DISEÑO Y DIMENSIONAMIENTO DE UN EQUIPO DE RESPUESTA ANTE INCIDENTES DE SEGURIDAD INFORMÁTICA (CSIRT). CASO DE ESTUDIO: ESCUELA POLITÉCNICA DEL EJÉRCITO.

Roberto Andrade[1], Walter Fuertes[2]

Dirección de Posgrado, Escuela Politécnica del Ejército, Sangolquí

robertoandrade533@hotmail.com, wmfuertesd@espe.edu.ec

Resumen

El presente artículo se enfoca en el diseño y dimensionamiento de un equipo de respuesta ante incidentes informáticos (CSIRT) para la Escuela Politécnica del Ejército. En este contexto se ha realizado una recopilación de información del estándar ISO/IEC 27035, la guía NIST SP 800-61, el modelo de gestión ITILv3 y las directrices del CERT/CC, relacionado con grupos de incidentes de seguridad informáticos para ser aplicados a la implementación del CSIRT académico. Para que el CSIRT apoye a los objetivos estratégicos de la ESPE se determinó los factores críticos de éxito (CSF) de la Institución y se analizó el esquema de seguridad informática existente en la ESPE comparados con los controles definidos en la norma ISO/IEC 27002; esta observación se efectuó realizando el análisis de riesgo conforme la guía NIST 800-30 y la herramienta de evaluación de seguridad CSET 4.0 del US-CERT. La factibilidad financiera se determinó en base al análisis de costo beneficio, considerando el presupuesto referencial para la implementación del CSIRT y el valor de la resolución de incidentes, aplicando el Proyecto de Modelación y Análisis de Costo de Incidentes - ICAMP-II. La validación de la eficiencia y operatividad de los procesos de manejo de incidentes de seguridad informática de la ESPE, se efectuó mediante simulaciones de varios escenarios utilizando la herramienta SIMPROCESS.

Palabras clave*:* CSIRT: grupo de respuesta ante incidentes informáticos, NIST: Instituto Nacional de Estándares y Tecnología, CERT/CC: equipo de respuesta a emergencias computacionales, ICAMP-II: proyecto de modelado y análisis de costo de incidentes.

Abstract

This article focuses on the design and dimensioning of Computer Security Incident Response Team (CSIRT) for the Escuela Politécnica del Ejército. In this context has made a compilation of information from the standard ISO/IEC 27035, the Guide NIST SP 800-61, the management model ITILv3 and the guidelines of the CERT/CC, related with groups of computer

security incidents to be applied to the implementation of the academic CSIRT. To ensure that the CSIRT supports the strategic objectives of the ESPE was determined the critical success factors (CSF) of the Institution and analyzed the existing computer security scheme at ESPE, which were compared with controls defined in ISO/IEC 27002 standard; this observation was performing with the risk analysis according to guide NIST 800-30 and CSET 4.0 US-CERT security assessment tool. The financial feasibility was determined in basis of cost-benefit analysis, considering the referential budget for implementation of the CSIRT and incident resolution value, applying the Incident Cost Analysis and Modeling Project - ICAMP-II. The validation of the efficiency and operability of the computer security incident management processes form ESPE, having structured processes and personnel associated with the CSIRT, was executed by simulations of various scenarios using the SIMPROCESS tool.

Key words: CSIRT: Computer Security Incidents Response Team, NIST: National Institute of Standards and Technology, CERT/CC: Computer Emergency Response Team/Coordination Center, ICAMP-II: incident cost analysis and modeling project

1. Introducción

El crecimiento en la penetración de Internet en Ecuador al 31.4 % al año 2011, según los datos del INEC (2011)está relacionado con el desarrollo de los servicios electrónicos asociados con la actividad social, comercial, financiera, educativa, salud, entre otras de la sociedad, conforme lo indica el Foro Mundial Económico en su reporte Global de Tecnología de Información del 2012 (Foro Mundial Económico, 2012). Sin embargo ha existido también un aumento en las amenazas informáticas que tienen como finalidad robar información personal, realizar ataques de denegación de servicio, realizar fraudes con tarjetas de crédito o afectar a la imagen de una institución, como lo demuestran en sus reportes anuales de ataques informáticos varias organizaciones relacionadas con temas de seguridad como es el caso de SYMANTEC (2012)

Esto ha obligado a las organizaciones a realizar un análisis más profundo acerca de la seguridad de la información y comprender que la implementación de mecanismos de seguridad como firewalls, herramientas antivirus y anti-spam, es solo parte de una arquitectura de seguridad, que debe integrar políticas, estándares, normas, modelos de gestión de tecnología y operaciones de seguridad, para minimizar el impacto ante un ataque a la actividades de la organización (Gonzáles R. , 2005).

Las organizaciones han entendido que si los mecanismos de protección implementados fallan, es necesario contar con procesos estructurados y personal especializado que maneje los incidentes de seguridad de información y restablezca los sistemas en el menor tiempo posible (Georgia, 2003). De esta manera lo comprendió el Gobierno de Estados Unidos cuando en el año de 1998 un gusano de internet Morris afecto al 10% de las máquinas en Internet de esa época, incluyendo a las de la NASA y provocando pérdidas estimadas en los 96 millones de dólares (Rajnovic, 2011), que llevo a la creación del primer grupo de respuesta ante incidentes computacionales (CERT/CC).

