ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Facultad de Ingeniería en Electricidad y Computación

"DISEÑO DE UN PLAN DE ACCIÓN PARA LA OPTIMIZACIÓN EN LA IMPLEMENTACIÓN DEL CENTRO DE RESPUESTAS A INCIDENTES INFORMÁTICOS Y DEL COMANDO DE OPERACIONES CIBERNÉTICAS EN EL ECUADOR"

INFORME DE MATERIA INTEGRADORA

Previo a la obtención del TÍTULO de:

INGENIERÍA EN ELECTRÓNICA Y TELECOMUNICACIONES

SOLANCH ANDREA CASTILLO RUEDA

SANDRA STEFANY RODRÍGUEZ VINUEZA

GUAYAQUIL – ECUADOR

AÑO: 2016

AGRADECIMIENTOS

Mis más sinceros agradecimientos a mis padres por la paciencia, el apoyo incondicional y el amor que me han brindado desde mis primeros pasos.

A todos los profesores que me han brindado su conocimiento y sus sabios consejos a lo largo de la carrera, en especial al Dr. Villao, por su paciencia y valioso tiempo invertido con el propósito de la finalización exitosa de este documento.

Solanch

Mis más sinceros agradecimientos a Dios en primer lugar por todas las bendiciones que me da y por permitirme concluir esta etapa de mi vida.

A mis padres y mis hermanos por ser mi apoyo en todo momento de mi vida y por siempre estar presentes cuando los necesito.

A mis compañeros y profesores en especial al Dr. Villao por todos los conocimientos y el apoyo que me han brindado.

Sandra Rodríguez

DEDICATORIA

El presente proyecto lo dedico a:

Mi mamá Aleyda y mi papá Kleber debido a que sin sus enseñanzas nunca hubiera podido concluir este documento.

A Isabella, mi amiga incondicional, que siempre estuvo junto a mí en los momentos difíciles recordándome que rendirse jamás es una opción.

A Joselyn, mi fiel confidente, mi buena amiga, la persona con la que más he compartido afinidades durante mi vida académica.

Solanch

El presente proyecto lo dedico a mi familia, en especial a mis padres, a mis hermanos y a mi abuelita que siempre estuvieron apoyándome en todos los momentos difíciles, y compartieron junto a mí todos los momentos alegres.

Sandra Rodríguez

TRIBUNAL DE EVALUACIÓN

Freddy Villao Quezada, PhD.	**José Menéndez Sanchez, MsC.**
PROFESOR EVALUADOR	PROFESOR EVALUADOR

DECLARACIÓN EXPRESA

"La responsabilidad y la autoría del contenido de este Trabajo de Titulación, nos corresponde exclusivamente; y damos nuestro consentimiento para que la ESPOL realice la comunicación pública de la obra por cualquier medio con el fin de promover la consulta, difusión y uso público de la producción intelectual"

Sandra Rodríguez Vinueza

Solanch Castillo Rueda

RESUMEN

En el mundo actual realizar todo tipo de transacciones desde cualquier lugar, tener nuestros dispositivos conectados en red, comunicarnos con personas en cualquier parte del mundo y muchas otras actividades que podemos realizar por medio de la red se han facilitado gracias a la tecnología; de igual manera se ha facilitado realizar delitos como fraudes, estafas, robos entre otros lo cual ha provocado que los ataques cibernéticos se incrementen descontroladamente, por tal motivo muchas personas tienen desconfianza al momento de navegar en la red, por lo que prefieren no usar todas estas facilidades y realizar sus transacciones y trámites de manera personal.

Para mitigar esta problemática proponemos un plan de acción para la optimización en los procesos de los centros de incidentes informáticos en Ecuador, el cual se ha diseñado analizando propuestas de planes de acción de los países con mejores prácticas aplicadas en seguridad cibernética.

El plan de acción propuesto se compone de 5 etapas las cuales son Difusión, Detección del Incidente, Análisis del Incidente, Definir Estrategias de Mitigación y Solución del Incidente; aplicando este plan de acción en los centros de respuestas a incidentes informáticos se espera mitigar los incidentes de diferentes maneras como enseñando a la ciudadanía a protegerse de ellos, detectar el incidente antes de que sea grave o de que ocurra, solucionar los incidentes de maneras más eficientes al tener una base de datos de incidentes pasados, controlar que los ISP cumplan todas las obligaciones que tienen con los usuarios.

Algunos de los resultados que se espera obtener con la implementación del plan de acción son incrementar el comercio electrónico, mejorar la confianza de los usuarios al momento de navegar en la red, cumplir con las líneas de acción de la UIT

ÍNDICE GENERAL

CAPÍTULO 1

1. INCIDENTES INFORMÁTICOS EN EL ECUADOR

1.1 Entorno Global

1.1.1 Rol de los Organismos Internacionales frente a la seguridad cibernética

El 23 de noviembre de 2001, el Consejo de Europa firmó El Convenio sobre la Ciberdelincuencia [1], éste es el único acuerdo que trata sobre la Seguridad de la Información y cubre todas las áreas relevantes de la legislación sobre Ciberdelincuencia, tales como Derecho Penal, Derecho Procesal, Jurisdicción y Cooperación Internacional; este Convenio entró en vigor el 1 de julio de 2004; también llamado Convenio de Budapest, está abierto a la entrada de países no europeos; en el 2006 Estados Unidos resolvió unirse al Convenio, mientras que a nivel latinoamericano, República Dominicana y Panamá han ratificado su adhesión al Convenio.

La Resolución 56/121 titulada “Lucha contra la utilización de la tecnología de la información con fines delictivos” [2], aprobada por la Asamblea General de las Naciones Unidas el 23 de enero de 2002 expresa su preocupación por el hecho de que los avances tecnológicos han abierto nuevas oportunidades de actividades delictivas, particular y específicamente en la utilización de la tecnología de la información para fines delictivos y observando que la dependencia de las tecnologías, aunque pueda variar de un Estado a otro, es cada vez mayor, y ha dado lugar a un aumento en la cooperación y coordinación a nivel mundial, debido a esto la utilización de esta tecnología con fines delictivos puede tener un impacto a nivel global; se resuelve invitar a todos los Estados Miembros a elaborar leyes y políticas nacionales y a adoptar prácticas para luchar contra la utilización de la tecnología de la información con fines delictivos.

La Resolución 57/239 titulada “Creación de una Cultura Mundial de Seguridad Cibernética” [3], aprobada por la Asamblea General de las Naciones Unidas el 31 de enero de 2003, reconoce que la necesidad de seguridad cibernética aumenta a medida que los países incrementan su participación en la sociedad de la información; esta resolución tiene en cuenta que el éxito en la implementación en la seguridad cibernética no es solo cuestión de prácticas de Gobierno o de orden público, sino que debe alcanzarse por medio de la prevención y con el apoyo de toda la sociedad. En este documento se establecen los nueve elementos que todos los países participantes deben tomar en cuenta para la creación de una cultura mundial de seguridad cibernética: conciencia, responsabilidad, respuesta, ética, democracia, evaluación de riesgos, diseño y puesta en práctica de la seguridad, gestión de la seguridad y por último reevaluación [4].

En diciembre de 2003 se expidió la ley titulada “The Spam Act 2003” [5] en Australia, que prohíbe el envío no solicitado de mensajes electrónicos con fines comerciales (conocidos como spam) con un link australiano; un mensaje posee un link australiano si fue originado en Australia, o si fue originado en el extranjero, pero su destino es una dirección australiana. Se establece que los únicos mensajes que se pueden enviar sin autorización son los de Organismos gubernamentales, los partidos políticos registrados, las organizaciones benéficas registradas y las instituciones educativas para los mensajes enviados hacia sus estudiantes actuales o anteriores.

En diciembre de 2003 el Congreso de Estados Unidos adopta la Ley de Control de Pornografía y Mercadeo No Solicitado (CAN-Spam, por sus siglas en inglés), el gobierno aprobó esta ley como medida de control para el rápido aumento de los mensajes electrónicos no deseados; esta ley exige que la Comisión Federal de Comunicaciones (FCC, por sus siglas en inglés) establezca normas regulatorias que controlen el envío de mensajes electrónicos no

deseados con fines comerciales, y los mensajes enviados de manera inalámbrica a teléfonos celulares [6].

Debido a la necesidad de aprovechar el abanico de posibilidades al poder acceder al conocimiento y a la tecnología para promover el alcance de los objetivos fijados en la Declaración del Milenio [7], en la cual se decide velar por que todos aprovechen los beneficios de las nuevas tecnologías, en particular de las tecnologías de la información y de la comunicación, la resolución 56/183 [8] aprobada por la Asamblea General de las Naciones Unidas decide crear la Cumbre Mundial sobre la Sociedad de la Información.

Esta cumbre se desarrolló en dos fases, la primera fase tuvo lugar en Ginebra acogida por el gobierno de Suiza del 10 al 12 de diciembre de 2003.

El objetivo de la primera fase era redactar y propiciar una clara declaración de voluntad política, y tomar medidas concretas para preparar los fundamentos de la Sociedad de la Información para todos, que tenga en cuenta los distintos intereses en juego [9].

En esta primera fase, se reconoce que la confianza y la seguridad es uno de los pilares más importantes de la Sociedad de la Información, además se admite que Internet se ha convertido en un recurso mundial disponible para el público. Se establecen los principios claves para la construcción de una Sociedad de la Información Integradora en la Declaración de Principios de Ginebra [10], en la cual el apartado B5 enuncia los puntos a continuación:

B5) *Fomento en la Confianza y Seguridad en la Utilización de las TIC*

35. El fomento de un clima de confianza, incluso en la seguridad de la información y la seguridad de las redes, la autenticación, la privacidad y la protección de los consumidores, es requisito previo para que se desarrolle la Sociedad de la Información y para promover la confianza

entre los usuarios de las TIC. Se debe fomentar, desarrollar y poner en práctica una cultura global de ciberseguridad, en cooperación con todas las partes interesadas y los organismos internacionales especializados. Se deberían respaldar dichos esfuerzos con una mayor cooperación internacional. Dentro de esta cultura global de ciberseguridad, es importante mejorar la seguridad y garantizar la protección de los datos y la privacidad, al mismo tiempo que se amplía el acceso y el comercio. Por otra parte, es necesario tener en cuenta el nivel de desarrollo social y económico de cada país, y respetar los aspectos de la Sociedad de la Información orientados al desarrollo.

36. Si bien se reconocen los principios de acceso universal y sin discriminación a las TIC para todas las naciones, apoyamos las actividades de las Naciones Unidas encaminadas a impedir que se utilicen estas tecnologías con fines incompatibles con el mantenimiento de la estabilidad y seguridad internacionales, y que podrían menoscabar la integridad de las infraestructuras nacionales, en detrimento de su seguridad. Es necesario evitar que las tecnologías y los recursos de la información se utilicen para fines criminales o terroristas, respetando siempre los derechos humanos.

37. El envío masivo de mensajes electrónicos no solicitados ("spam") es un problema considerable y creciente para los usuarios, las redes e Internet en general. Conviene abordar los problemas de la ciberseguridad y "spam" en los planos nacional e internacional, según proceda.

Además, se resuelve crear un Plan de acción [4] en el cual se establecieron líneas de acción denominadas con la letra C, la cual se enfoca en la seguridad de las TIC

(C5) “*Creación de confianza y seguridad en la utilización de las TIC*”

La confianza y la seguridad son unos de los pilares más importantes de la Sociedad de la Información.

a. Propiciar la cooperación entre los gobiernos dentro de las Naciones Unidas, y con todas las partes interesadas en otros foros apropiados, para aumentar la confianza del usuario y proteger los datos y la integridad de la red; considerar los riesgos actuales y potenciales para las TIC, y abordar otras cuestiones de seguridad de la información y de las redes.
b. Los gobiernos, en cooperación con el sector privado, deben prevenir, detectar, y responder a la ciberdelincuencia y el uso indebido de las TIC, definiendo directrices que tengan en cuenta los esfuerzos existentes en estos ámbitos; estudiando una legislación que permita investigar y juzgar efectivamente la utilización indebida; promoviendo esfuerzos efectivos de asistencia mutua; reforzando el apoyo institucional a nivel internacional para la prevención, detección y recuperación de estos incidentes; y alentando la educación y la sensibilización.
c. Los gobiernos y otras partes interesadas deben fomentar activamente la educación y la sensibilización de los usuarios sobre la privacidad en línea y los medios de protección de la privacidad.
d. Tomar medidas apropiadas contra el envío masivo de mensajes electrónicos no solicitados ("spam") a nivel nacional e internacional.
e. Alentar una evaluación interna de la legislación nacional con miras a superar cualquier obstáculo al uso efectivo de documentos y transacciones electrónicas, incluido los medios electrónicos de autenticación.

f. Seguir fortaleciendo el marco de confianza y seguridad con iniciativas complementarias y de apoyo mutuo en los ámbitos de la seguridad en el uso de las TIC, con iniciativas o directrices sobre el derecho a la privacidad y la protección de los datos y de los consumidores.
g. Compartir prácticas óptimas en el ámbito de la seguridad de la información y la seguridad de las redes, y propiciar su utilización por todas las partes interesadas.
h. Invitar a los países interesados a establecer puntos de contacto para intervenir y resolver incidentes en tiempo real, y desarrollar una red cooperativa entre estos puntos de contacto de forma que se comparta información y tecnologías para intervenir en caso de estos incidentes.
i. Alentar el desarrollo de nuevas aplicaciones seguras y fiables que faciliten las transacciones en línea.
j. Alentar a los países interesados a que contribuyan activamente en las actividades en curso de las Naciones Unidas tendentes a crear confianza y seguridad en la utilización de las TIC.

La Resolución 58/199 titulada “Creación de una cultura mundial de seguridad cibernética y protección de las infraestructuras de información esenciales” [11], aprobada por la Asamblea General de la Organización de los Estados Americanos del 30 de enero de 2004 reconoce que los Estados, las empresas, las organizaciones y los usuarios particulares cada vez le brindan mayor importancia a las tecnologías de información para la promoción del desarrollo socioeconómico y el intercambio de información; y observando que cada vez hay más vínculos entre las infraestructuras esenciales de la mayoría de los países como las utilizadas para la generación, transmisión y distribución de energía, el transporte aéreo y marítimo, los servicios bancarios y financieros, el comercio electrónico, el suministro de agua, la distribución de alimentos y la salud pública y

las infraestructuras de tecnologías de información esenciales que interconectan y afectan cada vez más sus operaciones; se resuelve anexar:

Los elementos para la protección de las infraestructuras de información esenciales

1. Contar con redes de alerta de emergencia en relación con las vulnerabilidades, las amenazas y los incidentes cibernéticos.
2. Crear más conciencia para que los interesados entiendan la naturaleza y el alcance de sus infraestructuras de información esenciales y la función que debe desempeñar cada uno en su protección.
3. Examinar las infraestructuras y determinar las interdependencias de éstas, mejorando así su protección.
4. Promover alianzas entre las partes interesadas, tanto públicas como privadas, para compartir y analizar las infraestructuras de información esenciales a fin de prevenir e investigar los daños y los ataques contra dichas infraestructuras, y responder a ellos.
5. Crear y mantener redes de comunicación para casos de crisis y probarlas para asegurarse de que seguirán siendo estables y seguras en situaciones de emergencia.
6. Garantizar que en las políticas sobre disponibilidad de datos se tenga en cuenta la necesidad de proteger las infraestructuras de información esenciales.
7. Facilitar el rastreo de los ataques contra las infraestructuras de información esenciales y, cuando corresponda, revelar la información recabada a otros Estados.
8. Ofrecer capacitación y hacer prácticas para mejorar las capacidades de respuesta y probar planes de continuidad y contingencia en el caso de un ataque contra las infraestructuras

de información, y alentar a las partes interesadas a emprender actividades similares.

9. Contar con leyes sustantivas y de procedimientos adecuados y personal capacitado para que los Estados puedan investigar los ataques contra las infraestructuras de información esenciales y enjuiciar a los responsables, y coordinar dichas investigaciones con otros Estados, cuando corresponda.

10. Cooperar a nivel internacional, cuando corresponda, para proteger las infraestructuras de información esenciales, en particular desarrollando y coordinando sistemas de alerta de emergencia, compartiendo y analizando información sobre vulnerabilidades, amenazas e incidentes y coordinando las investigaciones sobre los ataques contra dichas infraestructuras de conformidad con las leyes nacionales.

11. Promover la investigación y el desarrollo a nivel nacional e internacional y alentar la aplicación de tecnologías de seguridad que cumplan las normas internacionales.

Del 16 al 18 de noviembre del 2005 se inició la segunda fase de la Cumbre Mundial de la Sociedad de la Información realizada en Túnez, el objetivo de la segunda fase fue poner en marcha el Plan de Acción de Ginebra, hallar soluciones y alcanzar acuerdos en los campos de gobierno de Internet, mecanismos de financiación, el seguimiento y la aplicación de los documentos de Ginebra y Túnez [9]. Se destaca la importancia de enjuiciar la ciberdelincuencia, incluida la que se produce en una jurisdicción pero repercute en otra. Se definió el trabajo de la Gobernanza de Internet como *desarrollo y aplicación por los gobiernos, el sector privado y la sociedad civil, en el desempeño de sus respectivos papeles, de principios, normas, reglas, procedimiento de toma de decisiones y programas comunes que dan forma a la evolución y a la utilización de Internet* [4]. Adicionalmente se aprobó el Compromiso de Túnez [12], en el cual

se enfoca a la seguridad de las TIC’s en los puntos 9 y 15, detallados a continuación:

9. Reafirmamos la decisión de proseguir nuestra búsqueda para garantizar que todos se beneficien de las oportunidades que puedan brindar las TIC, recordando que los gobiernos y también el sector privado, la sociedad civil, las Naciones Unidas y otras organizaciones internacionales deben colaborar para acrecentar el acceso a la infraestructura y las tecnologías de la información y la comunicación, así como a la información y al conocimiento, crear capacidades, incrementar la confianza y la seguridad en cuanto a la utilización de las TIC, crear un entorno habilitador a todos los niveles, desarrollar y ampliar las aplicaciones TIC, promover y respetar la diversidad cultural, reconocer el cometido de los medios de comunicación, abordar las dimensiones éticas de la Sociedad de la Información y alentar la cooperación internacional y regional. Confirmamos que éstos son los principios claves de la construcción de una Sociedad de la Información integradora, cuya elaboración ha sido enunciada en la Declaración de Principios de Ginebra.

