciones legales.

Art. 43.- En caso de ausencia del Presidente de la Organización, le subrogará el Vicepresidente, con las mismas atribuciones y deberes hasta el término de su período, o mientras dure dicha ausencia si fuere temporal.

Art. 44.- ATRIBUCIONES Y DEBERES DEL VICEPRESIDENTE:

a) Subrogará al Presidente con las mismas atribuciones y deberes, en ausencia temporal o definitiva del mismo, según fuere el caso.

b) Actuar como tal en las sesiones de la Asamblea General y de la Directiva, con derecho a voz y voto; y, si no fuera miembro con derecho a voz (conforme el artículo 35);

c) Además cumplirá las comisiones que se le encomiende.

Art. 45.- ATRIBUCIONES Y DEBERES DEL SECRETARIO:

a) Actuar como tal en las sesiones de la Asamblea General y de la Directiva, con derecho a voz y voto, y, si no fuera miembro con derecho a voz (conforme el artículo 35); y elaborar las respectivas actas de las mismas;

b) Suscribir conjuntamente con el Presidente las convocatorias, el orden del día para las sesiones y las actas de las asambleas generales y de la directiva; y, redactar para firmar las actas que serán leídas a los presentes para su aprobación Elija un elemento.;

- c) Firmar conjuntamente con el Presidente las comunicaciones, acuerdos, resoluciones, etc;
- d) Dar el trámite correspondiente a las resoluciones de la Asamblea General y de la Directiva, para su cumplimiento;
- e) Certificar y conservar en orden, numerada, organizada, sistematizada, cuidado y protección todos los archivos y documentos; y cuando termine su periodo entregar mediante la respectiva acta a su sucesor;
- f) Llevar de forma organizada la nómina de todos los miembros (fundadores-adherentes-honorarios-incluidos-excluidos) con los respectivos datos personales (nombres y apellidos completos, nacionalidad y número de documento de identificación);
- g) Las que le correspondan conforme al Estatuto y demás disposiciones legales.

Art. 46.- ATRIBUCIONES Y DEBERES DEL TESORERO:

- a) Actuar como tal en las sesiones de la Asamblea General y de la Directiva, con derecho a voz y voto, y, si no fuera miembro con derecho a voz (conforme el artículo 35);
- b) Llevar e informar a la Asamblea General y Directiva en forma correcta la contabilidad;
- c) Realizar y mantener actualizado el inventario de los bienes, siendo responsable de los mismos conjuntamente con el Presidente;
- d) Recaudar las cuotas/dinero que por cualquier concepto se hayan legalmente resuelto y depositar en la cuenta bancaria que se hubiere aperturado para tal efecto, máximo en 48 horas luego de la recaudación;
- e) Suscribir los egresos conjuntamente con el Presidente; serán civil y penalmente responsables de aquellos que se hubieren hecho sin la debida autorización;

- f) Cancelar los vales, planillas, facturas y demás obligaciones de la Organización, verificando los documentos de respaldo; siempre que estuvieren expresamente autorizados por el Presidente, la Asamblea General o el estatuto;
- g) Presentar trimestralmente y por escrito a la Directiva, anualmente o cuando se le requiera a la Asamblea General un informe completo del movimiento económico y estado de situación financiera;
- h) Firmar los cheques en forma conjunta con el Presidente y/o las papeletas de retiro;
- i) Presentar mensualmente para el conocimiento de la Directiva la nómina de los miembros que estuvieren en mora del pago de sus cuotas ordinarias o extraordinarias, para los efectos previstos en este estatuto;
- j) Entregar con inventario a su sucesor todos los documentos que están a su cargo, previa acta de entrega- recepción; y,
- k) Las que le correspondan conforme al Estatuto y demás disposiciones legales.

TITULO III

DE LAS COMISIONES

Art. 47.- DE LAS COMISIONES: Es importante recalcar que las Comisiones no son parte de la Estructura Organizacional; sin embargo, a criterio de la Directiva y con el fin de cumplir con el ámbito de acción, fines y objetivos puede crear Comisiones permanentes, temporales u ocasionales, que serán ocupadas por los miembros previo su aceptación. De ser el caso, para una mejor organización nombraran un coordinador y elaboran informes de sus actividades para ser presentadas a la Directiva.

Las Comisiones pueden ser para asuntos sociales, educación, cultura, deportes, relaciones públicas, salud, etc., según las necesidades de la Organización.

La Asamblea General nombrará una comisión especial para que ejerza el control y supervisión sobre el funcionamiento y cumplimiento de las obligaciones estatutarias, por lo que, se constituirá como una fiscalizadora y control interno.