El objetivo de establecer grupo de respuesta ante incidentes informáticos denominados CERT, CSIRT o CIRT, es contar con un punto único de contacto en las organizaciones para la recepción de notificaciones de seguridad, manejo de incidentes y análisis de vulnerabilidades en los recursos y servicios que soportan a la información (Haller, 2011). Muchos países a nivel mundial han considerado la implementación de estos grupos como punto de contacto a nivel nacional ante eventos de seguridad informática (Killcrece, 2004)

Varias universidades han cumplido un rol principal en la implementación de los CSIRT nacionales, es así el caso de la Universidad de Carnegie Mellon en la que se estableció el primer grupo de respuesta ante incidentes y las universidades Autónoma de México, de Chile, Nacional de Asunción de Paraguay que son parte de los CERT de sus respectivos países (Universidad Carnegie Mellon, 2004)

A nivel latinoamericano la implementación de CSIRT´s académicos ha tomado fuerza en los últimos años y existe al menos un grupo de respuesta a incidentes de este tipo en cada país de la región exceptuando actualmente a Bolivia y Perú (Ministerio de Comunicaciones-República de Colombia, 2008). En el caso particular de Ecuador la Universidad Técnica Particular de Loja – UTPL, cuenta con un CSIRT académico implementado en el 2008 como parte del proyecto AMPARO y del trabajo de tesis de REBECA PILCO “Creación de un equipo de respuesta para la Universidad Técnica Particular de Loja - UTPL” (Pilco, 2008) y la Red Nacional de Investigación y Educación del Ecuador –CEDIA implemento en el año 2012 un CSIRT con la finalidad de ser un punto de contacto de las universidades ecuatorianas.

La Escuela Politécnica del Ejército ha tenido en cuenta que no está exenta de riesgos que afecten a la seguridad de su información y la importancia de mantener la disponibilidad de los servicios tecnológicos para el cumplimiento en sus actividades diarias, por lo que se ha enfocado en el mejoramiento de los controles de seguridad informática como se presenta en el trabajo

propuesto por Patricio Moscoso y Ricardo Guangalango (2011), "Evaluación técnica de la seguridad informática del data center de la Politécnica del Ejército" y el manejo de requerimientos de tecnología por parte de la comunidad académica de la Institución que se presenta en el trabajo de Alejandra Cuadros y Gabriela Velásquez (2011), "Análisis, rediseño e implantación de los procesos basados en ITIL, para el área de gestión y soporte técnico de la Unidad de Tecnología de Información y Comunicación de la Escuela Politécnica del Ejército"

En función a la misión de la ESPE en la formación profesional, la investigación y la vinculación con la comunidad, la implementación de un CSIRT académico a más de la protección a la información y servicios de la Institución, aportará a la creación de nuevos grupos especializados en el país y al fomentó de una cultura de seguridad informática en la sociedad (West-Brown, 1998).

En este contexto este artículo se enfoca en el proceso de diseño y dimensionamiento del equipo ante respuesta de incidentes para la Escuela Politécnica del Ejército, aplicando las directrices definidas en la norma ISO/IEC 27035 (International Organization for Standardization, 2011), la NIST 800-61, ITIL v3 y publicaciones del CERT/CC para la implementación del CSIRT académico, considerando la realidad de las universidades públicas del país, específicamente la ESPE en base a sus recursos tecnológicos, humanos y financieros disponibles y a su misión institucional.

El artículo ha sido estructurado de la siguiente manera: En la sección 2 se describe la metodología empleada para el análisis de factibilidad técnica y financiera para la implementación del CSIRT, en la sección 3 se presentan los resultados obtenidos y un breve análisis de los mismos, en la sección 4 se evalúa el aporte de la investigación a trabajos relacionados y en la sección 5 se presentan las conclusiones y líneas de trabajo futuras en base a los resultados obtenidos.

2. Metodología

Esta sección ha sido dividida en las siguientes 4 partes: Marco teórico, diseño y dimensionamiento, evaluación de la factibilidad financiera y simulación de los procesos de gestión de incidentes del CSIRT de la ESPE.

2.1 Marco teórico

Para el análisis de factibilidad técnica y financiera de la implementación del CSIRT de la ESPE, se realizó la recopilación de los procesos de gestión de incidentes de tecnología definidos en el modelo de gestión ITILv3 (United Kingdom´s Cabinet Office, 2011), la norma ISO/IEC 27035

(International Organization for Standardization, 2011), la guía NIST SP 800-61 rev2 (National Institute of Standards and Technology, 2011), el manual de gestión de incidentes del proyecto AMPARO (LACNIC, 2010) y las publicaciones realizadas por el CERT/CC de la Universidad Carniege Mellon (2004), sobre la cual se sustentó el dimensionamiento de la infraestructura tecnológica y la estructura organizacional del CSIRT (Georgia, 2003).

En base a la información recopilada se observó que el proceso de implementación del CSIRT, se conforma de cinco etapas con objetivos y actividades específicas (ver Figura 1).