15. Reconociendo los principios de acceso universal y sin discriminación a las TIC para todas las naciones, la necesidad de tener en cuenta el nivel de desarrollo social y económico de cada país, y respetando la orientación hacia el desarrollo de la Sociedad de la Información, subrayamos que las TIC son un instrumento eficaz para promover la paz, la seguridad y la estabilidad, así como para propiciar la democracia, la cohesión social, la buena gobernanza y el estado de derecho, en los planos regional, nacional e internacional. Se pueden utilizar las TIC para promover el crecimiento económico y el desarrollo de las empresas. El desarrollo de infraestructuras, la creación de capacidades humanas, la seguridad de la información y la seguridad de la red son decisivos para alcanzar esos objetivos.

Además, reconocemos la necesidad de afrontar eficazmente las dificultades y amenazas que representa la utilización de las TIC para fines que no corresponden a los objetivos de mantener la estabilidad y seguridad internacionales y podrían afectar negativamente a la integridad de la infraestructura dentro de los Estados, en detrimento de su seguridad. Es necesario evitar que se abuse de las tecnologías y de los recursos de la información para fines delictivos y terroristas, respetando siempre los derechos humanos.

1.1.2 Gobernanza de Internet

El debate por la Gobernanza se inició porque Internet es de todos, pero no le pertenece a nadie, además trasciende las fronteras de interés y soberanía de una sola institución o Estado [13].

En la primera fase de la Cumbre Mundial Sobre la Sociedad de la Información (CMSI) celebrada en Ginebra en el año 2003, se publicó la Declaración de Principios titulada “Construir la Sociedad de la Información: un desafío global para el nuevo milenio” en la cual se reconoce a Internet como un recurso accesible a nivel mundial y su gestión debe de ser un tema esencial en el desarrollo de la Sociedad de la Información siendo transparente, democrática y multilateral, además de poder contar con la plena participación de los gobiernos, el sector privado, la sociedad civil, y las organizaciones internacionales para poder coordinar y aunar esfuerzos y lograr garantizar la distribución equitativa de recursos, facilitar el acceso universal y garantizar el funcionamiento estable y seguro de internet, teniendo en cuenta el plurilingüismo.

Con este propósito los gobiernos solicitaron al Secretario General de las Naciones Unidas se establezca un grupo de trabajo sobre el gobierno de internet que garantice la participación e integración de los gobiernos y organismos internacionales relevantes además de

sociedad civil para que se investiguen y formulen propuestas de planes de acción antes del 2005, para la segunda fase de la Cumbre a realizarse en Túnez.

Durante la segunda fase de la Cumbre realizada en Túnez en el 2005 se adoptó la Agenda de Túnez para la Sociedad de la Información, donde se menciona por primera ocasión el término Gobernanza de Internet, en esta Agenda se reconoce que la Gobernanza de Internet supone más que la asignación de nombres y direcciones. Incluye otros aspectos importantes de política pública tales como, entre otros, los recursos críticos de Internet, la seguridad y protección de Internet los aspectos y cuestiones de desarrollo relativos a la utilización de Internet; temas sociales, económicos y técnicos, incluida la asequibilidad, la fiabilidad y la calidad de servicio. [14]

Se solicitó al secretario General de las Naciones Unidas que convoque a un nuevo foro para el segundo trimestre del 2006 con el fin de realizar diálogos sobre políticas de las múltiples partes interesadas (Foro de Gobernanza de Internet (FGI)). Se acordó que la primera reunión se lleve a cabo en Atenas en el 2006, propuesto como sede por el Gobierno de Grecia.

Hasta ahora se han realizado los siguientes foros:

- FGI Atenas, Grecia 2006
- FGI Río de Janeiro, Brasil 2007
- FGI Hyderabad, India 2008
- FGI Sharm El Sheikh, Egipto 2009
- FGI Vilnius, Lituania 2010
- FGI Nairobi, Kenia 2011
- FGI Baku, Azerbaiyán 2012
- FGI Bali, Indonesia 2013
- FGI Estambul, Turquía 2014
- FGI Madrid, España 2015

En estos foros se ha discutido entre otras cosas asuntos relacionados con el acceso universal, ciberseguridad, plurilingüismo, recursos críticos en Internet, impacto de las redes sociales, economía de internet.

El próximo foro se realizará en México en el año 2016.

1.1.3 Agenda sobre ciberseguridad global: Un marco para la cooperación internacional en materia de ciberseguridad

En 17 de mayo de 2007 el Dr. Hamadoun I. Touré, Secretario General de la UIT (Unión Internacional de las Telecomunicaciones) lanza la Agenda sobre Ciberseguridad Global (GCA por sus siglas en inglés Global Cybersecurity Agenda) [15], que es un marco de cooperación internacional destinado a mejorar la seguridad y a incrementar la confianza en la sociedad de la información. La GCA ha sido muy apoyada y reconocida en todo el mundo por dirigentes y expertos en Ciberseguridad.

Con el fin de ayudar al Secretario General de la UIT a elaborar propuestas estratégicas de promoción de la ciberseguridad destinadas a los Estados Miembros de la UIT se estableció el Grupo de Expertos de Alto Nivel sobre Ciberseguridad (GEANC) [15], el 5 de octubre de 2007. La GEANC es presidido por el Juez Stein Schjolberg (Noruega).

La GEANC ha elaborado recomendaciones que ayudarán a coordinar en todo el mundo la lucha contra la constante evolución de la ciberdelincuencia y las amenazas a las redes.

La Agenda sobre Ciberseguridad Global está basada en cinco pilares fundamentales que son:

1. Medidas Legales
2. Medidas Técnicas y de Procedimientos
3. Estructuras Organizacionales

4. Creación de Capacidades
5. Cooperación Internacional

En la figura 1.1 se puede observar los 5 pilares fundamentales en los cuales está basada la Agenda sobre Ciberseguridad Global con una pequeña descripción de cada uno.

Fuente: Elaborado por la UIT [16]

Figura 1.1: Aspectos de la cooperación internacional de La Agenda sobre Ciberseguridad Global de la UIT

Medidas Legales

El objetivo es crear estrategias para elaborar una legislación modelo sobre ciberdelincuencia, que se pueda aplicar en todo el mundo y se adapte a las legislaciones existentes en cada país. El GEANC reconoció que la Convención sobre la Ciberdelincuencia se puede utilizar como referencia válida o

como directrices, también debe tomarse en cuenta otras legislaciones sobre amenazas, como los correos indeseados (spam), el robo de identidad, y los ataques masivos y coordinados contra la explotación de infraestructuras esenciales de la información, los cuales también pueden ser considerados como ciberterrorismo, y para estos ataques la GEANC reconoció la Convención de 2005 del Consejo de Europa acerca de la Prevención del Terrorismo.

Medidas Técnicas y de Procedimientos

- *Promoción de la Ciberseguridad*

  Se pidió a la UIT que continuará los trabajos con los equipos especiales que están encargados de la ciberseguridad nacional y fomentará que sean parte de conferencias y foros mixtos mundiales y regionales. Además la UIT debe establecer un “compromiso a largo plazo” para crear y perfeccionar métodos de promoción de prácticas idóneas y técnicas de divulgación de ciberseguridad y la infraestructura de información esencial.

- *Normalización*

  La UIT en cooperación con otros organismos de normalización podría estudiar normas existentes de seguridad de las TIC (Tecnologías de la Información y de la comunicación) y posibilidades de mejorar sus propuestas de procedimientos de ciberseguridad.

- *Evaluación de la ciberseguridad*

  La UIT en cooperación con otros organismos competentes debería escoger un marco de “criterios comunes para la evaluación de la seguridad de las TIC” mundialmente aceptados, el cual se utilizará para evaluar y certificar elementos como sistemas operativos, soporte técnico,

navegadores internet, programas de correo electrónico entre otros.

- *Internet y tecnologías emergentes*
  El GEANC realizó recomendaciones sobre internet, gestión de identidad digital, y tecnologías emergentes. También se solicitó a la UIT que “iniciara un examen de la posibilidad de ofrecer capacidades fiables y compatibles de gestión global de identidad que comprendan servicios de resolución de identificador seguros.”

Estructuras Organizacionales

Están encargadas de optimizar las actividades de varios organismos, para ahorrar recursos y evitar que el mismo trabajo se duplique innecesariamente.

La GEANC resaltó que cada país debe generar sus propias estructuras organizacionales, para que estas puedan adaptarse a sus necesidades de ciberseguridad y dar asistencia a través de la cooperación regional o internacional; se recomienda que este sea flexible para que los demás países puedan adaptar a sus circunstancias. Los centros regionales de vigilancia, aviso y respuesta a incidentes deberían ofrecer servicio a varios países.

Creación de Capacidades

La GEANC recalcó que para la creación de capacidades en la ciberseguridad se necesita de recursos financieros, técnicos, humanos específicos y una cooperación internacional. Además añadió que la UIT cuenta con todos estos recursos y que debería enfocarse en los países en desarrollo y menos adelantados.

En el 2007 y 2008, la UIT estructuró 8 foros regionales acerca de ciberseguridad con el fin de brindar información y que el intercambio de prácticas idóneas sea más sencillo.

Cooperación Internacional

El coordinador de la UIT podría ser el que garantice la continuidad de la gestión de diversas de estas actividades cuando el trabajo de la GEANC concluya, y de esta manera mejorar la colaboración de los centros regionales e internacionales.

Los mecanismos de la UIT acerca de recolección de información de proyectos de ciberseguridad deberían mejorar para que de esta manera ellos pudieran divulgar esta información a todo el mundo y que cada país se pueda preparar de una mejor manera ante estos ataques.

“La UIT, con el mandato que le han encomendado los Estados Miembros y su posición en el sistema de las Naciones Unidas, está en una situación ideal para ser el abogado (de la ciberseguridad)” del nivel internacional al comunitario, declaró el GEANC.

Basada en estos pilares fundamentales la Agenda sobre Ciberseguridad Global quiere alcanzar las siguientes metas estratégicas:

a. Preparar estrategias que promuevan el desarrollo de una legislación modelo sobre ciberdelito, que resulte aplicable a escala mundial y sea compatible con las medidas legislativas ya adoptadas en los diferentes países y regiones.
b. Definir estrategias mundiales para crear las adecuadas estructuras institucionales nacionales y regionales, así como definir las correspondientes políticas para luchar contra el ciberdelito.

c. Diseñar una estrategia que permita establecer un conjunto mínimo y mundialmente aceptado de criterios de seguridad y planes de acreditación para equipos, aplicaciones y sistemas informáticos.
d. Definir estrategias para crear un marco mundial con miras a vigilar, alertar y responder ante incidentes y garantizar así la coordinación transfronteriza en lo que concierne a las iniciativas nuevas y existentes.
e. Diseñar estrategias mundiales tendentes a crear y apoyar un sistema de identidad digital genérico y universal y las correspondientes estructuras institucionales para garantizar el reconocimiento internacional de credenciales digitales.
f. Concebir una estrategia global para facilitar la creación de capacidad humana institucional con el fin de promover los conocimientos técnicos y prácticos en todos los sectores y las esferas antes mencionadas.
g. Formular propuestas para establecer un marco conducente a una estrategia mundial multipartita que fomente la cooperación, el diálogo y la coordinación internacionales en todas las esferas precitadas.

Iniciativa IMPACT

Una de las iniciativas generadas por la GCA es la “Alianza Internacional Multilateral contra las Ciberamenazas” (IMPACT), con la cual la UIT firmó un Memorándum de Entendimiento (MoU) durante ITU Telecom Asia 2008 en septiembre de 2008. Otra de las iniciativas generadas por la GCA es la “Protección de los Niños en Línea” (COP).

IMPACT fue instituida en mayo de 2008 por el Gobierno de Malasia con su sede cerca de Kuala Lumpur. IMPACT es una alianza de gobiernos, dirigentes de la industria y expertos en ciberseguridad, que colaboran en la mejora de la capacidad de la

comunidad mundial para evitar los ataques, defenderse de ellos y ofrecer la respuesta adecuada. La colaboración entre la UIT e IMPACT ofrece a los 191 Estados Miembros de la UIT los recursos y conocimientos técnicos especializados para fomentar la ciberseguridad en sus propios países y fuera de ellos. [17]

IMPACT se ha convertido en el hogar de la GCA; y facilita los siguientes recursos a los Estados Miembros de la UIT:

- *Centro de respuesta global*

  Este centro ofrece a la comunidad mundial un "Sistema de alerta temprana de red" (NEWS, Network Early-Warning System) disponible en tiempo real para identificar las amenazas y orientar en las medidas que se deben tomar ante estas. De igual manera da acceso a instrumentos y sistemas especializados como la "Plataforma de aplicación colaborativa electrónicamente segura para expertos" (ESCAPE, Electronically Secure Collaborative Application Platform for Experts) a los Estados Miembros de la UIT.

- *Capacitación y desarrollo de capacidades*

  IMPACT junto con grandes empresas e instituciones de las TIC brindará reuniones de información a los representantes de los Estados Miembros de la UIT sobre información de alto nivel, de esta manera informar a los gobiernos sobre las amenazas contra la Ciberseguridad.

- *Centro de garantías e investigación en seguridad*

  Junto con grandes expertos de las TIC se elaborará directrices globales sobre prácticas idóneas y un sistema internacional de referencia y certificación para la Ciberseguridad. En asociación con Symantec Corporation (EE.UU.), establecerá un "Centro de Excelencia para la puntuación de la seguridad pública". Su objetivo es que el sector académico realice investigaciones de nuevas

tecnologías, y de tecnologías especializadas con un pequeño número de usuarios que pueden ser vulnerables a ciberataques.

- *Centro de políticas y cooperación internacional*
  Dirigido por la UIT y junto con organismos de las Naciones Unidas, Interpol y la Organización de Cooperación y Desarrollo Económicos (OCDE), se contribuye a la formulación de nuevas políticas y a la armonización de legislaciones nacionales sobre Ciberseguridad, incluida la delincuencia en línea. También ofrecerá a los Estados Miembros de la UIT asesoramiento sobre política y reglamentación y fomentará la cooperación internacional por medio de programas específicos como ejercicios de emergencia coordinados para responder a los ciberataques.

Iniciativa Protección de los niños en línea

La UIT creó la COP “Protección de los niños en línea” en el marco de la GCA, a fin de proteger y promover la Ciberseguridad a los niños que usan internet. Sus objetivos consisten en identificar los riesgos para los niños en el ciberespacio, concienciar sobre esos riesgos por diversos medios y elaborar instrumentos para ayudar a los sectores público, privado y docente a minimizar los riesgos.

Del 17 al 18 de junio del 2008 tuvo lugar la reunión del foro de la Organización para la Cooperación y Desarrollo Económico (OCDE) llamado El Futuro de la Economía de Internet, durante la reunión ministerial se llevó a cabo una mesa redonda llamada Building Confidence en donde se trataron algunos aspectos sobre ciberdelincuencia y robo de identidad en los países miembros del OCDE, actualmente hay 34 países miembros, el resultado de esta reunión fue La Declaración de Seúl para el Futuro de la Economía de Internet, [18] en esta declaración para contribuir al desarrollo de

internet se realizó el apartado c referente al ámbito de seguridad y cibercrimen:

c) *Fortalecer la confianza y seguridad, a través de políticas que:*

- Protejan las infraestructuras de información crítica contra los riesgos de la seguridad a nivel nacional e internacional.
- Reduzcan la actividad maliciosa en línea, a través del reforzamiento de la cooperación nacional e internacional entre todas las comunidades de los partícipes en su camino hacia una efectiva prevención, protección, intercambio de información y respuesta.
- Promuevan la investigación para responder a las amenazas de seguridad emergentes.
- Incrementen la cooperación transfronteriza entre los gobiernos y las autoridades ejecutoras de la legislación en las áreas de mejora a la ciberseguridad, en el combate al spam, así como la protección de la privacidad, consumidores y menores de edad.

En enero del 2013 nace el primer Centro Europeo del Cibercrimen (EC3), [19] localizado en La Haya, Holanda. Fue creado para fortalecer la respuesta de los Estados en la Unión Europea (UE) ante los ciberdelitos, y para ayudar a proteger a los ciudadanos europeos, empresas y gobiernos; su establecimiento era una prioridad en la Estrategia de Seguridad Interna de la UE. Está dirigido por la Oficina Europea de Policía (EUROPOL). Se enfoca en las siguientes tres áreas:

- Cibercrímenes cometidos por grupos organizados que operan para generar beneficios a gran escala.
- Cibercrímenes que causan serios daños a sus víctimas, como explotación sexual y pornografía infantil.

- Cibercrímenes (incluidos ciberataques) que afecten críticamente la infraestructura y los sistemas de información de la Unión Europea

Según estudios realizados por la UIT en el año 2013, el 60% de niños y adolescentes se conectan a salas de charla diariamente y es aquí donde los pedófilos los acosan sexualmente, o simplemente se ponen en contacto con ellos para sacarles información privada que puede ser utilizada comercialmente. De igual manera estos niños son víctimas de dos tipos de ataques el cyberbullying y el grooming, los cuales se detallan más adelante.