Son responsables de sus actos frente a la misma en los términos previstos en la Constitución y demás normativa legal.

De igual manera, pueden ser ocupadas por personas voluntarias, previo la firma del documento que certifique que su trabajo o actividades serán de voluntariado. (esto en caso de que sí sean voluntarios)

CAPITULO V

PATRIMONIO SOCIAL Y ADMINISTRACIÓN DE RECURSOS

Art. 48.- PATRIMONIO SOCIAL: Constituye el Patrimonio Social de la Organización y son fuentes de ingreso para cumplir con los fines y objetivos, los siguientes:

- a) Las cuotas de ingreso o aportaciones ordinarias y/o extraordinarias legalmente aprobadas; y que tienen el carácter de no reembolsables; así como las recaudadas por las sanciones pecuniarias;
- b) Los bienes que adquiera a cualquier título;
- c) Los bienes que sean donados y aceptados, de ser procedente se aceptará con beneficio de inventario;
- d) Los recursos económicos que provengan de colectas, promociones y otras actividades lícitas que se realicen; y,
- e) Las asignaciones que a título gratuito recibiere del Estado u otros organismos de derecho público o privado, sean nacionales o extranjeros, para el cumplimiento de sus fines y objetivos.

Art. 49.- ADMINISTRACIÓN DE RECURSOS: Los recursos serán manejados con el mayor celo y pulcritud por la Directiva y la Asamblea General.

Anualmente la Directiva presentará a la Asamblea General un informe de los recursos existentes; además, hará una fiscalización sobre su manejo e inversión, para el efecto, podrá contratarse de ser necesario un profesional en Contabilidad y Auditoría o carrera a fin, o en su defecto podrá solicitar la colaboración de algún miembro de la Organización conocedor de la materia.

Art. 50.- El año económico se cerrará el 31 de diciembre de cada año y los balances serán presentados dentro de los tres primeros meses del año siguiente.

Art. 51.- Los bienes son indivisibles por lo que no pertenecen ni en todo ni en parte a ninguno de los miembros, y no son susceptibles de reparto entre sus miembros, sino que pertenecen totalmente a la Organización; y serán utilizados única y exclusivamente para el cumplimiento de sus fines y objetivos contemplados en estos estatutos.

CAPITULO VI

REFORMA DE ESTATUTOS

Art. 52.- La Organización en Asamblea General procederá a realizar reformas a su estatuto de acuerdo con sus necesidades, en cualquier tiempo, en una sola reunión de Asamblea General específicamente convocada para el efecto, con el voto favorable de las/los Elija un elemento.

(registrados ante la autoridad competente y que estén al día con sus obligaciones al momento de aprobarse las reformas).

CAPITULO VII

REGIMEN DE SOLUCIÓN DE CONTROVERSIAS

Art. 53.- Los conflictos internos de la Organización serán resueltos utilizando el diálogo y la conciliación en Asamblea General, dando a cada parte el derecho de expresarse; y, en caso de

persistir, se someterán primero a la Mediación y Arbitraje, y de continuar la controversia, a la justicia ordinaria, de ser el caso.

CAPITULO VIII

CAUSALES Y PROCEDIMIENTO DE DISOLUCIÓN Y LIQUIDACIÓN

Art. 54.- CAUSALES DE DISOLUCIÓN Y LIQUIDACIÓN: La Organización podrá disolverse por las siguientes causales:

- a) Por voluntad de sus miembros expresada en Asamblea General;
- b) Por no cumplir con el ámbito de acción, fines u objetivos por el lapso de cuatro años;
- c) Por no registrar su directiva dos periodos consecutivos; y,
- d) Por disposición legal.

Art. 55.- DISOLUCION VOLUNTARIA. - Para que se resuelva la disolución de la organización por decisión de sus miembros en Asamblea General, ésta deberá tomarse con el voto de las dos terceras partes de la totalidad de socios presentes, en sesión convocada expresamente para dicho efecto.

La convocatoria se realizará por cualquier medio que justifique el conocimiento de sus miembros, prefiriendo aquella que deje constancia de su recepción.

En esta sesión los miembros nombrarán un liquidador y resolverán sobre el destino de los bienes de la Organización que no podrán ser objeto de reparto entre los asociados mismos que deberán ser donados a otra entidad sin fines de lucro; pudiendo pasar a una institución de servicio social con fines análogos. A falta de una decisión de la Asamblea General, los bienes pasarán a poder del Ministerio de Inclusión Económica y Social-MIES, a fin de que sean entregados a otra institución de beneficencia social.