- Etapa 1. Alistamiento y definición de procedimientos.
- Etapa 2. Capacitación y entrenamiento.
- Etapa 3. Gestión de alertas e investigación.
- Etapa 4. Respuesta a incidentes y apoyo a la comunidad.
- Etapa 5. Operación, revisión y mejoramiento continuo.

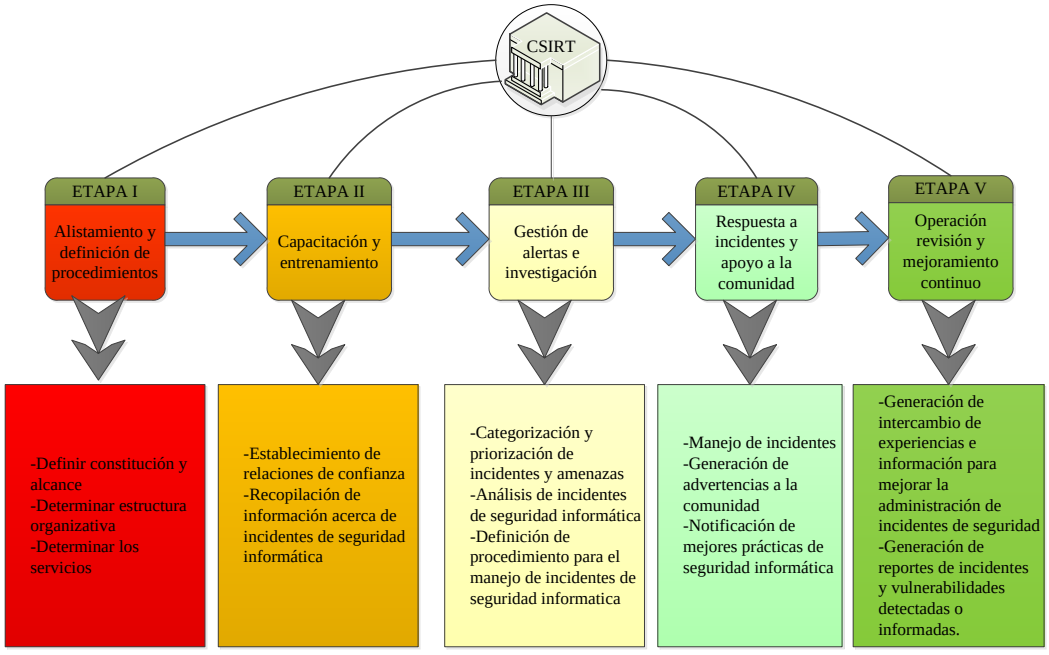

Figura 1. Etapas y actividades para la implementación de un CSIRT.

2.2 Diseño y dimensionamiento del CSIRT-ESPE

a. Evaluación de la estructura organizacional y controles de seguridad de la ESPE.

Para el diseño y dimensionamiento del CSIRT-ESPE se analizó la estructura organizacional de la Institución, a fin de determinar los factores de éxito crítico (Caralli, 2004), en función de los

cuales se establecieron la misión, visión y servicios del CSIRT (Killcrece, 2004); posteriormente se evaluó los controles de seguridad informática de la ESPE sobre los que se apoya el grupo de manejo de incidentes (ISO/IEC 27032, 2012).

La evaluación de seguridad se realizó mediante el análisis de riesgo conforme a la guía NIST SP 800-30 (2012) y el reporte generado por la herramienta de evaluación de seguridad CSET4.0 del US-CERT (2011), utilizando los datos obtenidos de los proyectos de tesis ("Evaluación técnica de la seguridad informática del data center de la Politécnica del Ejército" y "Análisis, rediseño e implantación de los procesos basados en ITIL, para el área de gestión y soporte técnico de la Unidad de Tecnología de Información y Comunicación de la Escuela Politécnica del Ejército"), de encuestas realizadas a personal de la UTIC, y de los procesos de contratación pública realizados por la Institución en los últimos 4 años.

Adicionalmente se realizó un análisis de la situación actual de los CSIRT académicos en Latinoamérica para contrastar con la propuesta planteada para la ESPE, a fin de verificar que la misma es factible de implementación basada en casos de éxitos en latinoamericana.

b. Procesos de gestión de incidentes de la CSIRT- ESPE.

El proceso de gestión de incidentes aplicado al CSIRT de la ESPE, se conforma de tres subprocesos (Alber, 2004): detección y análisis, manejo de incidente y cierre del incidente (ver Figura 2).

En la etapa de detección y análisis se recepta la información de incidentes vía email, requerimientos al *help desk*, o *logs* de los recursos tecnológicos; está información se registra en formularios en los que se detalla adicionalmente datos como: nombre del informante, correo electrónico, número telefónico, sistema o servicio afectado, fecha del incidente y si existen otros usuarios afectados. La información recopilada es analizada en un proceso denominado *triage*, en el cual se clasifica el incidente y se prioriza los recursos humanos y tecnológicos de acuerdo al nivel de impacto, para proceder a su resolución y posterior proceso de cierre del requerimiento recibido.

c. Evaluación de la factibilidad financiera CSIRT de la ESPE

Basándose en los datos obtenidos del diagnóstico de la estructura organizacional, tecnológica y de seguridad de la ESPE, se dimensionó los componentes y rubros relacionados con el hardware, software, personal y capacitación para la futura implementación del mismo en la Institución (Rajnovic, 2011). Posteriormente se procedió a la evaluación del costo beneficio de la

implementación del CSIRT, tomando como referencia el valor de la resolución de incidentes de seguridad informática propuesta en el proyecto de modelado y análisis de costo de incidentes ICAMP-II (USENIX, 2011), para el incidente de virus KIDO presentado en la ESPE en el año 2012 y el presupuesto referencial de implementación del CSIRT.