1.2 Entorno en América

1.2.1 Rol de los Organismos Regionales frente a la seguridad cibernética

La Estrategia Interamericana Integral para Combatir las Amenazas a la seguridad cibernética aprobada en la resolución AG/RES. 2004 (XXXIV-O/04) en la Asamblea General de la OEA (Organización de los Estados Americanos) funcionó a manera de mandato a la Secretaría del CICTE (Comité Interamericano contra el Terrorismo) para trabajar en asuntos de seguridad cibernética. [20] Uno de los principales objetivos de la Secretaría era el establecimiento de Equipos de Respuesta ante Emergencias Informáticas (CSIRT, por sus siglas en inglés), [21] éstos deberían de formarse en cada país para alerta, vigilancia y prevención, el plan del CICTE para el Programa de Seguridad Cibernética gira en la Implementación de siete puntos:

- Participación de la sociedad y del sector privado
- Crear conciencia
- Desarrollo de estrategias nacionales
- Brindar capacitación

- Ejercicios de gestión de crisis
- Misiones de asistencia técnica
- Compartir información y experiencia

En el 2015 el CICTE adoptó la Declaración sobre la Protección de Infraestructura Crítica ante las Amenazas Emergentes. [22]

Uno de los socios del proyecto de seguridad cibernética del CICTE es la Comisión Interamericana de Telecomunicaciones (CITEL), la cual también se encarga de la ciberseguridad en la región con su Comité Consultivo Permanente I: Telecomunicaciones/TIC (CCP I), la cual posee en su estructura un Grupo de Trabajo Despliegue de Tecnologías y Servicios que controla la Relatoría sobre Ciberseguridad, Evaluación de la Vulnerabilidad e Infraestructura Crítica, como parte de su labor se encarga de compartir las mejores prácticas, así como los conocimientos técnicos con la ayuda de becas para cursos de capacitación en los diferentes países de la región a técnicos de seguridad que trabajan en la infraestructura crítica de cada país.

En el ámbito regional, los gobiernos han desarrollado los Planes de Acción de la Sociedad de la Información en América Latina y el Caribe [23].

De acuerdo con los Objetivos de Desarrollo del Milenio (ODM) y la Cumbre Mundial sobre la Sociedad de la Información (CMSI), con visión de largo plazo se crea el eLAC [24].

El eLAC es un plan de acción para América Latina y el Caribe, que plantea que las tecnologías de la información y de las comunicaciones (TIC) son instrumentos de desarrollo económico y de inclusión social; este plan al ser de largo plazo posee distintas etapas; la primera etapa denominada eLAC2007 fue aprobado oficialmente en la Conferencia Preparatoria Regional Ministerial de América Latina y el Caribe para la Cumbre Mundial sobre la Sociedad de la Información, el 10 de junio de 2005 en Río de

Janeiro, Brasil. Este plan de acción duró dos años a partir de su creación (2005-2007), en el cual consideran a la seguridad en 5 puntos incluidos en las líneas de acción a continuación [25]:

A. *Acceso e inclusión Digital*

Meta 1: Infraestructura Regional

Medida 1.2: Realizar estudios regionales que orienten el desarrollo de esta infraestructura y tomen en cuenta la necesidad de incrementar la seguridad y confianza, y los factores de costo y beneficio de las TIC en el marco de los acuerdos internacionales, regionales y subregionales ya existentes.

Plazo: Mediados del 2006

B. *Creación de Capacidades y Conocimientos*

- *Meta 8:* Software

  Medida 8.1: En el contexto de eficiencia e inclusión social, establecer un grupo de trabajo regional para el intercambio de experiencias y criterios utilizados para el desarrollo y uso del software de código de fuente abierta y software libre, lo que incluye la realización de estudios sobre los desafíos técnicos, económicos, organizacionales, de capacitación y de seguridad.

  Plazo: Fines del 2006

- *Meta 14:* Gobernanza de Internet

  Teniendo presentes los “principios de Ginebra” adoptados en la primera fase de la Cumbre Mundial, particularmente los de multilateralidad, transparencia y democracia en la gobernanza de Internet e iniciativas ya en marcha:

  Medida 14.1: Promover diálogos, intercambios y cooperación regional sobre experiencias nacionales en gobernanza de Internet; capacitación en administración de recursos de

Internet (nombres de dominio, números IP (Internet Protocol) y protocolos); costos de interconexión internacional, ciberseguridad, spam y aspectos institucionales y tecnológicos relacionados.

Plazo: Mediados del 2007

C. *Transparencia y Eficiencia Públicas*

Meta 15: Gobierno Electrónico

Medida 15.5: Promover la adopción de modelos de seguridad y preservación de la información en todas las instancias del gobierno con el objetivo de generar confianza en la información digital administrada o brindada por el Estado.

Plazo: Mediados del 2007

D. *Instrumentos de política*

Meta 25: Marco Legislativo

Medida 25: Establecer grupos de trabajo subregionales para promover y fomentar políticas de armonización de normas y estándares, con el fin de crear marcos legislativos que brinden confianza y seguridad, tanto a nivel nacional como a nivel regional, prestando especial atención a la legislación sobre la protección de la privacidad y datos personales, delitos informáticos y delitos por medio de las TIC, spam, firma electrónica o digital y contratos electrónicos, como marco para el desarrollo de la sociedad de la información.

Plazo: Noviembre de 2005

El SEGUNDO PLAN DE ACCIÓN se denomina eLAC 2010. Sus metas para promover el uso de las tecnologías de la información y de las comunicaciones (TIC) fueron acordadas por autoridades regionales durante la II Conferencia Ministerial sobre la Sociedad de la Información en América Latina y el Caribe, realizada en El

Salvador, del 6 al 8 de febrero de 2008 [24]. Esta etapa también tiene un periodo de acción de dos años desde su fecha de aprobación (2008-2010). Respecto al tema de seguridad cibernética, este plan de acción en el punto 81 [26] invita a los países a estudiar la posibilidad de ratificar o adherirse al Tratado de Ciberdelitos del Consejo de Europa y su Protocolo adicional, como un instrumento facilitador de nuestra integración y adecuación normativa en esta materia, enmarcados en principios de protección de los derechos de privacidad.

El TERCER PLAN DE ACCIÓN sobre la Sociedad de la Información para América Latina y el Caribe (eLAC 2015) [27], fue aprobado en la Tercera Conferencia Ministerial sobre la Sociedad de la Información de América Latina y el Caribe que tuvo lugar del 21 al 23 de noviembre del 2010 en la ciudad de Lima, Perú. En este plan de acción las prioridades y lineamientos enfocados en la seguridad informática y de las TIC's son los siguientes:

B. GOBIERNO ELECTRÓNICO

Prioridad: Alcanzar un gobierno electrónico transaccional y participativo

- *Meta 7*: Poner a disposición de los ciudadanos y las empresas la máxima cantidad de datos, información, trámites y servicios en línea, con énfasis en su calidad y seguridad y en las necesidades de la población de más bajos ingresos y las micro, pequeñas y medianas empresas (MIPYME), y que todos ellos sean accesibles por múltiples medios convergentes interactivos e interoperables. En particular, promover el apoyo a la Red de Líderes de Gobierno Electrónico de América Latina y el Caribe (RED GEALC) como espacio de colaboración e impulso del gobierno electrónico en los países de la región.

- *Meta 9:* Implementar los cambios normativos necesarios para incrementar la interoperabilidad de los servicios públicos usando estándares abiertos, sin menoscabo de la protección de datos personales y del secreto comercial, la seguridad y la estabilidad de los sistemas de información.
- Meta 10: Promover en todos los países de la región la adopción de planes de protección a la infraestructura crítica de los sistemas de información que contemplen, entre otros, sistemas nacionales de respuesta a emergencias cibernéticas (Computer emergency response teams (CERT)) y equipos nacionales y regionales de respuesta ante incidentes relacionados con la seguridad informática (Computer security incident response teams (CSIRT)) y la implementación de formas de interacción y coordinación en respuesta a incidentes de seguridad, así como de intercambio de conocimiento y experiencias.

E. DESARROLLO PRODUCTIVO E INNOVACIÓN

Segundo Lineamiento: Promover el cierre de la brecha digital entre las grandes empresas y las micro, pequeñas y medianas empresas

La política de telecomunicaciones debe promover el acceso, transporte y uso de la banda ancha. El gobierno electrónico debe incrementar la cantidad de trámites en línea disponibles y abrir el sistema de compras públicas electrónicas a la participación de las MIPYME. A su vez, el marco jurídico debe facilitar el uso de la factura electrónica y, al mismo tiempo, dar más seguridad para el comercio electrónico.

F. ENTORNO HABILITADOR

Primer Lineamiento: Elaborar un entorno jurídico que facilite el desarrollo de la sociedad de la información

La difusión de las TIC depende de un adecuado entorno jurídico que asegure la validez de la firma y el documento electrónicos, así como el ágil combate a los delitos por y en medios informáticos, especialmente los referidos a la vida privada, los contenidos que promueven la pornografía infantil, el racismo y la violencia, así como los delitos económicos, como la piratería, el sabotaje, la distribución de virus, el espionaje, la falsificación y el fraude. El entorno jurídico debe asegurar también la transparencia del sector público y la protección de los datos personales. Asimismo, los países deben disponer de una legislación para el mundo digital que equilibre los derechos de autor con los requerimientos sociales de difusión del conocimiento y la información.

Colombia es el país que más genera ataques informáticos en Latinoamérica, seguido de Argentina, Perú, México y Chile. Mientras que a escala mundial, Estados Unidos es el país que lidera, seguido por China, Francia y Holanda [28].

En la figura 1.2 se observa un grafico de barras donde se resalta los sectores más vulnerables a ataques cibernéticos en Latinoamérica hasta el año 2014, estos datos se obtuvieron de [28].

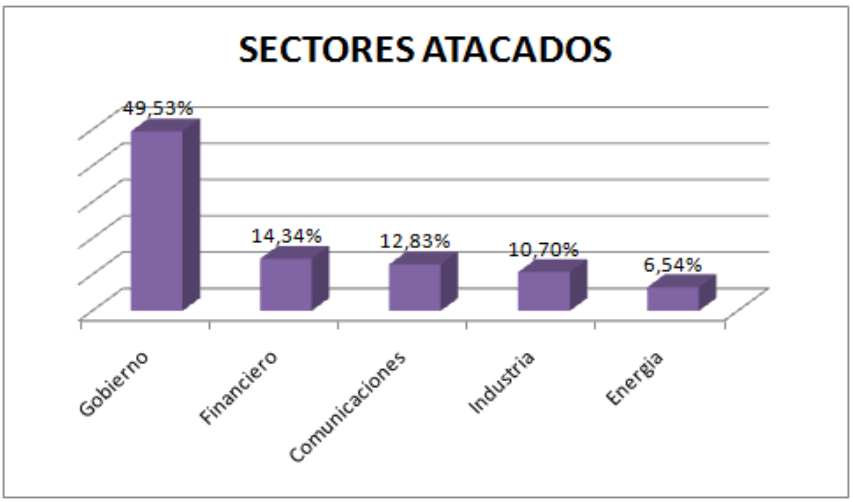


Figura 1.2: Sectores Afectados en Latinoamérica [28]

1.3 Entorno Ecuatoriano

1.3.1 Ciberseguridad en Ecuador

Los primeros tipos penales informáticos que se incluyeron en la legislación ecuatoriana fueron en 2002, en la promulgación de la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, artículos que posteriormente fueron incluidos en la reforma del Código Penal ecuatoriano del año 2003 a través del Título V, desde el artículo 57 al artículo 64, de la Ley de Comercio Electrónico, Firmas y Mensajes de Datos. En la cual se normalizaron delitos como la destrucción maliciosa de documentos, los daños informáticos, la apropiación ilícita, la estafa, delitos contra la información protegida y la violación del derecho a la intimidad.

Según Dmitry Bestuzhev hasta el 2011 en el Ecuador todavía no se trabajaba en seguridad de manera sistemática con políticas definidas.

El Ingeniero Fabián Jaramillo Ex Superintendente de Telecomunicaciones mencionó en el II Foro Regional de Estrategia Ecuador Digital 2.0-Banda Ancha, inaugurado el 20 de Noviembre de 2012 en Quito, que el usuario es el eslabón débil en la cadena de seguridad, porque permite el acceso para que códigos maliciosos ingresen en su computadora; recalca también que hasta el primer trimestre del año 2012 el 84.3% de los ataques reportados eran por códigos maliciosos. Antes de este año los ataques cibernéticos estaban dirigidos a los sitios web de instituciones o empresas; para finales de 2012 también afectaban sistemas de manejo de agua, electricidad, y sistemas de producción de las industrias. En este año el riesgo de posibilidades de infección en Ecuador estaba entre el 21 al 27%.

El 9 de mayo de 2012 durante el evento internacional LACNIC (Latin America & Caribbean Network Information Centre) XVII en Quito, se anunció que se implementaría el Centro de Respuestas a Incidentes Informáticos del Ecuador (CERT - Computer Emergency Response

Team o CSIRT - Computer Security Incident Response Team), para proteger a los ecuatorianos cuando navegan via internet.

En la figura 1.3 se observa el número de denuncias reportado en la Fiscalía General del Ecuador desde el 2009 hasta el 31 de Mayo de 2015, las cuales se obtuvieron de [29].

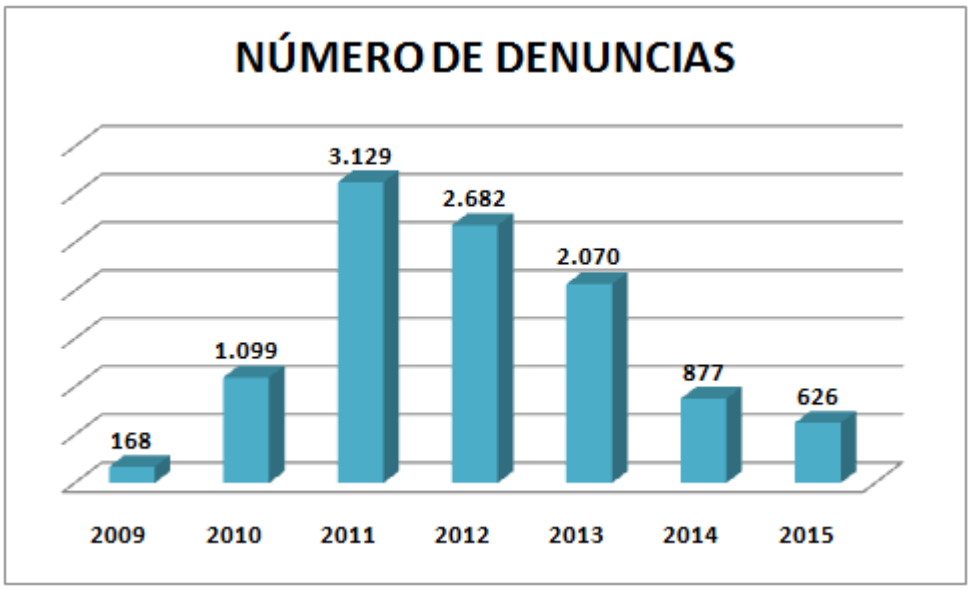


Figura 1.3: Número de denuncias en la Fiscalía General del Ecuador [29]

De acuerdo a la publicación de Diario El Telégrafo del 6 de Enero de 2014, en la sección Justicia, la mayoría de los ciudadanos son víctimas de prácticas como envíos de correos falsos, clonación de tarjetas y falsificación de páginas de los bancos.

Según Diario Expreso en su edición del 10 de septiembre del 2014, en los primeros cinco meses del año 2014 se han registrado 877 denuncias por delitos informáticos. Se menciona también que en el mundo invierten US$ 32.000 millones anualmente en ciberdefensa y que en este año según Kaspersky a escala mundial se detectaron cerca de 60`090.173 fraudes informáticos. Se indica además en la referida edición, que la ex Ministra de Defensa María Fernanda Espinosa afirmó: "*los funcionarios de Gobierno, incluido el Presidente*

de la República, han sido víctimas de ataques y hackeos en sus cuentas en las redes sociales". [29]

El Título V, desde el artículo 57 al artículo 64, de la Ley de Comercio Electrónico, Firmas y Mensajes de Datos fue derogada en la Disposición Derogatoria del Código Orgánico Integral Penal (COIP) publicado en el Suplemento del Registro Oficial No. 180 de 10 de febrero de 2014 y que entró en vigencia 180 días después, en este se incluyen algunas sanciones que reciben las personas que cometen delitos cibernéticos, las cuales se detallan a continuación.

El Artículo 173 sanciona a las personas que a través de un medio electrónico concrete un encuentro con una persona menor de dieciocho años, y este encuentro tenga finalidad sexual o erótica será sancionado con pena privativa de libertad de uno a tres años; si este se da mediante intimidación será sancionado con pena privativa de libertad de tres a cinco años, al igual que la persona que suplante la identidad de una persona y establezca comunicaciones de contenido sexual o erótico con una persona menor de dieciocho años.

En el Artículo 174 se sanciona a la persona que utilice cualquier medio electrónico para ofrecer servicios sexuales con menores de dieciocho años de edad, será sancionada con pena privativa de libertad de siete a diez años.

El Artículo 178 sanciona a la persona que viole la intimidad, interceda a datos de otra persona, o los difunda utilizando medios electrónicos será sancionado con pena privativa de libertad de uno a tres años.

El Artículo 186 sanciona a la persona que, para obtener un beneficio patrimonial para sí misma o para una tercera persona, mediante la simulación de hechos falsos o la deformación u ocultamiento de hechos verdaderos, induzca a error a otra, con el fin de que realice un acto que perjudique su patrimonio o el de una tercera, será sancionada con pena privativa de libertad de cinco a siete años. La pena máxima se aplicará a la persona que:

1. Defraude mediante el uso de tarjeta de crédito, débito, pago o similares, cuando ella sea alterada, clonada, duplicada, hurtada, robada u obtenida sin legítimo consentimiento de su propietario.
2. Defraude mediante el uso de dispositivos electrónicos que alteren, modifiquen, clonen o dupliquen los dispositivos originales de un cajero automático para capturar, almacenar, copias o reproducir información de tarjetas de crédito, débito, pago o similares.
4. Induzca a la compra o venta pública de valores por medio de cualquier acto, práctica, mecanismo o artificio engañoso o fraudulento.
5. Efectúe cotizaciones o transacciones ficticias respecto de cualquier valor. La persona que perjudique a más de dos personas o el monto de su perjuicio sea igual o mayor a cincuenta salarios básicos unificados del trabajador en general será sancionada con pena privativa de libertad de siete a diez años. La estafa cometida a través de una institución del Sistema Financiero Nacional, de la economía popular y solidaria que realicen intermediación financiera mediante el empleo de fondos públicos o de la Seguridad Social, será sancionada con pena privativa de libertad de siete a diez años. La persona que emita boletos o entradas para eventos en escenarios públicos o de concentración masiva por sobre el número del aforo autorizado por la autoridad pública competente, será sancionada con pena privativa de libertad de treinta a noventa días.

