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

Andrés Geovanny Romero Casañas
José Jonathan Ronquillo Panchana
Galo Fernando Tituana Vera
Ing. Alfonso Aranda
Facultad de Ingeniería en Electricidad y Computación (FIEC)
Escuela Superior Politécnica del Litoral (ESPOL)
Campus Gustavo Galindo, Km 30.5 vía Perimetral
Apartado 09-01-5863. Guayaquil-Ecuador
agromero@espol.edu.ec
jronquil@espol.edu.ec
gtituana@espol.edu.ec
jaranda@espol.edu.ec

Resumen

Este proyecto tiene como finalidad el diseño y operación del primer Equipo de Respuestas a Emergencias Informáticas en Ecuador, para este propósito realizamos un estudio sobre lo que es un Equipo de Respuestas a Emergencias Informáticas o CERT por su nombre en inglés, se presentan conceptos, definiciones, orígenes y antecedentes para conocer sobre el trabajo que realizan y la historia de estas organizaciones que se encuentran situadas en varios países del mundo y la importancia que tiene su creación en Ecuador, describimos la estructura organizacional que se utilizará, investigamos sobre los requisitos necesarios para la creación de organizaciones en nuestra nación buscando aquellas que prestan servicios similares para estudiar sus estructuras organizacionales, detallamos la inversión necesaria para llevar a cabo el proyecto, describimos costos de la infraestructura y el equipo que será utilizado, un análisis financiero completo en el que se estiman los costos y financiamiento del proyecto realizado con la ayuda de tablas y herramientas para el análisis financiero, planificamos la estrategia para la continuidad de operaciones del proyecto, en base a un análisis FODA planteamos las estrategias como ferias y congresos que permitirán la difusión y continuidad del proyecto, mostramos además, detalles sobre la metodología utilizada para la prestación de servicios, políticas a seguir y gráficos de los pasos utilizados en la realización de los servicios principales como los análisis forenses y consultorías.

Palabras Claves: *seguridad, informática, CERT, Ecuador, análisis, integridad, disponibilidad, confidencialidad, tecnología, inversión, sistemas.*

Abstract

This project aims to design and operation of the first Computer Emergency Response Team in Ecuador, for this purpose we conducted a study on what is an Computer Emergency Response Team or CERT by English name, presents concepts, definitions, origins and backgrounds to learn about the work they do and the history of these organizations are located in several countries and the importance of his creation in Ecuador, described the organizational structure to be used, we investigated the requirements for the creation of organizations in our nation pursuing those that provide similar services to study their organizational structures to study their organizational structures, we detail the investment necessary to carry out the project, describe the costs of infrastructure and equipment used, a financial analysis which estimates the costs and financing of the project with the help of tables and tools for financial analysis, we show the continuity planning of operations of the project, based on a SWOT analysis propose strategies such as fairs and conferences that will allow the distribution and continuity, also show details on the methodology used for the provision of services, policies, and making charts of the steps used in the accomplishment of core services such as forensic analysis and consultancies.

Keywords*: security, computer, CERT, Ecuador, analysis, integrity, availability, confidentiality, technology, investment, systems.*

1. Introducción

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

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

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

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

2. Definición de CERT

CERT (Computer Emergency Response Team) es un Equipo de Respuestas a Emergencias Informáticas. Un CERT es un referente de seguridad informática, lleva a cabo tareas de investigación que tengan como finalidad mejorar la confiabilidad de los sistemas existentes, encontrando amenazas y vulnerabilidades que estos puedan tener, ya sean nuevas tecnologías o versiones de los mismos.

3. FIRST (Foro de Respuesta a Incidentes y Equipos de Seguridad)

FIRST es una organización que agrupa a todos los CERT del mundo, su sede se encuentra en los Estados Unidos, fue fundado en 1990.

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

4. Objetivo General

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

4.1. Objetivos Específicos

Entre los objetivos específicos de un CERT tenemos los siguientes:
Informar sobre vulnerabilidades de seguridad y amenazas.
Divulgar y poner a disposición de la comunidad información que permita prevenir resolver incidentes de seguridad.
Realizar investigaciones relacionadas con la seguridad informática.
Educar a la comunidad en general sobre temas de seguridad.
Manejar estadísticas.