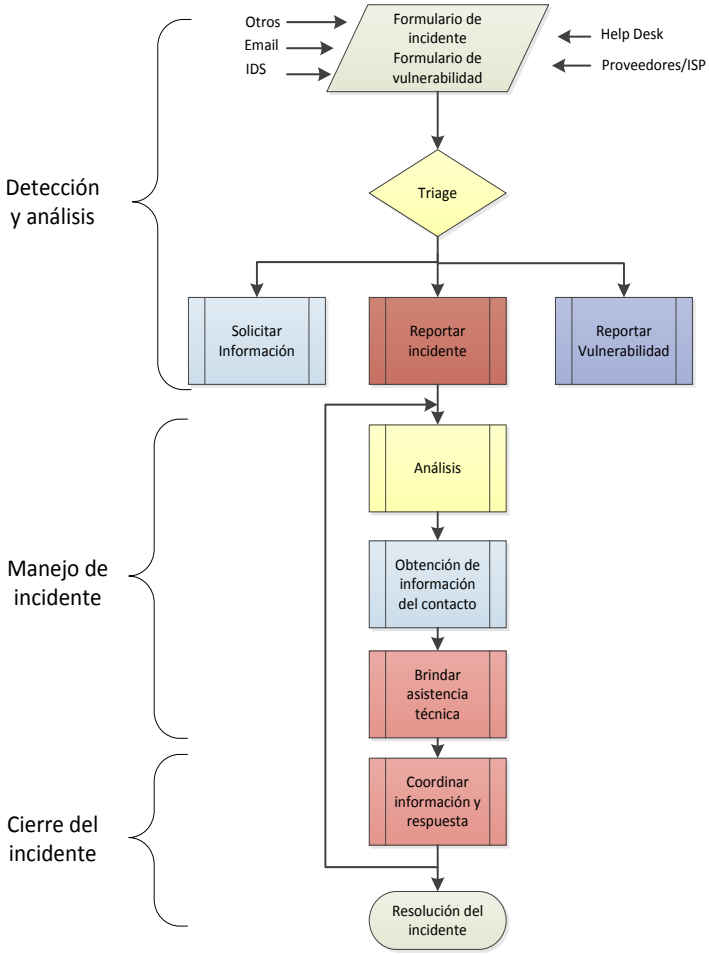

Figura 2. Proceso de manejo de incidentes de seguridad informática del CSIRT.

d. Simulación de los procesos de gestión de incidentes CSIRT-ESPE

Para evaluar las mejoras en los tiempos de resolución, la distribución de carga de requerimientos y el número de incidentes de informáticos de seguridad resueltos exitosamente, por parte del personal de la UTIC de la ESPE, al contar con procesos estructurados y capacitación en seguridad informática, se realizaron simulaciones de diferentes escenarios de manejo de incidentes de seguridad informática utilizando la herramienta SIMPROCESS (2012).

3. Evaluación de resultados y discusión

El análisis de factibilidad técnica y financiera permitió contribuir con la presentación de la propuesta para la implementación del CSIRT de la ESPE, evaluando componentes de hardware, software, personal y capacitación necesarios, así como su rubro asociado.

Considerando que la ESPE es una institución académica estatal sin fines de lucro que no está exenta de ataques de seguridad que afecten negativamente a la Institución; se realizó la evaluación del costo del código malicioso (KIDO), el cuál afecto a un total de 40 máquinas por un período de 4 días a la ESPE en el 2012. La estimación se realizó aplicando la propuesta del proyecto ICAMP-II, obteniéndose como resultado un valor de $16.742 con una desviación de $2.500. Del análisis del costo beneficio de contar con un CSIRT, se determinó que en caso de presentarse un ataque similar existirá una rentabilidad igual al valor del obtenido si el ataque fuera exitoso ($16.742), además de la contribución al fortalecimiento de una cultura de seguridad informática en la sociedad. Un factor a tomar en cuenta en el CSIRT académico es el recurso humano existente (estudiantes, profesores e investigadores) en la ejecución de investigaciones futuras relacionadas

Aunque del presupuesto referencial obtenido para la implementación puede ser alto para una institución académica (ver Tabla 1), este se compensa con el recurso humano disponible para investigación.

Tabla 1. Presupuesto referencial CSIRT de la ESPE.

Presupuesto Referencial	
Rubro	**Unidad**
Plataforma tecnológica	$22.385,00
Gastos operativos	$280.980,00
Equipos de oficina	$51.555,00
Arriendo servicios básicos	$5.400,00
Especialización	$16.600,00
TOTAL	**$376.920,00**

El CSIRT puede operar inicialmente utilizando la infraestructura tecnológica existente en la Institución y mediante el uso de herramientas de código abierto. El contar con procesos estructurados genera rentabilidad económica al no tener costos indirectos relacionados con el tiempo destinado por personal de la UTIC a resolver incidentes de seguridad informática.