El Artículo 190 sanciona a la persona que utilice fraudulentamente un sistema informático o redes electrónicas y de telecomunicaciones para facilitar la apropiación de un bien ajeno o que procure la transferencia no consentida de bienes, valores o derechos en perjuicio de esta o de una tercera, en beneficio suyo o de otra persona alterando, manipulando o modificando el funcionamiento de redes electrónicas, programas, sistemas informáticos, telemáticos y

equipos terminales de telecomunicaciones, será sancionada con pena privativa de libertad de uno a tres años. La misma sanción se impondrá si la infracción se comete con inutilización de sistemas de alarma o guarda, descubrimiento o descifrado de claves secretas o encriptadas, utilización de tarjetas magnéticas o perforadas, utilización de controles o instrumentos de apertura a distancia, o violación de seguridades electrónicas, informáticas u otras semejantes.

El Artículo 191 sanciona a la persona que reprograme o modifique la información de identificación de los equipos terminales móviles, con pena privativa de libertad de uno a tres años.

El Artículo 192 sanciona a la persona que intercambie, comercialice o compre bases de datos que contengan información de identificación de equipos terminales móviles, con pena privativa de libertad de uno a tres años.

El Artículo 193 sanciona a la persona que reemplace las etiquetas de fabricación de los terminales móviles que contienen información de identificación de dichos equipos y coloque en su lugar otras etiquetas con información de identificación falsa o diferente a la original, será sancionada con pena privativa de libertad de uno a tres años.

El Artículo 194 sanciona a la persona que comercialice terminales móviles con violación de las disposiciones y procedimientos previstos en la normativa emitida por la autoridad competente de telecomunicaciones, con pena privativa de libertad de uno a tres años.

El Artículo 195 sanciona a la persona que posea infraestructura, programas, equipos, bases de datos o etiquetas que permitan reprogramar, modificar o alterar la información de identificación de un equipo terminal móvil, con pena privativa de libertad de uno a tres años. No constituye delito, la apertura de bandas para operación de los equipos terminales móviles.

El Artículo 212 sanciona a la persona que de cualquier forma suplante la identidad de otra para obtener un beneficio para sí o para un tercero, en perjuicio de una persona, será sancionada con pena privativa de libertad de uno a tres años.

El Artículo 229 sanciona a la persona que, en provecho propio o de un tercero, revele información registrada, contenida en ficheros, archivos, bases de datos o medios semejantes, a través o dirigidas a un sistema electrónico, informático, telemático o de telecomunicaciones; materializando voluntaria e intencionalmente la violación del secreto, la intimidad y la privacidad de las personas, será sancionada con pena privativa de libertad de uno a tres años. Si esta conducta se comete por una o un servidor público, empleadas o empleados bancarios internos o de instituciones de la economía popular y solidaria que realicen intermediación financiera o contratistas, será sancionada con pena privativa de libertad de tres a cinco años.

Según el Artículo 230 será sancionada con pena privativa de libertad de tres a cinco años:

1. La persona que sin orden judicial previa, en provecho propio o de un tercero, intercepte, escuche, desvíe, grabe u observe, en cualquier forma un dato informático en su origen, destino o en el interior de un sistema informático, una señal o una transmisión de datos o señales con la finalidad de obtener información registrada o disponible.
2. La persona que diseñe, desarrolle, venda, ejecute, programe o envíe mensajes, certificados de seguridad o páginas electrónicas, enlaces o ventanas emergentes o modifique el sistema de resolución de nombres de dominio de un servicio financiero o pago electrónico u otro sitio personal o de confianza, de tal manera que induzca a una persona a ingresar a una dirección o sitio de internet diferente a la que quiere acceder.

3. La persona que a través de cualquier medio copie, clone o comercialice información contenida en las bandas magnéticas, chips u otro dispositivo electrónico que esté soportada en las tarjetas de crédito, débito, pago o similares.
4. La persona que produzca, fabrique, distribuya, posea o facilite materiales, dispositivos electrónicos o sistemas informáticos destinados a la comisión del delito descrito en el inciso anterior.

El Artículo 231 sanciona a la persona que, con ánimo de lucro, altere, manipule o modifique el funcionamiento de programa o sistema informático o telemático o mensaje de datos, para procurarse la transferencia o apropiación no consentida de un activo patrimonial de otra persona en perjuicio de esta o de un tercero, será sancionada con pena privativa de libertad de tres a cinco años. Con igual pena, será sancionada la persona que facilite o proporcione datos de su cuenta bancaria con la intención de obtener, recibir o captar de forma ilegítima un activo patrimonial a través de una transferencia electrónica producto de este delito para sí mismo o para otra persona.

El Artículo 232 sanciona a la persona que destruya, dañe, borre, deteriore, altere, suspenda, trabe, cause mal funcionamiento, comportamiento no deseado o suprima datos informáticos, mensajes de correo electrónico, de sistemas de tratamiento de información, telemático o de telecomunicaciones a todo o partes de sus componentes lógicos que lo rigen, será sancionada con pena privativa de libertad de tres a cinco años. Con igual pena será sancionada la persona que:

1. Diseñe, desarrolle, programe, adquiera, envíe, introduzca, ejecute, venda o distribuya de cualquier manera, dispositivos o programas informáticos maliciosos o programas destinados a causar los efectos señalados en el primer inciso de este artículo.

El Artículo 233 la persona que destruya o inutilice información clasificada de conformidad con la Ley, será sancionada con pena

privativa de libertad de cinco a siete años. La o el servidor público que, utilizando cualquier medio electrónico o informático, obtenga este tipo de información, será sancionado con pena privativa de libertad de tres a cinco años. Cuando se trate de información reservada, cuya revelación pueda comprometer gravemente la seguridad del Estado, la o el servidor público encargado de la custodia o utilización legítima de la información que sin la autorización correspondiente revele dicha información, será sancionado con pena privativa de libertad de siete a diez años y la inhabilitación para ejercer un cargo o función pública por seis meses, siempre que no se configure otra infracción de mayor gravedad.

El Artículo 234 sanciona a la persona que sin autorización acceda en todo o en parte a un sistema informático o sistema telemático o de telecomunicaciones o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho, para explotar ilegítimamente el acceso logrado, modificar un portal web, desviar o re direccionar de tráfico de datos o voz u ofrecer servicios que estos sistemas proveen a terceros, sin pagarlos a los proveedores de servicios legítimos, será sancionada con la pena privativa de la libertad de tres a cinco años.

El Artículo 354 sanciona a la o el servidor militar, policial o de servicios de inteligencia que en tiempo de paz realice uno de estos actos, será sancionado con pena privativa de libertad de siete a diez años, cuando:

1. Obtenga, difunda, falsee o inutilice información clasificada legalmente y que su uso o empleo por país extranjero atente contra la seguridad y la soberanía del Estado.
2. Intercepte, sustraiga, copie información, archivos, fotografías, filmaciones, grabaciones u otros sobre tropas, equipos, operaciones o misiones de carácter militar o policial.

3. Envíe documentos, informes, gráficos u objetos que pongan en riesgo la seguridad o la soberanía del Estado, sin estar obligado a hacerlo o al haber sido forzado no informe inmediatamente del hecho a las autoridades competentes.
4. Oculte información relevante a los mandos militares o policiales nacionales.
5. Altere, suprima, destruya, desvíe, incluso temporalmente, información u objetos de naturaleza militar relevantes para la seguridad, la soberanía o la integridad territorial. Si la o el servidor público realiza alguno o varios de estos actos en tiempo de conflicto armado, será sancionado con pena privativa de libertad de diez a trece años.

En el Artículo 476 la o el juzgador ordenará la interceptación de las comunicaciones o datos informáticos previa solicitud fundamentada de la o el fiscal cuando existan indicios que resulten relevantes a los fines de la investigación, de conformidad con las siguientes reglas:

4. Previa autorización de la o el juzgador, la o el fiscal, realizará la interceptación y registro de los datos informáticos en transmisión a través de los servicios de telecomunicaciones como: telefonía fija, satelital, móvil e inalámbrica, con sus servicios de llamadas de voz, mensajes SMS, mensajes MMS, transmisión de datos y voz sobre IP, correo electrónico, redes sociales, videoconferencias, multimedia, entre otros, cuando la o el fiscal lo considere indispensable para comprobar la existencia de una infracción o la responsabilidad de los partícipes.

En la agenda política de defensa de las FF.AA. se ha incluido un proyecto para constituir el Comando de Operaciones Cibernéticas que está operativo desde 2015 y requirió una inversión inicial de US$ 8’000.000.

Centro de Respuesta a Incidentes Informáticos

La idea de un Centro de Respuestas a Incidentes Informáticos debe ser detectar e identificar la amenaza, bloquearla, monitorizarla, reportar, guardar registros y evidencias de la amenaza, responderla, pedir información a los organismos actores involucrados dentro de la respuesta a la amenaza de ser necesario, hacer uso de la infraestructura disponible y necesaria y comunicar a los demás equipos de apoyo o CSIRTs conectados, para así mitigar las posibles consecuencias que produce un incidente de seguridad informática. [30]

1.4 Delitos Cibernéticos

1.4.1 Delitos contra la confidencialidad, la integridad y la disponibilidad de datos y sistemas informáticos

Acceso ilícito a Sistemas Informáticos

Los delitos clasificados como “piratería” se refieren al acceso ilícito a un sistema informático, este es uno de los delitos más antiguos en este campo [31]. Algunos ejemplos de delitos de piratería son irrupción de sitios web protegidos con contraseña [32] y la burla de protección de contraseña de un computador.

Los motivos de los ciberdelincuentes son diversos. Algunos se limitan a burlar la seguridad informática solo para probar sus capacidades, tal es el caso del ataque que tuvo la NASA (National Aeronautics and Space Administration) en agosto de 1999, un adolescente de 16 años llamado Jonathan James irrumpió su seguridad y logró tener acceso además al sistema informático del Departamento de Defensa de Estados Unidos. Otros actúan por motivos políticos (conocido como piratería activista o hacktivism) como es el caso de Edward Snowden, que es un analista de sistemas especializado en seguridad informática que trabajaba para la Agencia de Seguridad Nacional (NSA, por sus

siglas en inglés) que reveló como Estados Unidos espiaba a sus ciudadanos, al gobierno de otros países y, a prácticamente cualquiera a través de la actividad de internet y los registros de llamadas telefónicas.

Muchas veces el fin del delincuente no es la perpetración del sistema, sino solo es el medio para realizar la manipulación de datos, el espionaje o la denegación del servicio.

En Ecuador este delito está tipificado en el artículo 415 numeral 1 del Código Penal, con una pena que va desde los tres hasta los cinco años de cárcel y una multa desde 200 hasta 600 dólares americanos. [33]

Espionaje de Datos

Los sistemas informáticos contienen con frecuencia información confidencial; si se está conectado a internet, los ciberdelincuentes pueden acceder a su información desde cualquier parte del mundo, la información confidencial puede ser muy valiosa; por ejemplo en 1980 varios piratas alemanes consiguieron entrar en el sistema de seguridad de Estados Unidos, y le vendieron información obtenida a agentes de la Unión Soviética. Los delincuentes siempre encuentran varias formas de acceder a los sistemas informáticos de sus víctimas [34]

Interceptación ilícita de Datos Informáticos

Los ciberdelincuentes pueden interceptar transferencias de datos con el fin de registrar el intercambio de información. Los delincuentes pueden atacar cualquier infraestructura de comunicaciones y cualquier servicio Internet. Las tecnologías inalámbricas gozan de mayor popularidad; hoy en día hoteles, bares y restaurantes ofrecen acceso a Internet a sus clientes a través de puntos de acceso inalámbrico, los delincuentes que deseen pinchar las comunicaciones de datos pueden hacerlo desde cualquier lugar dentro del radio de comunicación entre

el computador y el punto de acceso (el radio de acceso depende de la potencia transmisora del punto de acceso). Aún cuando las comunicaciones inalámbricas estén cifradas, los ciberdelincuentes son capaces de descifrarlas y guardar los correspondientes datos. Para conseguir acceso a información confidencial los delincuentes configuran puntos de acceso dentro del radio del punto de acceso original, seleccionan un nombre de tal manera que los clientes seleccionen el punto de acceso fraudulento; si los usuarios confían en el proveedor de acceso para proporcionar seguridad, lo más probable es que no apliquen sus propias medidas de seguridad, y sea más fácil interceptar las comunicaciones.

Actualmente existe una herramienta específica diseñada para registrar las pulsaciones realizadas en el teclado de un equipo. Gracias a esta herramienta el ciberdelincuente puede robar un gran volumen de información confidencial sin que la víctima se percate de ello; su nombre es keylogger y es un tipo de software malintencionado que se sitúa entre el teclado y el sistema operativo. En ataques mayores los delincuentes pueden acceder a la computadora de su víctima por acceso remoto y guardar su información en otro equipo. La manera más común de infectar un equipo es a través de una web maliciosa, la cual ataca lo vulnerable del equipo e instala el software malintencionado; otro método es a través de descarga de una aplicación legítima, atacando el canal de descarga o instalando el software malintencionado en dicha aplicación. [35]

Atentado contra la Integridad de los Datos Informáticos

Los datos informáticos son de vital importancia en empresas públicas y privadas, los usuarios privados y en general para cualquier tipo de administración; los infractores pueden atentar contra la integridad de los datos borrándolos, alterándolos, suprimiéndolos o restringiendo su acceso. Los virus informáticos son un ejemplo bastante común de supresión de datos. [33]

Atentado contra la Integridad del Sistema Informático

Es posible realizar ataques físicos a los sistemas informáticos; si el delincuente tiene acceso físico al sistema informático puede destruir los equipos. Algunos ejemplos de ataques a sistemas informáticos a distancia son los gusanos o los ataques de denegación de servicio (DoS). Un ejemplo claro de este tipo de atentados es el gusano informático Stuxnet, que fue descubierto en el año 2010, el cual alteró el funcionamiento de un proceso industrial, ya que fue diseñado con la finalidad de dañar equipos físicos y modificar las indicaciones de los operadores a cargo de la supervisión, para impedir, de este modo, que se identificara cualquier anomalía en los equipos [36]. A diferencia de los gusanos los ataques de denegación de servicio atacan a un objetivo único, en el año 2000 durante un pequeño intervalo empresas del alcance de CNN, Ebay y Amazon sufrieron ataques DoS, inhabilitando sus servicios durante horas o inclusive días. [33]

1.4.2 Delitos relacionados con el contenido

Material erótico o pornográfico (excluida la pornografía infantil)

En algunos países la pornografía no infantil también es ilegal.

En África los países de Argelia, Egipto, Libia, Sudán, Nigeria y Ethiopia el intercambio de pornografía entre adultos se considera un acto ilegal.

Mientras que en Sudáfrica la pornografía es legal en Internet, pero la pornografía emitida por un canal de televisión abierto o por suscripción se considera ilegal.

La realidad en Europa resulta ser un poco diferente; en el año 2014 todos los proveedores de internet bloquearon el acceso a páginas web pornográficas a sus clientes, con el legítimo deber de proteger a los menores de edad del acceso a contenido pornográfico; el filtro impuesto por los proveedores solo será quitado si una persona adulta

expresa que así lo desea, cabe resaltar que los teléfonos móviles que llegaron al mercado también tuvieron ese filtro restrictivo.

El continente asiático ha sido un poco más estricto respecto a este tema, a principios del 2015 el Servicio Federal de Supervisión de Telecomunicaciones ruso anunció el bloqueo inmediato a 11 portales de internet de contenido pornográfico, pues albergaban contenidos ilegales relacionados con menores de edad. Recordando que India tiene el mayor número de usuarios de pornografía después de China, el gobierno indio a mediados del 2015 decidió bloquear 857 páginas web debido a que atentan contra la decencia y moral

Mientras que en Australia la pornografía es legal pero posee restricciones, la Oficina de Aduanas de Australia está en pleno poder de realizar la búsqueda de pornografía en teléfonos celulares, tablets y computadoras portátiles a personas que arriben al país. [33]

Pornografía infantil

A nivel global la pornografía infantil se considera como un acto criminal, a diferencia de la pornografía adulta que es legal o ilegal dependiendo del país al que se pregunte. Se considera ilegal su reproducción, comercialización y consumo en todo el mundo, sin embargo debido al internet y su inmensa popularidad y muchas veces anonimato que presta, este delito se sigue cometiendo, sobre todo en la deep web (internet profunda), ya que la mayor parte de la web no es accesible por buscadores estándar, para accesar a la deep web se debe utilizar un programa que esconda sus direcciones MAC (Media Access Control) y física y además que sea capaz de acceder a la deep web, la venta de pornografía infantil es muy lucrativa, ya que los coleccionistas están dispuestos a pagar altas sumas de dinero, por ver a niños en un contexto sexual. [33]

Racismo, lenguaje ofensivo y exaltación de la violencia

Los grupos radicales e insurgentes utilizan la capacidad que posee Internet para acceder a la mayoría de hogares, para llegar a personas a manera de propaganda, con distintos fines, entre ellos la adhesión de nuevos miembros a sus filas, como es el caso del grupo ISIS (Islamic State of Iraq and Syria), autoproclamado como Estado Islámico, ya que en teoría representa los ideales de todos los musulmanes, grupo que en efecto sube videos a Internet para difundir de manera global sus masacres y decapitaciones, y así poder crear un impacto en la manera de pensar de todo individuo que lo vea, y este grupo ha logrado su objetivo, ya que algunos musulmanes de todo el mundo se han adherido a sus filas, inclusive musulmanes que residen en Australia y el Reino Unido; pero no solamente lo utilizan como propaganda, Internet también puede ser utilizado como herramienta para comprar, vender, intercambiar artículos relacionados con ideologías nazi, como banderas con símbolos, libros y uniformes. La difusión de correos electrónicos, videos subidos a plataformas como Youtube y boletines informativos.