5. Estudio organizacional

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

Figura 1. Logotipo de ECCERT

5.1. Misión

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

5.2. Visión

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

5.3. Talento humano

Se realiza un análisis de las personas necesarias para que el Ecuador Computer Emergency Response Team funcione de la mejor manera en su comienzo, personas que tendrán tareas asignadas y serán responsables de que se lleven a cabo eficientemente; el talento humano que formará parte de la organización estará constituido por:

Tabla 1. Descripción del personal

Descripción del personal	Cantidad
Director General de Seguridad Informática	1
Director de Proyectos e Investigación de Seguridad Informática	1
Jefe del Departamento de Informática Y Respuesta ante Incidentes	1
Asistente Contable de la Dirección General	1
Equipo de Respuestas ante Incidentes	4

6. Descripción de servicios

ECCERT contará con una base de datos de los agentes interesados en los servicios que provee, logrando así una mejor comunicación entre ambas partes y logrando obtener el mayor beneficio posible a los servicios disponibles, entre los cuales destacamos: Análisis forenses, Escaneo de vulnerabilidades, Seguimiento de incidentes, Consultoría de seguridad y Capacitaciones

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

7. Portal Web

El Portal Web será la herramienta de comunicación entre la Organización y la comunidad interesada en conocer las nuevas y diferentes formas de ataques y vulnerabilidades presentadas en las diferentes aplicaciones, sistemas operativos y software en general. El usuario podrá registrarse y así poder acceder a varios servicios que ofrece el portal, como son las alertas generales, el foro de discusiones y una serie de encuestas que se realizarán a menudo para evaluar los conocimientos de la comunidad.

8. Inversión

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

Tabla 2. Inversión total

Inversiones fijas	Monto
Equipos de oficina	$ 9.710,00
Muebles de oficina	$ 3.935,00
Instalación de oficina	$ 1.500,00
Total de inversiones fijas	$ 15.145,00
Capital de trabajo	$ 4.849,00
Gastos de constitución	$ 910,00
Total	$ 20.904,00

9. Financiamiento

Como primera opción se tiene la factibilidad de realizar préstamos para proyectos de la Corporación Financiera Nacional, por la cantidad de $ 15,000.00 como lo muestra la tabla de la amortización, con una tasa del 10,5%(tasa mínima bancaria) y con 24 pagos mensuales de $ 695.64

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

Tabla 3. Amortización del Préstamo

Amortización del préstamo	
Monto	$ 15.000,00
Tasa de interés	10,50%
Pago	$ 695,64
Tiempo	24 meses

10. Continuidad del proyecto

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

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

10.1. Congresos

Los congresos de CERT son una iniciativa donde se presentan y discuten temas sobre seguridad informática, un área de alto interés para el desarrollo de la industria, organizaciones públicas y las empresas en un mundo globalizado altamente interconectado por la red de redes: Internet. CONGRESO CERT ofrece la oportunidad de conocer el estado de arte de la ciencia y la tecnología, como también para identificar los problemas y mostrar soluciones técnicas.

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

10.2. Ferias tecnológicas

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

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

11. Conclusiones

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

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

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

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

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

12. Agradecimientos

Agradecemos a todas las personas que ayudaron al desarrollo de este trabajo, a quienes nos aportaron conocimientos y entregaron información necesaria para culminar este trabajo, a todos ellos nuestro total agradecimiento.

13. Referencias

[1] CLCERT, Manual de Gestión de Incidentes de Seguridad Informática, www.proyectoamparo.net, Octubre del 2010

[2] Ec-Council , Computer Forensics - Investigation Procedures and Response, Cengage Learning, Diciembre del 2010

[3] Hossein Bidgoli, Handbook of information security Volume 3, California State University Bakersfield, Diciembre del 2010

[4] Chris Prosise - Kevin Mandia, Incident response and computer forensics, McGraw-Hill, Diciembre del 2010

[5] Carnegie Mellon University, Steps for Creating National CSIRTs, http://www.cert.org/cert/, Septiembre del 2010

[6] Forum for Incident Response and Security Teams, FIRST, http://www.first.org/, Septiembre del 2010
[7] Secretaría de la Función Pública de Argentina, Arcert, http://www.arcert.gov.ar/, Septiembre del 2010
[8] U. de Chile, Clcert, http://www.clcert.cl/, Septiembre del 2010
[9] Cámara de Comercio de Guayaquil, http://www.lacamara.org, Octubre del 2010
[10] Segu-Info, Seguridad de la información, http://www.segu-info.com.ar/, Septiembre del 2010
[11] Derechoecuador, Revista Judicial, http://www.derechoecuador.com, Noviembre del 2010.