En base al análisis de seguridad realizado con la herramienta CSET4.0 se determinó las mejoras a realizarse en los controles de seguridad existentes en la ESPE (ver Figura 3).

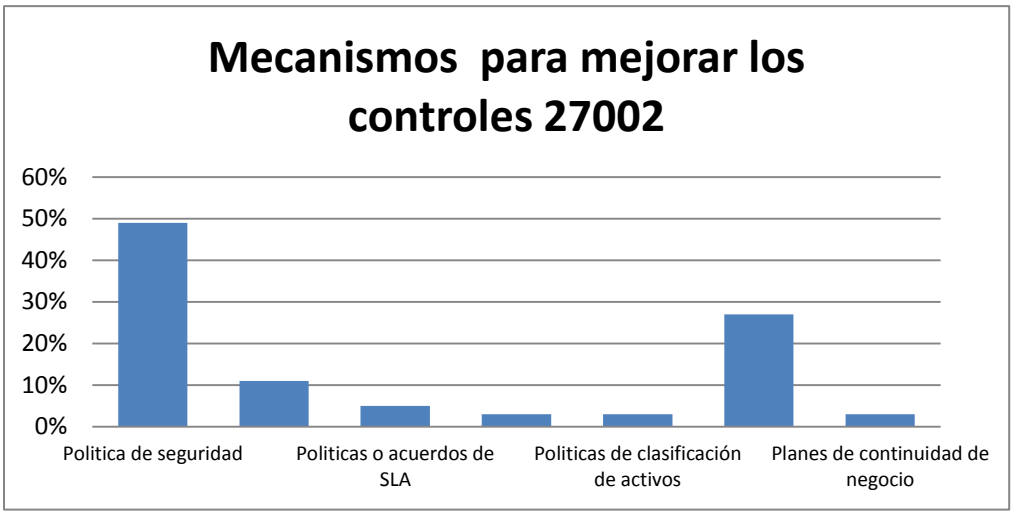

Figura 3. Mejoras a los controles de seguridad de la ESPE.

Evaluando la estructura organizacional de la ESPE se determinó los factores de éxito crítico de la Institución (ver Tabla 2), en base a lo cual se definió los servicios a ofertar por el CSIRT, así como su misión, visión, políticas, relaciones de confianza, priorización y métricas de evaluación (Dorofee & Kilcrece, 2007).

Tabla 2. Mejoras a los controles de seguridad de la ESPE.

Factores de éxito crítico	Servicios CSIRT
Gestión de cumplimientos de acuerdos	1.Manejo y resolución de incidentes 2.Configuración y mantenimiento de herramientas de seguridad, aplicaciones e Infraestructura 3.Auditorías de seguridad 4. Alertas
Planes de seguridad informática	1.Configuración y mantenimiento de herramientas de seguridad, aplicaciones e Infraestructura 2.Planeamiento de recuperación ante desastres y continuidad del negocio 3. Planeamiento de políticas de seguridad.
Programas de capacitación y entrenamiento	1.Entrenamiento y educación

a. Misión CSIRT de la ESPE

La misión determinada para el CSIRT de la ESPE en base al análisis organizacional de la Institución es la siguiente: “Brindar el servicio de manejo de incidentes informáticos a la comunidad académica de la ESPE, a través de auditorías y planes de seguridad informática, que permitan garantizar la disponibilidad de los servicios tecnológicos de la Institución”.

b. Visión CSIRT de la ESPE

La visión definida para el CSIRT de la ESPE en base al análisis organizacional de la Institución se definió como: "Consolidarse dentro de la Institución como un organismo de apoyo y asesoría para la comunidad académica para el mejoramiento de la seguridad informática en los diferentes recursos tecnológicos de la ESPE y fomentar la participación de la comunidad académica en temas relacionados con la seguridad de la información#.

c. Políticas del CSIRT de la ESPE

De acuerdo al análisis a los controles de seguridad de la norma ISO/IEC 27002 (International Organization for Standardization, 2007) evaluados para la ESPE, para el funcionamiento eficiente del CSIRT se debe implementar las siguientes políticas:

- Política de seguridad de la información
- Política de usuarios
- Política de transmisión de información
- Política de notificación de incidentes
- Política de tratamiento de incidentes

d. Establecimiento de relaciones de confianza para el CSIRT de la ESPE

El establecimiento de relaciones de confianza permite mejorar los procesos de manejo de incidentes, a través del intercambio de información entre grupos similares. A nivel local se estable acuerdos con:

- CSIRT-CEDIA
- CSIRT-SUPERINTENDENCIA DE TELECOMUNICACIONES
- CSIRT-FFAA

Mientras que a nivel internacional las relaciones de confianza se establecen con:

- FIRST
- OAS
- ITU-D
- IMPACT
- AP-CERT

e. Priorización manejo de incidentes

La priorización del manejo de incidentes de la ESPE se determina en base al análisis de riesgo realizado y los tiempos de resolución son establecidos en concordancia con el modelo de gestión ITIL v3 utilizado en la UTIC (véase Tablas 3 y 4).