Cabe recalcar que estos actos no están penalizados en todos los países, ya que en algunos países se amparan bajo el principio de libertad de expresión. Un ejemplo de conflictos de leyes y censura en Internet es el caso de la empresa estadounidense de servicios en línea Yahoo! que fue denunciado por la asociación francesa Ligue contre le Racisme et l'Antisémitisme (LICRA), que lucha contra el racismo y el antisemitismo por la venta de artículos nazis; en Estados Unidos la primera enmienda constitucional avala el derecho a la libre expresión de las ideas, mientras que en Francia existen disposiciones legales contra el nazismo: usar o exhibir en público una insignia o un emblema que evoque una asociación declarada como criminal, en este caso los artículos nazis (R-645-1 del código penal francés). [37]

Delitos contra la religión

Algunos países penalizan la disponibilidad de información o material en la web que pueda afectar directa o indirectamente los sentimientos religiosos de sus creyentes, cada vez son más frecuentes las apariciones o despliegues de blogs o diferentes sitios webs abiertos a debates, amparados bajo la libertad de expresión, sin embargo en el marco penal de algunos países están contemplados este tipo de delitos, como por ejemplo la formulación de observaciones peyorativas sobre el Sagrado Profeta o la profanación de copias del Corán. [33]

Juegos ilegales y juegos en línea

Los juegos de azar no son muy bien vistos por las legislaciones de ciertos países, debido a la alta tasa de concurrencia y poco control que existe en internet, algunos de estos juegos en línea han sido utilizados para realizar ciertos delitos entre ellos fraude, intercambio y presentación de pornografía infantil y difamación.

Algunos países como España requieren de un título habilitante para poder ofrecer determinados juegos, los cuales serán juegos regulados, éstos están detallados por la Dirección General de Ordenación del Juego, la cual recalca que cualquier juego no regulado será denominado como prohibido y deberá atenerse a las sanciones del caso, dichas sanciones pueden llegar a un monto de 50 millones de euros. [33]

Difamación o información falsa

Bajo la premisa de la libre opinión, Internet se ha convertido en un sitio virtual lleno de foros de debate, blogs personales y redes sociales, en los cuales puede publicarse tanto información falsa como fidedigna.

En muchos casos las personas infractoras se aprovechan de que el proveedor que ofrece la publicación gratuita o económica no verifica o no exige que cada usuario publique sus verdaderos datos personales para poder identificarlo; casos como publicaciones de fotografías de

carácter íntimo o información falsa sobre hábitos sexuales son algunos ejemplos de estos delitos.

Pero no siempre se utiliza la colaboración de publicaciones particulares para fines delictivos, Wikipedia es un gran ejemplo de esto, autoproclamada como una enciclopedia libre y accesible por todos. [33]

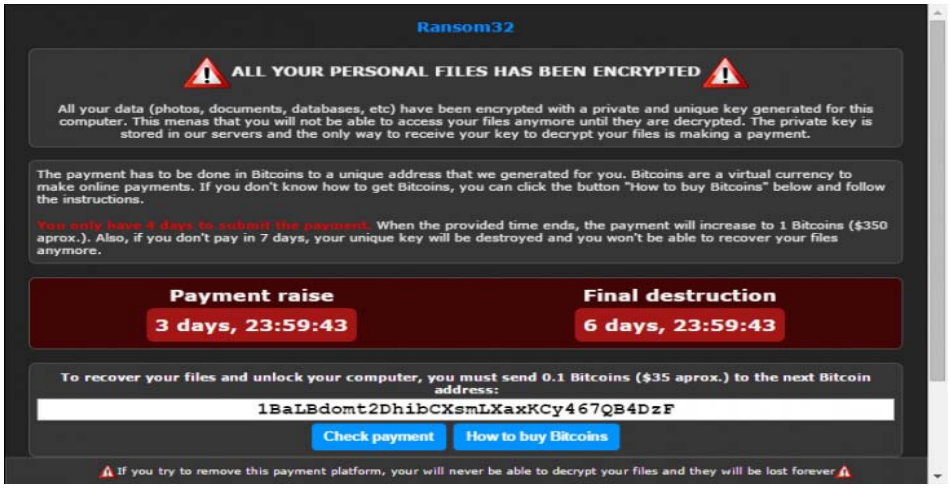
Correo basura y amenazas conexas

El envío masivo de mensajes no solicitados se lo denomina correo basura, también denominado spam. Los infractores envían miles de millones de correos basura con fines publicitarios o anunciantes, a menudo también se envían software de carácter pernicioso. Los correos basura son enviados a menudo por redes zombi, llamadas botnets [38], estas redes controlan un conjunto de robots informáticos de forma remota para que infecten a los servidores, y muchos de ellos hacen llegar los correos no deseados. Sin embargo se tienen informes de que en el 2015 el nivel de spam ha sido el más bajo de los últimos 12 años, esto se debe en gran parte a la lucha de los Estados a nivel mundial, en el Reino Unido la policía ha desmantelado 7 botnets distintos, la lucha en América Latina también es constante, ya que los países de Argentina, Brasil y México son tres de las mayores fuentes de spam con 3.23%, 2.78% y 1.73% a nivel mundial.

Pero sabemos que la tecnología está en evolución constante, así que desde el 2014 la Corporación de Internet para la Asignación de Nombres y Números de Dominio (ICANN, por sus siglas en inglés) permitió el registro de otras terminales de dominio tales como .cool, .work, .tienda, .viajes, hasta ahora estaban las terminales .edu, .org, .com, o también las que se asignaban a los países como .co (Colombia), .ec (Ecuador), .uk (United Kingdom); al cambiar las terminales de dominio se dio paso a una nueva forma de spam. Así los correos enviados desde direcciones de dominio, por ejemplo .work, hacen referencia o publicidad a ofertas de trabajo o mantenimiento del

hogar, o los de .science hacen publicidad a registros de educación a distancia en centros de educación a distancia. Recordemos que la publicidad de este tipo de correos no necesariamente es verdadera, a menudo es publicidad engañosa y en muchos casos es la puerta de entrada a software malintencionado, también llamado malware. La mala noticia es que si bien el volumen de spam ha disminuido, la creación de nuevos softwares malintencionados es cada vez mayor, tal es el caso de un software llamado ransomware, cada vez más popular y más actual, este tipo de software suele llegar en un correo, al abrirlo se instala en la computadora y encripta todos tus archivos Windows, Mac OS X o Linux y te amenaza con borrarlos, a no ser que pagues una cierta cantidad de dinero. En enero del 2016 hizo su aparición un nuevo malware de este tipo llamado Ransom32 [39].

El mensaje de amenaza que genera el malware Ransom32 se puede observar en la figura 1.4.



Fuente: EMSISOFT Blog

Figura 1.4: Aviso de rescate mostrado por el malware Ransom32 [39]

Otras formas de contenido ilícito

El Internet no solamente es utilizado por los infractores o delincuentes para dar ataques directos, puede ser usado para proporcionar

información o instrucciones para la manipulación de elementos con los que puedan manufacturar y operar artículos perjudiciales no solo para el que los fabrica, sino para las personas a su alrededor; por ejemplo, es natural encontrar recetas para preparar potentes venenos o en algunos casos armas, además la web es utilizada entre muchas otras cosas para la venta de diferentes productos y servicios, sin embargo la legalidad de un producto está únicamente dada por la legislación de cada país, y una tienda de la web situada en un país en el que la comercialización de un producto es totalmente legal puede vender a todo el mundo, independientemente de que el comprador resida en un país en el cual la venta de dicho producto no es legal. [33]

1.4.3 Delitos en materia de derechos de autor y de marcas

Delitos en materia de derechos de autor

Desde el inicio de la digitalización, al pasar todos los sistemas analógicos y digitales e incorporar a la industria del ocio la prestación de servicios a los DVD como subtítulos, avances, cambio de idioma. Este cambio ha dado paso a nuevos tipos de posibles violaciones de derechos de autor; antes de la digitalización la copia de un disco o de un casete no tenía la misma calidad que la original, actualmente la pérdida de calidad es nula ayudando a la proliferación de copias de las copias. [33]

Delitos en materia de marcas

La reputación de una empresa está por lo general relacionada a su marca, los delitos que se hacen afectando o utilizando la marca de una empresa, muchas veces junto con su nombre pueden dañar la reputación o la confiabilidad de la marca para siempre, en muchas veces se hace esto con la ayuda de internet, como es el caso de la técnica del phishing, (pesca, en español) la cual es un delito informático que consiste en realizar una estafa utilizando el nombre y

marca de un tercero, sus víctimas son principalmente los bancos, los infractores mandan millones de correos a sus víctimas con el nombre y la marca de la empresa, al abrir este correo los usuarios son re direccionados a una supuesta página web de la empresa, los más experimentados copian con exactitud la página web de la entidad bancaria y el usuario al querer accesar a la página web con su nombre y su contraseña y en eventos posteriores se podrá llegar a dar casos de usurpación de identidad o de recargos importantes a tarjetas de crédito, en casos bancarios. [33]

1.4.4 Delitos informáticos

Fraude y fraude informático

En internet hay fraudes muy difundidos con los que no se utiliza ningún sistema informático, aunque empleen una tecnología informática, por lo cual algunas legislaciones no los considera delitos informáticos, sino fraudes comunes, un timo muy común es la llamada estafa nigeriana, la cual utiliza una técnica en la cual hacen que sus víctimas pierdan una cantidad lo suficientemente baja de dinero, como para que la probabilidad de que pierdan tiempo y energía reportando o haciendo la debida investigación para rastrear a los estafadores sea muy baja, la estafa nigeriana consiste en hacer que sus víctimas crean que se les va a retribuir una cantidad muy grande de dinero a cambio de que solo paguen los impuestos de la transacción, utilizan un lenguaje muy educado y a menudo son muy convincentes. De acuerdo con informes del Departamento de Estado, ciertas personas que han respondido a este correo electrónico han sido amenazadas e incluso algunas asesinadas.

Las subastas en línea es otro de los fraudes más habituales en línea, que puede afectar tanto al comprador como a la persona que subasta; se puede ofrecer toda clase de artículos de dudosa procedencia o peor aún no disponibles para la venta y exigir su pago por adelantado

y por el otro lado se puede solicitar mercancía para su envío sin intención alguna de concretar el pago convenido. [33]

Falsificación informática

Se entiende por falsificación a la manipulación o alteración de documentos digitales, como por ejemplo crear un documento que parece de una institución fiable tal como se hace en el phishing o alterar imágenes.

Para poder ganar una contienda judicial, las contrapartes deben de presentar las pruebas competentes al caso, las pruebas de tipo digital pueden ser correos electrónicos o mensajes enviados por cualquier plataforma de mensajería instantánea como Whatsapp. Al ser el servicio de mensajería instantánea más utilizado a nivel mundial (un décimo de toda la población mundial lo utiliza), en algunos casos judiciales se han aceptado este tipo de pruebas, pero antes se debe de presentar la adveración de un perito informático, ya que Whatsapp es una aplicación insegura fácilmente manipulable [40].

En el caso de los documentos, en el pasado solo se reconocían como legítimos los documentos físicos, pero con los avances de las tecnologías de la información y la comunicación, los documentos digitales han sido reconocidos, sustituyendo a los documentos físicos, avalándose legalmente con firmas electrónicas.

Robo de identidad

La identidad digital de una persona es de suma importancia, ya que desde la web se accede a diferentes servicios, entre ellos los de índole bancaria involucrando tarjetas de crédito, códigos de acceso asociados a una cuenta, entre otros; los estafadores usan los distintos tipos de técnicas de la ingeniería social, que lo que busca es manipular a las personas para que éstas hagan lo que ellos quieren. Según Kevin Mitnick, conocido como el mejor hacker de la historia, el éxito de las técnicas de ingeniería social se basa en 4 principios:

1. Todos queremos ayudar.
2. El primer movimiento es siempre de confianza hacia el otro
3. No nos gusta decir no.
4. A todos nos gusta que nos alaben.

Los datos que más solicitan los atacantes son el número de seguridad social o pasaporte, la fecha de nacimiento, dirección y números de teléfono y las contraseñas de cuentas financieras y no financieras. [33]

Utilización indebida de dispositivos

Todos los equipos informáticos pueden utilizarse para cometer un delito informático, desde los equipos más básicos para realizar actividades perniciosas efectivas mezclándolas con técnicas de ingeniería social, hasta los equipos más sofisticados, cuyo funcionamiento se haya muchas veces detallado en internet, para realizar ataques más específicos y peligrosos. Debido a la simplificación y al acceso global a múltiples herramientas para poder realizar ciberdelitos, el número de infractores o atacantes ha crecido a escala mundial. [33]

1.5 Problema a resolver

El problema a resolver es el incremento descontrolado del fraude cibernético y de los ataques informáticos que se dan en la actualidad en el Ecuador. La dependencia del ciberespacio cada vez es mayor, tanto para empresas como para personas naturales; realizar todo tipo de trámites se ha facilitado por medio de internet pero del mismo modo se facilitan los fraudes y robos.

Con los muchos avances de la tecnología y la facilidad de acceder a una computadora los ataques cibernéticos han ido incrementándose; este uso indebido de las computadoras es lo que ha provocado que se necesite la creación de leyes y normas que regulen todos estos ataques, así como penas legales para las personas que los efectúan.

Los ataques o delitos informáticos involucran robos, fraudes, estafas, entre otros y con el paso de los años se ha hecho más sencillo realizarlos, tanto así que por medio de la web se puede encontrar como realizar casi todos estos delitos y cualquier persona con acceso a una computadora y conexión a la red pueden de manera sencilla encontrar métodos para realizarlos, de igual forma pueden encontrar como falsificar la dirección IP o la dirección MAC de su computadora, para de este modo, poder protegerse de ser encontrados realizándolos, lo que dificulta que puedan ser atrapados y por consiguiente fomenta que más personas los realicen, ya que, si realizan pequeños ataques y no los hacen de manera frecuente las posibilidades de ser atrapados es mínima; la falta de información acerca de las leyes que sancionan a estos atacantes también produce que las personas que son víctimas de ellos no los denuncien, quizás por miedo a venganzas por parte de los atacantes, o porque piensan que es una pérdida de tiempo dado que las leyes no son muy fuertes en nuestro país, o simplemente no saben que este tipo de actos son penados por la ley; muchas veces las personas que son víctimas de la ciberdelincuencia no se enteran sino hasta mucho después de realizado, ya que no usan frecuentemente la red, por tanto no están revisando todo el tiempo sus cuentas.

1.6 Objetivo General

Proponer un diseño de un Plan de Acción para la Optimización en los Procesos de los Centros de Incidentes Informáticos en Ecuador

1.7 Objetivos Específicos

1. Identificar los distintos centros de gestión de incidentes informáticos en el Ecuador, además de sus debilidades y fortalezas con el fin de elaborar un Plan de Acción que se enfoque en minimizar las debilidades y afianzar las distintas fortalezas.

2. Evaluar los sistemas de prevención que utilizan las entidades públicas y privadas para prevenir ser víctima de algún delito cibernético, a fin de proponer una optimización para estos.
3. Incentivar a los organismos encargados de la ciberseguridad en Ecuador a difundir los derechos y obligaciones de la ciudadanía al momento de navegar en la web.
4. Elaborar un diagrama de flujo del proceso que deberían seguir los centros de respuesta a incidentes informáticos desde que reciben el incidente hasta que le dan solución.

1.8 Alcance

El trabajo de investigación propuesto aspira abarcar la mayor parte de los delitos cibernéticos ocurridos, que afecten directa o indirectamente la soberanía, seguridad e identidad del Estado ecuatoriano, así como de las personas naturales o jurídicas que habitan en Ecuador, para esto se investigarán y analizarán las diferentes prácticas y procedimientos que utilizan los centros de respuesta a incidentes informáticos en el país; exceptuando al Centro de Operaciones Cibernéticas del Ecuador debido a la falta de disponibilidad de las personas indicadas que podrían brindarnos la información necesaria para la elaboración de la propuesta de este documento.

1.9 Justificación

La seguridad que se tiene en la web no es muy confiable y esto da cabida a que cualquier persona pueda apropiarse de información confidencial, por lo cual es necesario que haya una protección frente a todos estos robos y ataques que se están dando en Ecuador cada vez de manera más frecuente. Dado a las crecientes actividades transaccionales realizadas a través de la web, se da la oportunidad para el crecimiento de actividades no lícitas; esto se debe en gran parte a los beneficios de la globalización que trae consigo

que los usuarios puedan conectar sus cuentas desde varios dispositivos al mismo tiempo, en gran parte esto es de ayuda ya que se pueden realizar todo tipo de transacciones desde cualquier lugar donde estemos y además tener en línea varios dispositivos; pero de igual manera esto nos hace más vulnerables a ataques ya que con que una persona pueda acceder a cualquiera de estos dispositivos ya puede tener acceso a todas nuestras cuentas y hackearlas de maneras sencillas.

Mejorar la efectividad a la hora de desplegar una acción en el ámbito de la ciberseguridad en el Ecuador es una manera de que se pueda elevar la confianza digital la cual se ha reducido considerablemente por miedo a todos los ataques que se tienen. Las personas a sabiendas de que pueden realizar muchos trámites por medio de la red prefieren hacerlos personalmente, por miedo a que sus cuentas sean robadas o clonadas; este miedo es el que se quiere ayudar a disminuir dando a las personas una mayor seguridad y protección en todo momento que se encuentren en la red, además de enseñarles cómo proteger sus propias cuentas de estos tipos de ataques, o por lo menos hacerlas menos vulnerables y por tanto menos atractivas para estos ciberdelincuentes.

CAPÍTULO 2

2. DISEÑO DEL PLAN DE ACCIÓN

2.1. Centros responsables de la ciberseguridad en Ecuador

2.1.1. EcuCERT

El Centro de Respuesta a Incidentes Informáticos de la Agencia de Regulación y Control de las Telecomunicaciones del Ecuador (EcuCERT), es el organismo encargado actualmente de la seguridad de las redes de telecomunicaciones de todo el país, así como el uso de la red de internet; este coopera con otros equipos CSIRT dentro y fuera del Ecuador.

Su misión es brindar a su Comunidad Objetivo el apoyo en la prevención y resolución de incidentes de seguridad informática, a través de la coordinación, capacitación y soporte técnico [41].

Su principal fin es lograr masificar el uso de internet, las TIC y los sistemas de telecomunicaciones en todo nuestro país, mediante la coordinación, nacional e internacional de acciones técnicas destinadas a lograr usos más seguros de las redes, que satisfagan la confianza de la comunidad que las utiliza.

Su comunidad objetivo es la Agencia de Regulación y Control de las Telecomunicaciones, el sector de las telecomunicaciones nacionales y las instituciones del Estado Ecuatoriano, así como aquellas instituciones del sector privado que demanden sus servicios.