La persona designada como liquidador puede ser uno de los miembros, quien asume la responsabilidad de realizar el informe (existan o no bienes) y pone a consideración de la asamblea general para su aprobación.

Los resultados de la disolución y liquidación se pondrán en conocimiento de la Cartera de Estado a cuyo control está sometida la organización, a fin de que se proceda a elaborar el Acuerdo de Disolución y Liquidación.

Art. 56.- DE LA DISOLUCIÓN CONTROVERTIDA: La Cartera de Estado a cargo del otorgamiento de personalidad jurídica de la organización, podrá de oficio declarar la disolución de la organización, cuando se hubiere incurrido en las causales legales establecidas para tal disolución (Por disminuir el número de socios del mínimo legal, por no cumplir o desviar sus fines específicos para los cuales fue creada, por atentar contra el orden público y comprometer la seguridad del Estado, etc.). En la resolución que declare disuelta a la organización, nombrará una comisión liquidadora quien se encargará de sanear las deudas de la organización y se procederá a elaborar el Acuerdo Ministerial de Disolución y Liquidación.

DISPOSICIONES GENERALES:

PRIMERA. - La Organización como tal no podrá intervenir ni desarrollar actividades o programas prohibidos por la Constitución de la República del Ecuador, la ley, el orden público, las buenas costumbres y demás instrumentos legales; tales como asuntos de carácter político, racial, sindical o religioso ni directa ni indirectamente, ni dirigir peticiones a nombre del pueblo.

SEGUNDA. - En caso de recibir subvenciones presupuestarias del Estado, se someterá a la supervisión de la Contraloría General del Estado y los procesos de control que correspondan conforme la normativa legal aplicable.

TERCERA. - La Organización se sujetará a la legislación nacional vigente, de modo particular cumplirá con las obligaciones contempladas en la Ley, y se someterá a la supervisión de los respectivos Organismos de Control del Estado.

CUARTA. - Se entienden incorporadas al presente estatuto y forman parte del mismo, las disposiciones de la Constitución de la República del Ecuador, el Código Civil y demás normativas dictadas por el Estado y el ente regulador.

DISPOSICIONES TRANSITORIAS:

PRIMERA. - El presente Estatuto entrará en vigencia desde la fecha de aprobación por parte del Ministerio de Inclusión Económica y Social-MIES.

SEGUNDA. - Una vez que sea aprobado el presente estatuto y se haya otorgado la Personalidad Jurídica, la Directiva Provisional, dentro del plazo de 15 días convocará a Asamblea General, a fin de elegir y designar a la Directiva que presidirá a la Organización para el periodo que expresa este estatuto, la misma que será enviada para su registro en el MIES de forma inmediata.

CERTIFICACIÓN: Certifico que el presente Estatuto, fue leído, discutido y aprobado por los miembros fundadores, en la ciudad de Haga clic aquí para escribir texto., el Haga clic aquí para escribir texto. de Haga clic aquí para escribir texto.

Sr. (a) Haga clic aquí para escribir texto.

SECRETARIO/A

Apéndice B *Formulario de Acceso a la Biblioteca Técnica*

FORMULARIO DE ACCESO A LA BIBLIOTECA TÉCNICA “AECIE”		V 1.0	
Información de los miembros			
<i>Nombres:</i>		<i>Apellidos:</i>	
<i>Cargo:</i>		<i>Empresa a la que Pertenece:</i>	
<i>Fecha:</i>		<i>Correo electrónico:</i>	
Seleccione el acceso que necesita			
<i>Tipo de Acceso:</i>			
ACCESO A BIBLIOTECA		OTROS	
Justificación (Detallar claramente los motivos que fundamentan su solicitud)			
Normas que se deben cumplir			
<p>a) Utilizar el acceso concedido única y exclusivamente para tareas propias de la función NO debe utilizarse para ningún otro fin.</p> <p>b) Proteger la información a la que tiene acceso de manera autorizada, a través de la habilitación de las reglas.</p> <p>c) Es responsabilidad del usuario autorizado con el acceso, el manejo y uso seguro de las contraseñas que los diferentes componentes de la plataforma tecnológica le soliciten.</p> <p>d) El usuario por ningún motivo deberá compartir sus contraseñas con otras personas.</p> <p>e) Sujetarse a todos los procesos de control y monitoreo que realice la AECIE.</p>			
Firmas			
Solicitante		Presidente	
Nombre:		Nombre:	
CI:		CI:	