Tabla 3. Priorización manejo de incidentes

Priorización manejo de incidentes	Impacto	
	Servicio	**Vector de amenaza**
ALTA	1.Sistema de Gestión Administrativa 2. Sistema Financiero 3. Sistemas de Gestión académica	1.Actividad de código malicioso 2.Vulnerabilidad de Parches
MEDIANA	1.Portal de servicios Institucionales 2.Correo electrónico Institucional	1.Actividad de reconocimiento 2.Deformación WEB 3.Spam
BAJA	1.Servicios de Internet 2.Repositorios de FTP 3.Telefonía	1. Denegación de servicio. 2.Uso no autorizado

Tabla 4. Tiempo de resolución de incidentes.

Ponderación del riesgo	Acción y período de ejecución	
	Tiempo de respuesta	**Respuesta post-incidente**
ALTO	1 hora	SI
MEDIANO	4 horas	No, al menos que sea requerido
BAJO	Siguiente día laboral	NO

f. Métricas para la evaluación del cumplimiento y desempeño del CSIRT.

La eficiencia de los procesos de manejo de incidentes de seguridad informática requiere de su monitoreo continuo por lo cual se establecieron métricas de evaluación (véase Tabla 5).

Tabla 5. Métricas de evaluación de los procesos de manejo de incidentes

Descripción	Métrica
Mantenimiento de la Calidad del Servicio	Número de incidentes de severidad Alta (total y por categoría) Número de incidentes severidad Mediana y Baja Número de otros incidentes Número de incidentes incorrectamente categorizados Número de incidentes incorrectamente escalado Número de incidentes que no pasaron por el *Help Desk* Número de incidentes que no fueron cerrados/resueltos sobre las horas Número de incidentes resueltos antes de que el usuario notifique Número de incidentes abiertos nuevamente.
Mantenimiento de satisfacción al cliente	Número de usuarios/clientes encuestas enviadas Número de encuestas respondidas Promedio de puntaje encuesta a usuario (total o por categoría de pregunta) Promedio de tiempo de espera antes de la respuesta al incidente
Resolución de incidentes en los tiempos establecidos	Número de incidentes registrados Número de incidentes resueltos por *Help Desk* Número de incidentes intensificados por *Help Desk* Tiempo promedio para restablecer el servicio desde la primera llamada Tiempo promedio para restaurar la severidad del incidente Tiempo promedio para restaurar la urgencia del incidente

g. Simulación de procesos de gestión de incidentes

Los resultados obtenidos al contar con procesos de gestión de incidentes de seguridad informáticos como parte del CSIRT de la ESPE, se determinaron en base a simulaciones realizadas con la herramienta SIMPROCESS (véase Figura 4).

En la simulación se consideraron varios parámetros como: ponderación de los incidentes, personal del CSIRT, tiempos de resolución entre otros. Los tiempos para la ejecución de los diferentes procesos del manejo de incidentes, se establecieron de acuerdo a recomendaciones definidas en el modelo de gestión ITILv3, y los niveles de escalamiento de acuerdo al proceso establecido actualmente en la UTIC (ver Tabla 6).

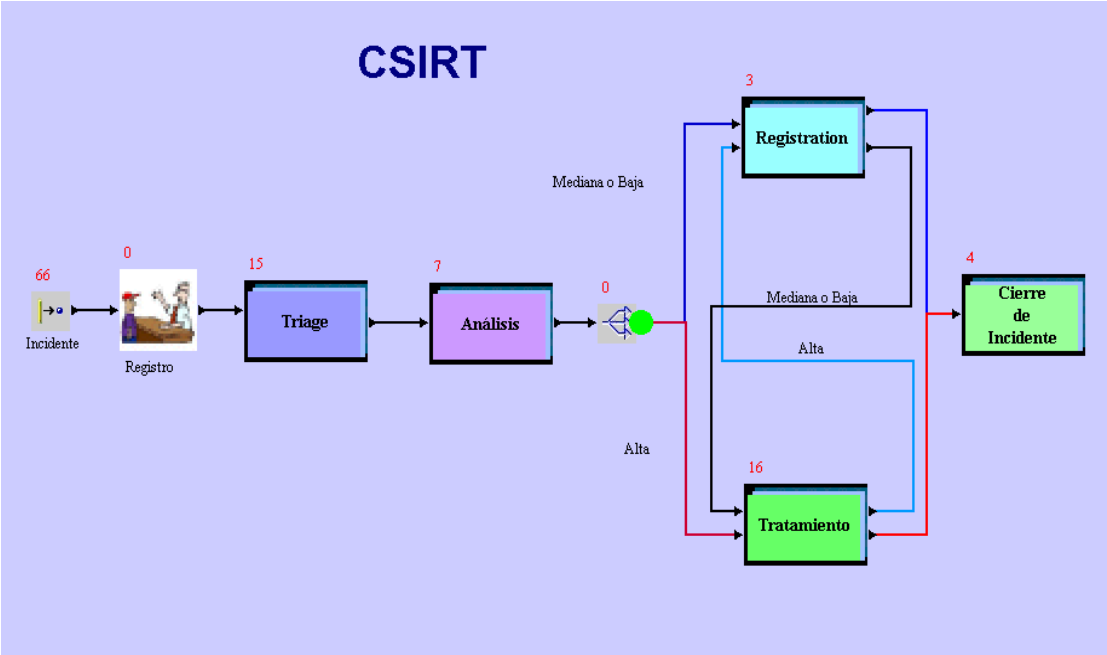

Figura 4. Proceso de manejo de incidentes simulado en SIMPROCESS.