En una entrevista con Marco Rivadeneira Fuentes Coordinador del EcuCERT el 14 de enero de 2016, se pudo conocer que actualmente EcuCERT trabaja con incidentes que reciben ya sea por denuncias en su página web, o por stakeholders que son personas objetivos que pueden afectar ser afectadas por un incidente cibernético. Actualmente EcuCERT maneja 4 redes que

son una red para ARCOTEL (Agencia de Regulación y Control de las Telecomunicaciones), esta red es burocrática y es para manejo de las regulaciones en general; una segunda red que es para uso interno de EcuCERT en la cual se gestionan y se da seguimiento a los incidentes; la tercera es una red de laboratorio, la cual usan para analizar los incidentes por medio de un Sandbox, también tienen un equipo llamado Fred el cual lo utilizan para copiar toda la información de algún equipo que pudiera estar infectado y así poder analizarlo sin romper la cadena de custodia en el caso de que el incidente tenga consecuencias penales; y por último una red forense la cual usan para análisis. Hasta el momento EcuCERT no cuenta con equipos para monitorear y prevenir estos incidentes por falta de presupuesto, por lo cual lo hacen a través de stakeholders.

Cuando EcuCERT recibe un incidente lo marca para poderle dar seguimiento, luego informa al ISP (Internet Service Provider) que maneja la red afectada para que ellos solucionen el incidente, y como aún no existe una normativa que regule el tiempo en que el ISP debe dar una solución a este incidente a EcuCERT no le queda más que esperar a que el ISP le dé solución cuando sea posible. Casi todos los incidentes que reciben son críticos ya que de alguna manera se ve afectada una red ya sea para robo de información, transgiversar datos, desfigurar páginas, etc.

EcuCERT trabaja en conjunto con el USCERT (Centro de Respuestas a Incidentes de Estados Unidos), y utiliza su Protocolo TLP (Protocolo Semáforo en inglés Traffic Light Protocol) para la gestión de incidentes; este protocolo es un conjunto de designaciones usadas para asegurar que la información confidencial se comparta con la audiencia correcta. Emplea cuatro colores para indicar diferentes grados de sensibilidad y las consideraciones de intercambio

correspondientes a aplicar por el o los destinatarios como se muestra en la tabla 1 [42].

COLOR	¿Cuándo debe ser usado?	¿Cómo debe ser compartida?
ROJO	Las fuentes pueden utilizar TLP: ROJO cuando la información no se puede desempeñar con eficacia sobre los grupos adicionales, y podría conducir a impactos sobre la privacidad, reputación, u operaciones de los grupos si se utilizan mal.	Los beneficiarios no pueden compartir información de TLP: ROJO con terceros fuera del intercambio específico, reunión o conversación en la que se discute en un principio.
AMBAR	Las fuentes pueden utilizar TLP: AMBAR cuando la información requiere de apoyo para que se desarrolle de manera efectiva, pero conlleva riesgos para la privacidad, reputación u operaciones si es compartida fuera de las organizaciones involucradas.	Los beneficiarios sólo podrán compartir información TLP: AMBAR con miembros de su propia organización que necesiten saber, y sólo lo más ampliamente necesario para actuar sobre esa información.
VERDE	Las fuentes pueden utilizar TLP: VERDE cuando la información es útil para el conocimiento de todas las organizaciones participantes, así como con sus compañeros dentro de la comunidad o sector en general	Los beneficiarios pueden compartir TLP: Información VERDE con sus compañeros y organizaciones asociadas dentro de su sector o de la comunidad, pero no a través de los canales de acceso público.
BLANCO	Las fuentes pueden utilizar TLP: BLANCO cuando la información lleva a un mínimo o ningún riesgo previsible de mal uso, de conformidad con las normas y procedimientos aplicables para la difusión pública.	Información TLP: BLANCO se puede distribuir sin restricciones, sujeto a los controles de autor.

Tabla 1: Protocolo Semáforo (TLP)

EcuCERT tiene un plan operativo anual que lo maneja junto con ARCOTEL; para cumplirlo ellos tratan de optimizarse cada 3 meses.

2.1.2. CSIRT-UTPL

El CSIRT-UTPL es el Equipo de Respuesta a Incidentes de Seguridad Informática de la Universidad Técnica Particular de Loja, se encarga de brindar atención, soporte y respuesta a incidentes de seguridad, enfocando también sus servicios en el área de investigación en temas que contribuyan a mejorar la seguridad de los sistemas de la UTPL.

El CSIRT-UTPL es uno de los CSIRT que trabaja en conjunto con el EcuCERT; los dos cuentan con páginas en la red las cuales son muy informativas ya que se puede encontrar información de qué son los ataques cibernéticos en general, también proporcionan información de cómo protegerse de algunos ataques o poder ser menos vulnerable; a más de que se puede reportar alguna denuncia si es que ha sido víctima de uno de estos ataques.

El CSIRT-UTPL ofrece servicios proactivos, reactivos, de gestión y calidad de la seguridad como [43]:

- Alertas y Advertencias
- Manejo de Incidentes
- Servicios de Detección de Intrusiones
- Definición de nuevas políticas de seguridad.
- Concientización
- Educación y Capacitación a los usuarios en el uso de políticas y reportes.

2.1.3. CSIRT CEDIA

El CSIRT (Computer Incident Response Team) es un Equipo de Respuesta a Incidentes de seguridad que es responsable de recibir, revisar y responder a informes y actividad sobre incidentes de seguridad. Sus servicios son generalmente prestados para un

área de cobertura definida que podría ser una entidad relacionada u organización de la cual dependen, una corporación, una organización de gobierno o educativa [44].

El CSIRT-CEDIA es el Equipo de Respuesta a Incidentes de Seguridad Informática del CEDIA (Consorcio Ecuatoriano para el Desarrollo de Internet Avanzado).

Su propósito es apoyar a los miembros de la comunidad del CEDIA (que actualmente son 37, entre los cuales se encuentra la Escuela Superior Politécnica del Litoral - ESPOL) a implementar medidas proactivas con el objetivo de reducir los riesgos de incidentes de seguridad informáticos.

En una entrevista realizada al ingeniero Ernesto Pérez responsable del área de seguridad del CEDIA el 26 de enero de 2016, se pudo conocer que el CSIRT CEDIA se encarga de procesar los eventos recibidos por parte de FEEDS que es un sistema de reportes a nivel mundial, el cual le informa cuando detecta vulnerabilidades en Ecuador; además eventos que reciben mediante denuncias en su página web. CSIRT CEDIA recibe aproximadamente 300 eventos al día, donde la mayoría son indicadores previos, es decir eventos de vulnerabilidad. Actualmente cuentan con 3 honeypots (tecnología que será definida más adelante) en su red para detectar intentos de ataques, tienen previsto desplegar más honeypots para dar una mejor seguridad a las instituciones miembros, además quieren implementar una red de sensores en conjunto con la Red Nacional de Investigación de Brasil para detectar eventos maliciosos que puedan estar ocurriendo. CSIRT CEDIA utiliza softwares libres, YARI, que lo utilizan para llevar un control estadístico de los eventos; OTRS, es un sistema de tickets para marcar los eventos y NESSUS, que es un escáner de vulnerabilidad, el cual lo utilizan como software preventivo y lo

corren una o dos veces al año en las instituciones miembros para analizar sus vulnerabilidades.

El tiempo que transcurre desde que CSIRT CEDIA recibe el evento hasta que hace el aviso al afectado es de 8 horas máximo, en la mayoría de los casos es automático, es decir entre 15 y 30 minutos. CSIRT CEDIA calcula que en resolver un evento tarda entre 24 horas y 3 semanas; la mayoría de los eventos son resueltos en 2 días.

El CSIRT CEDIA cuando recibe el evento le coloca un ticket con un código para poder darle seguimiento al evento; si el evento no es a una de las instituciones miembros de CEDIA lo envían al ECUCERT y al ISP a cargo de la red que está siendo afectada, en cambio si la institución afectada sí es miembro de CEDIA el CSIRT en primer lugar le da una prioridad (baja, media o alta) dependiendo de la gravedad del evento, luego envía un aviso a la institución para que ésta lo pueda corregir, y le da un seguimiento hasta resolver el evento.

2.1.4. Comando de Operaciones Cibernéticas en el Ecuador

El Comando de Operaciones Cibernéticas es una institución anunciada por primera vez en septiembre del 2014 por las Fuerzas Armadas del Ecuador, el cual dio aviso de su puesta en marcha para el 2015. El Comando de Operaciones Cibernéticas está a cargo del Ministerio Nacional de Defensa, ya que éste considera al espacio cibernético como “vital” para la seguridad del Estado y sus ciudadanos; para su puesta en marcha el Estado asignó como primera inversión 8 millones de dólares.

Gracias al trabajo investigativo que se debe de hacer para poder culminar con éxito cualquier proyecto, en este caso, proyecto de fin de carrera, nos tomamos con seriedad la tarea de buscar

información, y fuimos a la Segunda División del Ejército ubicada en pleno centro de la ciudad de Guayaquil, expusimos nuestra tarea e inquietudes y muy cordialmente nos atendieron y re direccionaron hacia la Base Naval Sur ubicada en Guasmo Oeste al sur de la ciudad, para que nos dirijamos al Centro de Comunicación Social de Guayaquil, cuya jefatura la ejerce la Capitán de corbeta Rosa Morales Quinatoa, quien nos relató que la persona más idónea para que nos ofreciera una entrevista con las especificaciones y detalles que necesitábamos era el Contralmirante de la Armada del Ecuador Remigio Haro Muñoz, actual Director de Logística de la Armada, el cual acudimos a visitar a su oficina al día siguiente, lamentablemente no se encontraba en la ciudad para la entrevista, así que su asistente nos confirmó que cuando él arribara a la ciudad y ella le hiciese llegar nuestra carta de petición formal de entrevista se nos iba a comunicar por medio de una llamada telefónica para la confirmación de disponibilidad para una cita a convenir; al día siguiente llamó y nos dijo que nuestra entrevista se debía de re direccionar por interno con la persona experta en el tema más adecuada con la que podríamos platicar. Han pasado más de 3 semanas desde la única y última comunicación por parte de la Srta. Asistente del Contralmirante de la Armada del Ecuador Remigio Haro Muñoz; puesta esta situación dedicamos estas líneas para comentar el porqué de la falta de información en este documento acerca de un organismo tan importante para la ciberseguridad en el Ecuador, como es el Centro de Operaciones Cibernéticas. A pesar de todo esto tenemos la firme convicción de que nuestra propuesta de Plan de Acción puede también ser aplicable a este centro, debido al carácter procedimental del mismo.

2.2. Plan de Acción para la Optimización en los Procesos de los Centros de Incidentes Informáticos en Ecuador

De lo analizado anteriormente se establece que existe una necesidad latente de mejorar las medidas que se toman tanto para detectar y procesar un fraude cibernético como para prevenirlo en Ecuador.

Analizando propuestas de planes de acción en los países con mejores prácticas aplicadas en seguridad cibernética, se ha planteado una propuesta que desarrollamos a continuación.

El Plan de Acción para la Optimización en los Procesos de los Centros de Incidentes Informáticos en Ecuador se compone de 5 etapas [45].

En la figura 2.1 se presenta el Plan de Acción desarrollado con sus 5 etapas.

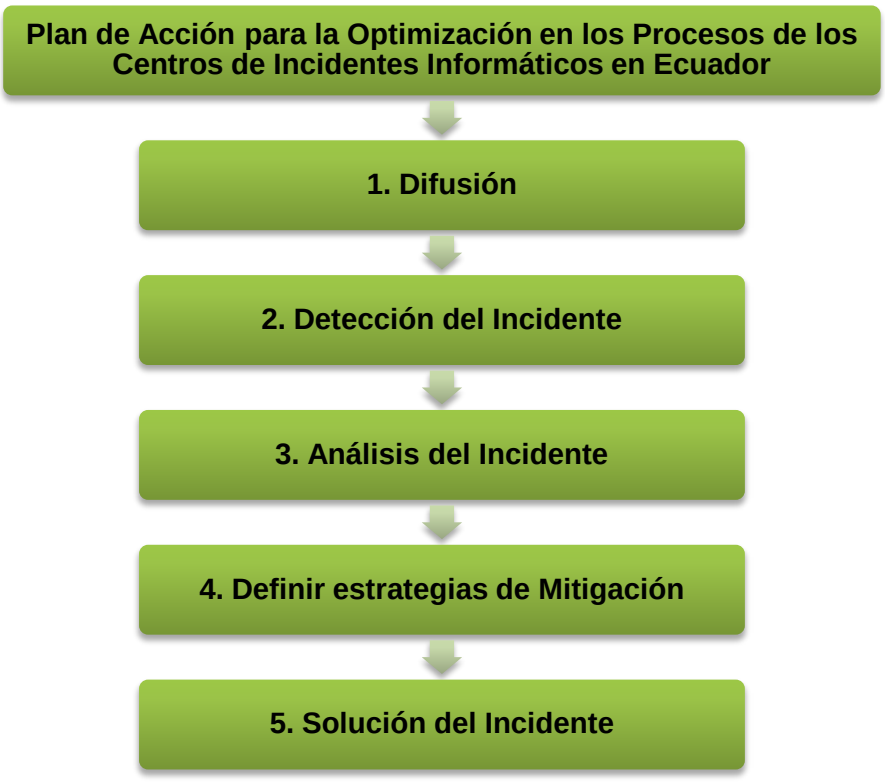


Figura 2.1: Esquema del Plan de Acción para la Optimización en los Procesos de los Centros de Incidentes Informáticos en Ecuador

1. *Difusión*

   Una declaración clara de políticas y procedimientos ayudará a la población objetivo a entender la mejor manera de reportar un incidente, y sobre todo qué apoyo deberá esperar después. Las expectativas claras de la población y las limitaciones de los centros de respuesta, ayudarán a lograr una interacción más efectiva con los afectados.

   Para lograr que los ciudadanos en general se informen de estas políticas y demás actividades que realizan los centros de respuesta a incidentes o eventos de seguridad informática se deben de tomar en cuenta el uso de actividades de difusión y promoción en conjunto con academias, instituciones educativas, municipios, etc., de manera que los usuarios en general conozcan sobre:

   - Las dudas más frecuentes de los usuarios, por lo general se formulan en las preguntas que se receptan de manera reiterada en los centros de respuesta; éstos deberían de publicar en su página web un Frequently Asked Questions (FAQ, por sus siglas en inglés) utilizando un lenguaje sencillo, para que cualquier persona que acceda a la página lo pueda entender.
   - Informar sobre qué es un ataque, los tipos de ataques más frecuentes, quienes son las personas más vulnerables a estos ataques.
   - Las vulnerabilidades que se detectan y los métodos fáciles de mitigación en los sistemas informáticos populares actualmente mediante el uso de redes sociales como Twitter, Facebook, Instagram, etc., actualizándolas periódicamente con la finalidad de que más personas se puedan proteger.
   - Las formas de prevención contra ataques, como disminuir las vulnerabilidades que tenemos al momento de conectarnos a la red, proteger nuestras cuentas, actualizar el software de nuestros dispositivos para hacer que este sea más seguro.

- Formas en las que se puede saber si la página a la que se ingresa es falsa, enseñar que no se debe acceder a cualquier enlace, y que se debe revisar que la dirección de la página sea válida, y cómo hacerlo.
- Los derechos que tiene el usuario de internet, como el derecho a la privacidad, seguridad de que los datos que proporciona no serán divulgados sin su consentimiento, además de que sigue teniendo los mismos derechos cuando está en la red que cuando no lo está.
- Las medidas que toman los centros de prevención y detección de incidentes para prevenir y solucionar los ataques cibernéticos.
- Las leyes que sancionan los incidentes, las cuales para nuestro país están mencionadas en el COIP.
- Las obligaciones que tienen los proveedores de internet de garantizar a los clientes y usuarios los derechos que les corresponden, la transparencia de la información, la confidencialidad de los mensajes transmitidos y de sus datos personales, etc.
- Las obligaciones que tienen los proveedores de internet de informar a sus clientes cuando son vulnerables, y pasar las alertas a las entidades competentes para poder mitigar la vulnerabilidad.

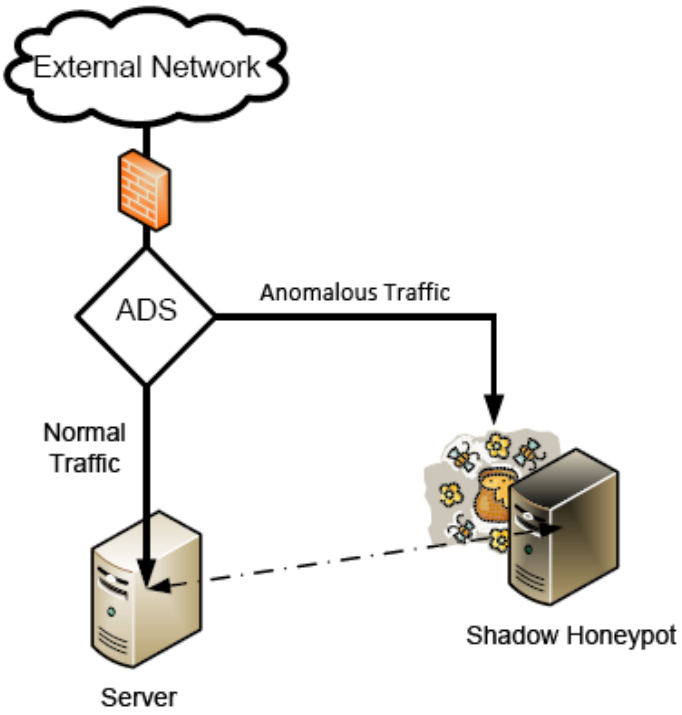
2. *Detección del Incidente*

   En Ecuador los incidentes no son detectados a tiempo, los organismos que controlan la tasa de incidentes tienen una manera de proceder pasiva al respecto, por lo cual se infiere que el número de incidentes a solucionar es mayor de lo que sería si se tomaran medidas de prevención.