Para las diferentes simulaciones se utilizó un valor promedio de 100 requerimientos diarios realizados al *Help Desk* de la ESPE, de acuerdo a los reportes obtenidos de la herramienta de administración de tickets *Service Desk*, utilizada por la UTIC para la gestión de incidencias informáticas y requerimientos de TI solicitados por la comunidad académica de la ESPE.

Tabla 6. Tiempos de resolución y niveles de escalamiento UTIC.

Niveles de soporte	Tiempo de resolución	Niveles de escalamiento	Nomenclatura
Soporte primer nivel	30 min	Help Desk	GT1
Soporte segundo nivel	60 min	Redes y comunicaciones	GT2
Soporte tercer nivel	4 horas	Sistemas de información	GT3
Proveedores	24 horas	Proveedores/CSIRT´s	GT4

La simulación se realizó analizando cuatro escenarios diferentes que se describen a continuación:

- **Escenario 1:** Proceso de manejo de incidentes en el que se cuenta con un experto en seguridad y documentación organizada bajo el modelo de gestión ITILv3. Los incidentes de seguridad informática son resueltos por el personal del CSIRT, *Help Desk* y soporte de segundo y tercer nivel de la UTIC.
- **Escenario 2:** Proceso de manejo de incidentes en el que no se cuenta con un experto en seguridad y documentación organizada bajo el modelo de gestión ITILv3. Los incidentes de seguridad informática son resueltos por el personal del *Help Desk* y soporte de segundo y tercer nivel de la UTIC.
- **Escenario 3:** Proceso de manejo de incidentes en el que no se cuenta con un experto en seguridad ni documentación organizada bajo el modelo de gestión ITILv3. Los incidentes de seguridad informática son resueltos por el personal del *Help Desk* y soporte de segundo y tercer nivel de la UTIC.
- **Escenario 4:** Proceso de manejo de incidentes en el que se cuenta con dos expertos en seguridad y documentación organizada bajo el modelo de gestión ITILv3. Los incidentes de seguridad informática son resueltos por el personal del CSIRT, *Help Desk* y soporte de segundo y tercer nivel de la UTIC.

Para la simulación se establecieron los siguientes parámetros en la herramienta SIMPROCESS.

Categoría de incidentes: Se definió tres entidades que hacen referencia a los niveles de ponderación de incidentes de seguridad informáticos: Alta, Mediana y Baja (ver Figura 5). Estos valores son iguales para los 4 escenarios de análisis.

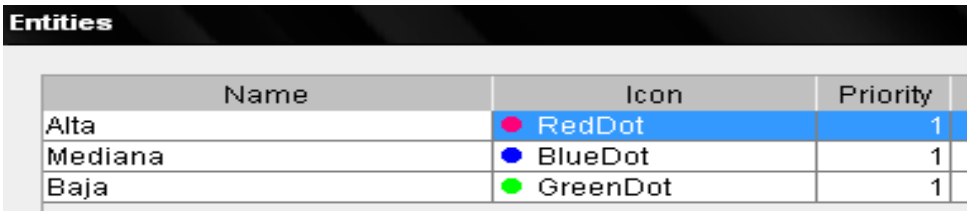

Figura 5. Ponderación de incidentes definidos en SIMPROCESS.

Recursos: Para el proceso de simulación se tomó en cuenta el número de personal de la UTIC en *Help Desk*, y en soporte de segundo (GT2) y tercer nivel (GT3) de la UTIC, que está asignado en el manejo de incidentes informáticos. Adicionalmente se consideró la contratación de un experto certificado en incidentes de seguridad (*Incident Handler*) para personal del CSIRT.

En la herramienta SIMPROCESS, las áreas de *Help Desk*, GT2 y GT3 definen en el campo ***resources,*** y la cantidad de personal para cada área se define en el campo ***Global Attribute Definitions*** (ver Figuras 6 y 7).

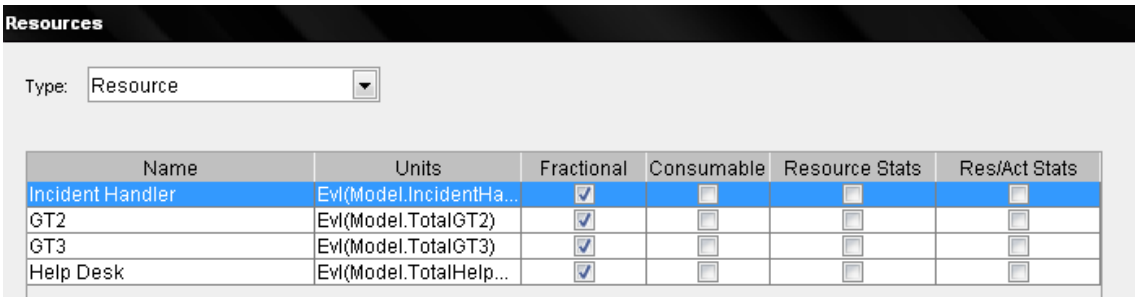

Figura 6. Definición de las áreas de TI en la herramienta SIMPROCESS.