   Algunos métodos de prevención de estos incidentes que se pueden implementar en nuestro país son:

   - Colocar sensores que detecten anomalías en la red, como honeypots, que es una trampa para detectar, desviar o

contrarrestar de alguna manera, los intentos de uso no autorizado de los sistemas de información; generalmente un honeypot puede ser una computadora, datos o un sitio de red que parecen ser parte de una red pero que en realidad están aislados, protegidos y monitorizados, y que parecen contener información o recursos que serían valiosos para los posibles atacantes. Un honeypot es una herramienta de seguridad informática utilizada para recoger información sobre los atacantes y sus técnicas [46]; y de esta manera monitorear la red constantemente para detectar posibles incidentes antes de que estos sucedan. En la figura 2.2 se muestra un sistema Honeypot.



Fuente: Raj Jain [47]

Figura 2.2: Segmentación del tráfico en un sistema Honeypot

- Hacer que cada proveedor de internet (ISP) tenga un departamento de detección de eventos o incidentes para poder prevenirlos o detectarlos a tiempo para que no se den, o si se dan no sean graves, ni tan perjudiciales para el cliente o usuario.
- Fomentar que los ISP realicen un monitoreo periódico de sus redes para que de esta manera puedan detectar vulnerabilidades que puedan tener sus clientes para poder avisarles y que estas puedan ser solucionadas antes de que algún ciberdelincuente las detecte y pueda atacar al usuario.
- Los centros de respuesta a incidentes deberían desplegar redes de sensores que les permitan detectar con mayor eficiencia y rapidez cualquier anomalía que se pueda dar en las redes del país, y de esta manera evitar que se dé un incidente.

3. *Análisis del Incidente*

Cualquier incidente que se suscite en el Ecuador y sea manifestado a un organismo competente a darle solución, deberá primero pasar por una serie de procedimientos antes de darle la solución adecuada; este procedimiento se puede ver detallado en la figura 2.3:

Figura 2. 3: Actividades del Análisis del Incidente

a. *Marcar y comprobar el incidente*

Primero se debe marcar el incidente, es decir darle un ticket o un código para poder nombrar este incidente, y diferenciarlo de los demás; esto también ayuda a poder llevar un seguimiento del

incidente tanto internamente como la persona o entidad que realizó la denuncia, o que es afectada por este.

Se deberá además comprobar la validez de un incidente informático que llegue a la base de datos de cualquier centro de respuesta que deba darle solución, deberá establecerse primero si es o no un incidente y si ha ocurrido en realidad, además del alcance que tiene y el impacto que tendría si no llega a solucionarse.

b. *Selección y Clasificación del incidente*

Se interpreta el incidente con el propósito de identificar el alcance del incidente, la extensión del daño causado por el mismo y la naturaleza del incidente, de acuerdo con lo cual se le asigna prioridad alta, media o baja dependiendo el caso; además de verificar si tiene relación con antiguos incidentes o correlación con incidentes contemporáneos para determinar si existe una solución previa, para lograr esto se deben de realizar dos actividades esenciales si la prioridad amerita:

- Recolección de evidencia forense

  Consiste en la recolección, preservación, documentación y análisis de la evidencia de un sistema computacional comprometido para ayudar en la reconstrucción de acontecimientos que conducen al compromiso del sistema. Esta recopilación de información y evidencia debe de ser hecha de tal manera que los documentos sean admisibles como parte de evidencia ante una corte o juzgado. Para llevar a cabo esta complicada tarea es recomendable hacer una imagen de bit, o una copia del disco duro del sistema afectado, verificando los cambios del sistema como nuevos programas, imágenes, servicios y usuarios, comprobando en el proceso la existencia de puertas traseras abiertas y troyanos.

- Rastreo y seguimiento

  La identificación de los sistemas a los cuales un intruso ha tenido acceso debe involucrar rastreo para el reconocimiento de la puerta de entrada al sistema por parte del intruso, además de la identificación del o de los sistemas que utilizó para ganar el acceso, inclusive hasta llegar a la identidad del atacante; cabe recalcar que esto solo se llega a dar en Ecuador si la fiscalía solicita los servicios del centro de respuesta.

El nivel de soporte y rapidez de solución de un incidente está fuertemente ligado a la prioridad que se le establezca para su gestión, y ésta a su vez está relacionada con el tipo y la gravedad de afectación, la institución u organismo que es atacado, el tamaño de la comunidad de usuarios que es afectado, además de los propios recursos para gestión de incidentes con los que cuente el centro de respuesta. Para la asignación de recursos y de la prioridad se les dará preferencia a los incidentes que tengan los siguientes aspectos en orden decreciente:

- Amenazas a la seguridad física de los seres humanos.
- Ataques de raíz (roots) o a nivel de sistema a cualquier sistema de gestión de información o cualquier parte de la infraestructura de una red troncal.
- Ataques de raíz (roots) o a nivel de sistema de cualquier máquina de servicio público ya sea multiusuario o con propósito dedicado.
- Compromiso de cuentas de servicio confidencial restringido o instalaciones de software, en particular los que utilizan aplicaciones de sistemas de información de gestión (MIS, por sus siglas en inglés) que contienen datos confidenciales, o aquellas utilizadas para la administración del sistema.

- Ataques de denegación de servicio (DoS, por sus siglas en inglés) en cualquiera de los elementos de los tres ítems anteriores.
- Cualquiera de los ítems anteriores, originados en la población objetivo de cada centro de respuesta.
- Los ataques de gran escala de cualquier tipo, por ejemplo los ataques de sniffers (espías), los ataques de ingeniería social, los descifrados de contraseñas.
- Amenazas, hostigamientos y otros delitos involucrando cuentas de usuario individuales.
- Compromiso de cuentas de usuario individuales en sistemas multiusuario.
- Compromiso de los sistemas de escritorio.
- Falsificación y tergiversación y otras violaciones relacionadas con la seguridad de las normas y regulaciones locales, por ejemplo el correo electrónico falso.
- Denegación de servicio en cuentas de usuario individuales, por ejemplo el mailbombing o inundación de correo.

Los tipos de incidentes no mencionados anteriormente serán priorizados de acuerdo con su severidad y extensión.

Cada centro de respuesta comprende que existe una gran variación en el nivel de experiencia y conocimientos del administrador de sistema del ISP o de la institución académica o investigativa (depende de cada población objetivo); cada centro de respuesta se debe comprometer a presentar información y asistencia al nivel adecuado de cada persona, el centro de respuesta no puede capacitar a la persona pertinente en el poco tiempo que se dispone y tampoco puede hacer el mantenimiento del sistema en su nombre, lo que sí debe de hacer es mantener a su población objetivo informada de posibles vulnerabilidades en su sistema antes de que sean explotados por terceros.

c. *Coordinación del Incidente*

Para concluir con el análisis del incidente se debe:

- Determinar la causa inicial del incidente (vulnerabilidad explotada)
- Facilitar el contacto y brindar la información de evolución de la solución a otros sitios que pueden estar involucrados o verse afectados, además de la víctima, esto incluye a los sitios que proveen soporte IT (Information Technology) a la víctima.
- Facilitar el contacto entre el organismo o institución universitaria o investigativa afectada (depende de la población objetivo) y los funcionarios policiales apropiados si fuese necesario
- Enviar reportes a otros centros de respuesta, ya que la recomendación es que éstos trabajen en conjunto con la finalidad de que el incidente no se repita, una excelente recomendación es crear un foro de intercambio de experiencias y conocimientos a nivel nacional, para que el proceso sea más ameno gracias a la organización y al apoyo conjunto.
- Realizar anuncios a los usuarios, si es recomendable o aplicable.

4. Definir Estrategias de Mitigación

Estas estrategias de mitigación van a depender de las personas afectadas por el incidente, ya que si es un ISP o alguna empresa que cuente con un departamento que se encargue de la seguridad informática, el centro de respuesta solo tendría que informar sobre el incidente y darle seguimiento para verificar la solución del mismo, pero en cambio si el atacado no es ninguno de los anteriores se puede brindar además una guía como ayuda para que el atacado

logre mitigar el incidente; esta guía estaría conformada por tres pasos como se puede observar en la figura 2.4:

Figura 2.4: Guía para mitigar el incidente

a) Asistencia Técnica

Incluye el análisis de los sistemas comprometidos, y una guía (de ser necesaria) de cómo se puede mitigar o evitar el incidente si es que este aún no se ha completado.

b) Erradicación

Eliminación de la causa de un incidente de seguridad (la explotación de la vulnerabilidad) y sus efectos (por ejemplo, la posibilidad de acceso al sistema por parte de un intruso)

c) Recuperación

Ayudar a los perjudicados en la restauración de los sistemas y servicios que se han visto afectados, para la recuperación de su estado antes de que se produjese el incidente.

Con los incidentes que ya han sido mitigados se puede formar una base de datos, de manera que si el evento o incidente ya ha ocurrido antes tal cual o similar se pueda dar una solución de manera más rápida y eficiente utilizando como guía el incidente anterior.

5. *Solución del Incidente*

Para dar una solución eficiente al incidente y saber que se lo puede dar como concluido o cerrado se debe:

- Extraer la vulnerabilidad
- Asegurar el sistema de los efectos del incidente
- Evaluar si ciertas acciones son más favorables para la recolección de resultados en la proporción coste-riesgo, en particular aquellas medidas apuntadas a una eventual acusación o acción disciplinaria: recolección de evidencia después del hecho, observación de un incidente en progreso, establecimiento de trampas para intrusos, etc.
- Recolección de evidencia donde la persecución penal o acción disciplinaria universitaria se contemple.

Se debe tener en cuenta que no todos los incidentes llegan a tener una solución por diversos motivos, ya sea que al afectado no le interese dar solución, o que no sea algo muy grave por lo cual no le afecte y no le de importancia, etc. Por lo general los incidentes a los que no se logra dar una solución son de prioridad baja y por tanto no son tan graves.

El incidente se marca como cerrado positivo en el caso de que si se le haya dado una solución, y como cerrado negativo en el caso de que no se haya solucionado porque los afectados así lo quisieron.

En adición el centro de respuesta podrá recopilar estadísticas sobre su población objetivo, y notificará a la población cuando sea necesaria la asistencia en caso de incidentes conocidos.

Las 3 últimas etapas del Plan de Acción propuesto en el presente proyecto integrador (Análisis del Incidente, Definir Estrategias de

mitigación y Solución del Incidente) se las puede observar un poco resumido en un diagrama de flujo en la figura 2.5.

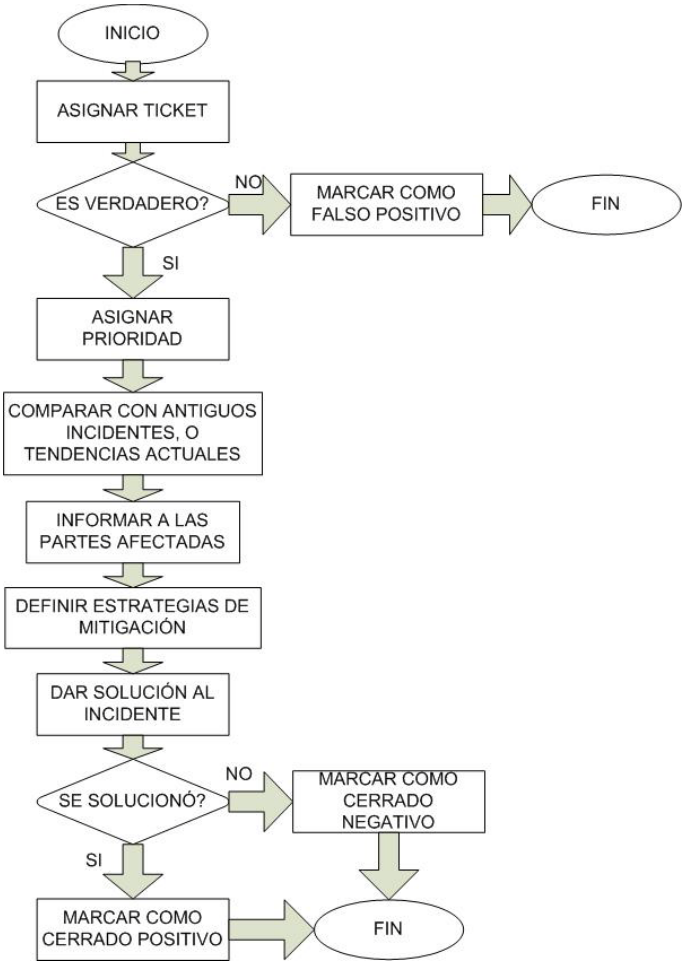


Figura 2.5: Diagrama de Flujo del Plan de Acción

CAPÍTULO 3

3. RESULTADOS Y BENEFICIOS DE LA IMPLEMENTACIÓN DEL PLAN DE ACCIÓN

3.1. Beneficios

Los beneficios que se obtienen al implementar el Plan de Acción para la Optimización en los Procesos de los Centros de Incidentes Informáticos en Ecuador detallado en el capítulo 2 son:

- El hecho de que se mejore la difusión dedicándole más tiempo o asignación de recursos, puede ayudar en gran medida a mitigar los ataques, puesto que las personas que pueden verse afectadas o víctimas tendrán información de primera mano acerca de qué son los ataques cibernéticos, los tipos de ataques cibernéticos más frecuentes y cómo evitar ser vulnerable ante éstos, además de poseer el conocimiento de que en Ecuador sí existen leyes que sancionan estos delitos de índole informático con lo cual la población se sentiría motivada a denunciarlos en caso de ser víctimas de ciberdelincuentes.
- Fomentar la sensibilización de los usuarios sobre la privacidad en línea y los medios de protección de la privacidad ayudará a la defensa de los usuarios frente a ataques de espionaje o estafa, tan comunes hoy en día alrededor del mundo.
- La detección temprana del incidente antes de que se llegue a dar el suceso reporta un gran beneficio ya que se evitará que el atacante llegue hasta el afectado, sin que llegue siquiera a reportarse como incidente, gracias a esto se podrán mitigar más los incidentes.
- El establecimiento de prioridades ayuda a agilizar la gestión de incidentes más relevantes en cuanto a daños o perjuicios ocasionados, ya que como se especifica en el anterior capítulo los más perjudiciales para las víctimas se les asigna prioridad máxima, que significa que se intentarán solucionar lo más rápido luego de que

sea detectado, de manera que la víctima sea lo menos afectada en lo posible.

- La confianza se vería aumentada dramáticamente en medida que la difusión de las medidas de seguridad implementadas por los organismos que protegen la integridad de los usuarios es reforzada.
- El afianzamiento de las transacciones en línea hechas por los usuarios, sobre todo aquellas que involucren entidades bancarias o tarjetas de crédito, realizando consumos ya sea nacional o internacionalmente.
- Al buscar colaboración para aunar esfuerzos tanto nacional e internacionalmente mediante una estrategia colaborativa se pueden ayudar a más víctimas en menor tiempo, además de la posibilidad de descubrir nuevos tipos de ataques, mejores maneras de resolver un incidente, información acerca de nueva tecnología tanto de hardware como de software para solucionar problemas informáticos es una ayuda indiscutible en todos los aspectos que involucran seguridad cibernética para el entorno nacional.
- Al tener una base de datos sobre los incidentes anteriores la mitigación de nuevos incidentes se puede hacer de manera más rápida y eficiente, y de este modo se puede evitar que el atacante cause mayores daños en el afectado.
- El Plan de Acción desarrollado en este proyecto complementará las buenas prácticas que tienen algunos centros para poder hacerlas más óptimas, además de que al aplicarlas en los centros que no las tengan lograrían que sus centros sean más eficientes al momento de controlar un incidente.
- Con el desarrollo de este proyecto se espera ganar un incremento en el comercio electrónico en nuestro país, además que la ciudadanía tenga una mayor confianza al sentirse seguros al momento de navegar en el ciberespacio; también se espera incrementar los servicios de Gobierno Digital, para que la ciudadanía pueda realizar sus trámites de una manera más rápida, eficaz y eficiente; reduciendo

los costos de estos trámites para el gobierno; de igual manera que exista una mayor transparencia por parte del sector público.

3.2. Resultados

En un mundo globalizado como en el que vivimos actualmente, se dice que cada individuo tiene una identidad en el ciberespacio, ya sea para entretenimiento (juegos online), interacción social (Facebook, Twitter, Instagram, Pinterest, Snapchat), para recibir información personal (Gmail, Hotmail, Yahoo), inclusive para conocer y establecer contactos de trabajo (LinkedIn). Conectarse a Internet ha pasado de ser un lujo a una necesidad con el paso de los años alrededor de todo el mundo; y esto no solo se da en el hogar, cada vez hay más compañías que permiten a sus colaboradores llevar sus propios dispositivos móviles (Smartphones o tablets) para conectarse a la red de la empresa, práctica conocida como Bring Your Own Device (BYOD), si un colaborador posee una vulnerabilidad en su dispositivo móvil y se conecta a la red de la empresa, deja una puerta abierta para que cualquier atacante acceda a su red corporativa, entonces las complicaciones abarcan mayores problemas, para evitar este y cualquier otro tipo de incidentes a nivel informático se deben de plantear políticas claras y difundidas correctamente a nivel nacional en el ámbito de seguridad cibernética. A continuación plantearemos los resultados detallados de implementar el Plan de Acción del capítulo anterior para prevenir, asegurar, detectar y responder ante un incidente informático, además de ciertas preocupaciones que las autoras de este documento tienen al momento de redactar el mismo.

Los centros de respuesta gracias a la difusión, pueden ayudar a establecer sólidamente una cultura de seguridad cibernética en su región o comunidad objetivo, deberá entenderse que esto es un proceso en el cual se deben de implicar a todas las partes expertas para poder influir en el pensamiento cultural, más que en el temor al ataque, en las

medidas a tomar para evitar ser blancos fáciles para los ciberdelincuentes; al mantener mayor informada a la comunidad objetivo, ojalá a la ciudadanía en general, sobre los riesgos que implica ser víctima de un incidente, se promoverá a la concientización de la inversión o actualización de software mejor preparados para asegurar su espacio cibernético. Además se va a lograr cumplir con el apartado B5 “Fomento en la Confianza y Seguridad en la Utilización de las TIC” de la Cumbre Mundial de la Sociedad de la Información; ya que de esta manera la población va a sentirse más confiada y segura al momento navegar en la red. Se sabe que para llegar a más personas se deben de utilizar medios de uso masivo, un buen ejemplo de estos medios son las redes sociales que difunden sus contenidos casi a tiempo real llegando a los hogares de millones de personas en todo el mundo; Facebook, Twitter, Youtube e Instagram son los más conocidos y difundidos; el 1 de abril del 2014, Matt Carpenter, responsable de operaciones de ventas de Twitter para Latinoamérica durante un desayuno organizado en Quito por IMS (Internet Media Services) indicó que Ecuador ya sobrepasó el millón de usuarios de esta red social; EcuCERT debe de saberlo y por eso tiene su cuenta en Twitter (@EcuCERT), sin embargo, hasta la fecha de finalización de este documento, su actividad en la red social no se actualiza desde el 15 de mayo del 2014 por motivos desconocidos.

Al implementarse un foro de preguntas y respuestas, y realizar un FAQ con la frecuencia que se crea conveniente en la página web del centro de respuesta se puede ayudar a usuarios a solucionar rápidamente sus problemas por sí mismos, sin necesidad de denunciarlo y esperar por instrucciones o respuestas del centro, ya que como la gestión de prioridad es selectiva, quizá las preguntas más comunes son las más sencillas de resolver, por lo tanto de mínima prioridad, pero a la vista del usuario una pérdida de valioso tiempo; además se va a lograr que la comunidad esté más informada observando casos o preguntas de otras personas y así puedan disminuir su vulnerabilidad protegiéndose, o no cometiendo errores que ya los hicieron otras personas.

Con una buena difusión se va a lograr cumplir con la línea de acción C5 “Creación de Confianza y Seguridad en la Utilización de las TIC” del Plan de Acción de la Cumbre Mundial sobre la Sociedad de la Información. Además también se cumple con uno de los 5 pilares “Medidas Técnicas y Procedimientos” de la Agenda sobre Ciberseguridad Global.

Un monitoreo constante que se ejecute por parte de los organismos encargados de la ciberseguridad en el país, debería disminuir los riesgos que tiene la población objetivo al acceder a internet, como el lamentable caso de la pornografía infantil, en todos los países, el medio de mayor distribución de este tipo de pornografía es la web, y el mejor medio de detección para este tipo de infractores son los honeypots.

En cuanto al modo de manejar la información notamos mucho hermetismo por parte del centro gubernamental en Ecuador, nos pareció que no existe la suficiente transparencia al momento de mostrar la información ya que no hay una buena divulgación de los métodos que utilizan y de la existencia de los mismos en general.

Actualmente tenemos la preocupación de si se está realizando una correcta prevención de estos incidentes por parte del EcuCERT, ya que no se ha encontrado la suficiente evidencia de esto; se conoce que ellos trabajan ya sobre los incidentes pero lo que se quiere en gran medida es detectarlos para evitar que estos ocurran.

Las entrevistas que se han tenido con los distintos centros no fueron muy productivas, en vista de que no se obtuvo la información necesaria para el correcto desarrollo del proyecto; exceptuando la teleconferencia con el Ing. Ernesto Pérez del CSIRT CEDIA, de la cual se obtuvo información oportuna, tal como que existe la preocupación latente de la desorganización a nivel general en la gestión frente a un incidente de mayor magnitud en Ecuador, de hecho esto se confirma gracias a una encuesta realizada por la OEA (Organización de Estados Americanos) para todos los países en su región publicada en abril del 2015 acerca de percepción de preparación para incidentes informáticos, Ecuador fue el

único país sudamericano que afirmó no sentirse preparado en lo absoluto para gestionar, atacar, prevenir, detectar o solucionar un incidente informático.

En la figura 3.1 se puede observar cuan preparados están los países de América ante un incidente cibernético.

Fuente: Reporte de Seguridad Cibernética e Infraestructura Crítica de las Américas [22]

Figura 3.1: Percepción de la Preparación para los Incidentes Cibernéticos

Un impedimento clave para enfrentar amenazas sería sin duda la falta de presupuesto que tiene el Estado para con los organismos gubernamentales, al estar el país en recesión se asignan menos recursos, por lo cual si bien no se minimizan los esfuerzos en estos organismos, se disminuiría la capacidad de adquisición de últimas tecnologías o actualizaciones de infraestructura crítica para la obtención de resultados, sin mencionar que el talento humano más capacitado es el más escaso, y por lo tanto el más costoso.

CONCLUSIONES Y RECOMENDACIONES

Conclusiones

Del trabajo realizado se desprenden las siguientes conclusiones:

1. De acuerdo a estudios de la OEA Ecuador no se siente preparado para gestionar en general un incidente informático.
2. Consideramos que los centros de respuestas a incidentes no tienen un buen sistema de detección para evitar los ciberataques.
3. El comercio electrónico se verá beneficiado en el Ecuador, ya que el usuario, al conocer que existen centros encargados de Ciberseguridad en el país, sentirá una mayor confianza al momento de realizar sus transacciones por medios informáticos
4. Consideramos que los centros de respuesta a incidentes informáticos en Ecuador tienen debilidades al momento de detectar y de dar solución temprana a los incidentes.
5. No existe una difusión adecuada por parte de los centros de respuestas a incidentes informáticos; gran parte de la ciudadanía inclusive desconoce la existencia de los mismos.
6. El incremento de los ataques cibernéticos cada vez es mayor en nuestro país, por lo que generar estrategias de detección y solución de los incidentes es necesario

Recomendaciones

Del trabajo realizado se desprenden las siguientes recomendaciones:

1. Sería conveniente que los centros de respuestas a incidentes informáticos en Ecuador adopten el plan de acción propuesto para mitigar los ataques cibernéticos que existen en nuestro país y obtener un mejor control de la Ciberseguridad.
2. Sería recomendable que los centros de respuestas a incidentes informáticos tengan una mayor difusión sobre los procesos que realizan.
3. Se debería asignar un mayor presupuesto a los organismos gubernamentales encargados de la Ciberseguridad en Ecuador.
4. Se recomienda renovar el plan de acción de cada uno de los centros de respuesta a incidentes informáticos por lo menos cada 5 años, ya que como los ataques se van actualizando y renovando las medidas de prevención y solución también deben hacerlo.
5. Sería beneficioso que en un proyecto futuro se diseñe un plan de prevención más detallado para poder evitar los incidentes informáticos.
6. Se sugiere que al cabo de aproximadamente 3 años de realizado este proyecto, se realice un nuevo análisis para el diseño de un plan de acción para la optimización en los procesos de los centros de respuestas a incidentes informáticos, ya que el avance tecnológico acarrea nuevos tipos de delitos informáticos.

BIBLIOGRAFÍA

[1] Convenio sobre Ciberdelincuencia, Budapest, Hungría, 2001

[2] Distr. General, “Lucha contra la utilización de la tecnología de la información con fines delictivos”, en Quincuagésimo sexto período de Sesiones de la Asamblea General de las Naciones Unidas, Nueva York, Estados Unidos, Dic. 2001.

[3] Distr. General, “Creación de una cultura mundial de seguridad cibernética”, en Quincuagésimo séptimo período de Sesiones de la Asamblea General de las Naciones Unidas, Nueva York, Estados Unidos, Ene. 2003.

[4] Y. Utsumi, “Cumbre Mundial de la Sociedad de la Información: Documentos Finales”, Unión Internacional de Telecomunicaciones, Ginebra, Suiza, Dic. 2005.

[5] Australian Communications and Media Authority, (2015, Abril 16). Key Elements of the Spam Act [Online]. Disponible en: http://www.acma.gov.au/Industry/Marketers/Anti-Spam/Ensuring-you-dont-spam/key-elements-of-the-spam-act-ensuring-you-dont-spam-i-acma

[6] Federal Communications Commission, (2010, Sep. 09). CAN-SPAM: Correo Electrónico Comercial Indeseado [Online]. Disponible en: https://transition.fcc.gov/cgb/policy/canspamSpanish.html

[7] Distr. General, “Declaración del Milenio”, en Quincuagésimo quinto período de Sesiones de la Asamblea General de las Naciones Unidas, Nueva York, Estados Unidos, Sept. 2000.

[8] Distr. General, “Cumbre Mundial sobre la Sociedad de la Información”, en Quincuagésimo sexto período de Sesiones de la Asamblea General de las Naciones Unidas, Nueva York, Estados Unidos, Ene. 2002.

[9] Unión Internacional de Telecomunicaciones. (2006, Enero 17). INFORMACIÓN BÁSICA: ACERCA DE LA CMSI [Online]. Disponible en: http://www.itu.int/net/wsis/basic/about-es.html

[10] Unión Internacional de Telecomunicaciones (2004, May. 12). Declaración de Principios. Construir la Sociedad de la Información: un desafío global para el nuevo

milenio [Online]. Disponible en: http://www.itu.int/net/wsis/docs/geneva/official/dop-es.html

[11] Distr. general, “Creación de una cultura mundial de seguridad cibernética y protección de las infraestructuras de información esenciales”, en Quincuagésimo octavo período de Sesiones de la Asamblea General de las Naciones Unidas, Nueva York, Estados Unidos, Ene. 2004.

[12] Unión Internacional de Telecomunicaciones (2006, Jun. 28). Compromiso de Túnez [Online]. Disponible en: https://www.itu.int/net/wsis/docs2/tunis/off/7-es.html

[13] C. Aguerre,. "Perspectivas de gobernanza en Internet," Dixit, no. 5, pp. 08-09, Dic. 2007.

[14] F. Villao, “LA GOBERNANZA DE INTERNET,” FIECriteria, vol. 1, no. 1, Noviembre, 2014.

[15] S. Schjølberg, “ITU Global Cybersecurity Agenda (GCA) High-Level Experts Group (HLEG)”, Moss, Norway, 2008

[16] La Agenda sobre Ciberseguridad Global [Online]. Disponible en: http://www.itu.int/itunews/manager/display.asp?lang=es&year=2008&issue=09&ipage=18&ext=html; Visto el 26 de Noviembre de 2015

[17] Impacto sobre la Ciberseguridad Mundial [Online]. Disponible en: https://www.itu.int/net/itunews/issues/2009/08/22-es.aspx; Visto el 3 de Diciembre de 2015

[18] Organización para la Cooperación y Desarrollo Económico, “The Seoul Declaration for the Future of Internet Economy,” en Reunión Ministerial en el Futuro de la Economía de Internet, Seúl, Corea, 2008, pp. 07-08.

[19] Policía Europea (EUROPOL). (2015). Combating cybercrime in a digital age. [Online]. DIsponible en: https://www.europol.europa.eu/ec3

[20] Organización de los Estados Americanos (OEA). (2016). Seguridad Cibernética. [Online]. Disponible en: https://www.sites.oas.org/cyber/Es/Paginas/default.aspx

[21] Comité Interamericano Contra el Terrorismo (CICTE). (2016). Seguridad Cibernética. Disponible en: http://www.oas.org/es/sms/cicte/programas_cibernetica.asp

[22] Trend Micro Incorporated, "Reporte sobre Seguridad Cibernética e Infraestructura Crítica en las Américas," OEA., Irving, Texas, Abr. 2015.

[23] J. Navarro Isla, ”Aspectos Legales de las Tecnologías de la Información y el Comercio Electrónico”, CGMPS Consultores Especializados S.C., México, 2011

[24] Comisión Económica para América Latina y El Caribe. eLAC. [Online]. Disponible en: http://www.cepal.org/elac2015/.

[25] Representantes ministeriales de América Latina y El caribe, “Plan de Acción sobre la Sociedad de la Información de América Latina y El Caribe eLAC 2007,” en Conferencia Preparatoria Regional Ministerial de América y Latina y el Caribe para la Cumbre Mundial sobre la Sociedad de la Información, Río de janeiro, Brazil, 2005, pp. 01-03-04-05-07.

[26] Representantes ministeriales de América Latina y El caribe, “Compromiso de San Salvador,” en Segunda Conferencia Ministerial sobre la Sociedad de la Información de América y Latina y el Caribe, San Salvador, El Salvador, 2008, pp. 13.

[27] Representantes ministeriales de América Latina y el Caribe, “Plan de acción sobre la Sociedad de la Información y del Conocimiento de América Latina y El Caribe (eLAC2015),” en Tercera Conferencia Ministerial sobre la Sociedad de la Información de América Latina y el Caribe, Lima, Perú, 2010, pp. 07-08-11-12.

[28] A. Gordón (2014, Noviembre 17). Ataques Cibernéticos Crecen en Latinoamérica [Online]. Disponible en:

http://www.elcomercio.com/tendencias/ataquesciberneticos-virus-latinoamerica-informe-seguridad.html. Visto el 27 de Noviembre de 2015

[29] F. Villao, “EL CÓDIGO ORGÁNICO INTEGRAL PENAL (COIP) Y LOS DELITOS INFORMÁTICOS”, Guayaquil, Ecuador, 1 de Noviembre de 2015

[30] Superintendencia de Telecomunicaciones 2012, Revista Supertel No. 14

[31] See Levy, Hackers, 1984; Hacking Offences, Australian Institute of Criminology, 2005, available at: http://www.aic.gov.au/publications/htcb/htcb005.pdf.; Taylor, Hacktivism: In Search of lost ethics? in Wall, Crime and the Internet, 2001, page 61

[32] Sieber, Council of Europe Organised Crime Report 2004, page 65.

[33] UIT, "El Ciberdelito: Guía para los países en desarrollo", 2009.

[34] See Sieber, Council of Europe Organised Crime Report 2004, page 88 et seqq; Ealy, A New Evolution in Hack Attacks: A General Overview of Types, Methods, Tools, and Prevention, available at: http://www.212cafe.com/download/e-book/A.pdf

[35] Malenkovich, Serge. (2013, Abril 9). ¿Qué es un Keylogger? [Online]. Disponible en: https://blog.kaspersky.com.mx/que-es-un-keylogger-2/453/

[36] Farwell, James P.; Rafal Rohozinski; “Stuxnet and the Future of Cyber War”, *Survival*, vol. 53, número 1, 2011

[37] D. Ramírez, “Conflicto de leyes y censura en internet: el caso Yahoo!,” Comunicación y Sociedad, no. 8, pp. 155-178, Jul-Dic. 2007

[38] BBC mundo. (2015, Agosto 5). Por qué ahora recibimos la mitad de correo basura que hace 5 años [Online]. Disponible en:

http://www.bbc.com/mundo/noticias/2015/08/150803_tecnologia_por_que_disminuyo_spam_lv

[39] D. Cáceres. (2016, Enero 4). El primer virus ransomware del año 2016 alcanza un nuevo nivel de amenaza [Online]. Disponible en:

http://articulos.softonic.com/virus-ransomware-2016-secret-level

[40] J. Rubio. (2015, Septiembre 29). Vulnerabilidad en Whatsapp: falsificación de mensajes manipulando la base de datos [Online]. Disponible en:

http://peritoinformaticocolegiado.es/vulnerabilidad-en-whatsapp-falsificacion-de-mensajes-manipulando-la-base-de-datos/

[41] EcuCERT. (2015). EcuCERT Centro de Respuesta a Incidentes informáticos del Ecuador [Online]. Disponible en: https://www.ecucert.gob.ec/nosotros.html#ANCHOR_Box5

[42] US-CERT. (2016, Enero 25). Traffic Light Protocol (TLP) Matrix and Frequently Asked Questions [Online]. Disponible en: https://www.us-cert.gov/tlp

[43] CSIRT-UTPL. (2015). Servicios CSIRT [Online]. Disponible en: http://csirt.utpl.edu.ec/

[44] redcedia. (2015). Quiénes Somos [Online]. Disponible en: https://csirt.cedia.org.ec/quienes-somos/

[45] Brownlee y Guttman . (1998, Junio). Expectations for Computer Security Incident Response [Online]. Disponible en: https://www.ietf.org/rfc/rfc2350.txt

[46] L. Alegsa. (2010, Mayo 12). Definición de honeypot [Online]. Disponible en: http://www.alegsa.com.ar/Dic/honeypot.php

[47] R. Jain. (2008, Abril 15). A Practical Guide to Honeypots [Online]. Disponible en: http://www.cse.wustl.edu/~jain/cse571-09/ftp/honey/

ANEXOS

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

LISTA DE ABREVIATURAS

ARCOTEL	Agencia de Regulación y Control de las Telecomunicaciones
CAN-SPAM	Controlling the Assault of Non-Solicited Pornography And Marketing
CCP I	Comité Consultivo Permanente I
CERT	Computer Emergency Response Team
CICTE	Comité Interamericano Contra el Terrorismo
CITEL	Comisión Interamericana de Telecomunicaciones
CMSI	Cumbre Mundial sobre la Sociedad de la Información
COIP	Código Orgánico Integral Penal
COP	Children's Online Protection
CEDIA	Consorcio Ecuatoriano para el Desarrollo de Internet Avanzado
CSIRT	Computer Security Incident Response Team
DoS	Denial of Service
EC3	The European Cybercrime Centre
ESCAPE	Electronically Secure Collaborative Application Platform for Experts
EUROPOL	Oficina Europea de Policía
FAQ	Frequently Asked Questions
FCC	Federal Communications Commission
FGI	Foro de Gobernanza de Internet
GCA	Global Cybersecurity Agenda
GEALC	Gobierno Electrónico de América Latina y el Caribe
GEANC	Grupo de Expertos de Alto Nivel sobre Ciberseguridad
ICANN	Internet Corporation for Assigned Names and Numbers
IMPACT	International Multilateral Partnership Against Cyber Threats

IP	Internet Protocol
ISIS	Islamic State of Iraq and Syria
ISP	Internet Service Provider
IT	Information Technology
LACNIC	Latin America & Caribbean Network Information Centre
LICRA	Ligue contre le Racisme et l'Antisémitisme
MAC	Media Access Control
MIPYME	Micro, Pequeña y Mediana Empresa
MoU	Memorandum de Entendimiento
NASA	National Aeronautics and Space Administration
NEWS	Network Early-Warning System
NSA	National Security Agency
OCDE	Organización de Cooperación y Desarrollo Económico
ODM	Objetivos de Desarrollo del Milenio
OEA	Organización de los Estados Americanos
TIC	Tecnologías de la Información y la Comunicación
TLP	Traffic Light Protocol
UE	Unión Europea
UIT	Unión Internacional de Telecomunicaciones
UTPL	Universidad Técnica Particular de Loja