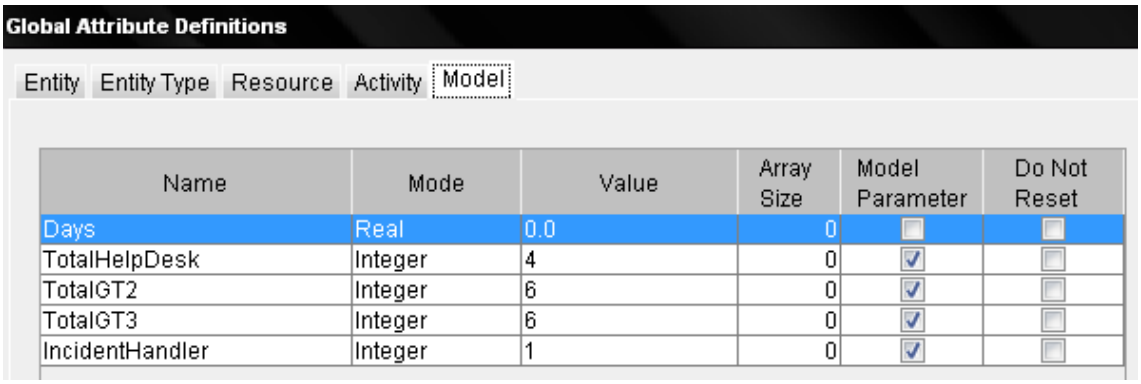

Figura 7. Definición del número de personal en cada área de la UTIC y del CSIRT.

Registro: Se consideró para la etapa de registro de incidentes, que la notificación pueden venir de diferentes fuentes hacia el personal del *Help Desk* y del CSIRT (*Incident Handler*). Se estima el tiempo de 1 minuto para que el personal notificado registre la incidencia.

Triage: Para este proceso se consideraron las siguientes variantes en los escenarios de análisis; primero se consideró que la evaluación del incidente (categorización y priorización) debe realizarse por parte de un experto certificado en seguridad con un tiempo estimado de 10 minutos. En el segundo y tercer escenario se considera que no se cuenta con un experto en seguridad certificado y la evaluación la realiza el personal de *Help Desk* con un tiempo de resolución de 30 minutos (ver Figura 8).

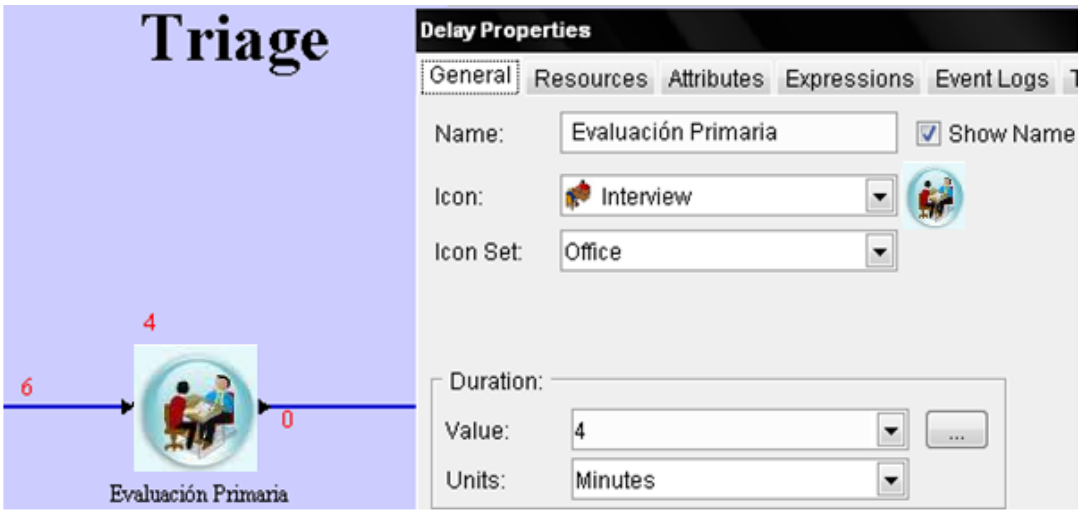

Figura 8. Definición del proceso de *Triage* en SIMPROCESS

Análisis: Para esta parte del proceso se consideraron para las simulaciones dos variantes de escenarios. En el primer escenario las incidencias categorizadas como altas son analizadas por personal del CSIRT, de *Help Desk* y de soporte de segundo y tercer nivel de la UTIC. Para el segundo escenario no se cuenta con personal de CSIRT y el proceso de análisis es efectúa por personal de *Help Desk* y de soporte de segundo y tercer nivel de la UTIC (ver Figura 9).

Obtención de registros (Registration): En esta etapa del proceso se simuló el contar con registros de incidentes ocurridos anteriormente. La simulación en esta etapa del proceso comprende dos variantes de escenarios. En el primero que se cuenta con documentación estructurada de incidencias anteriores o procedimientos de manejo de incidentes en un valor de 80%; Para el segundo escenario se consideró el caso contario con una existencia limitada documentación de un valor del 20%.

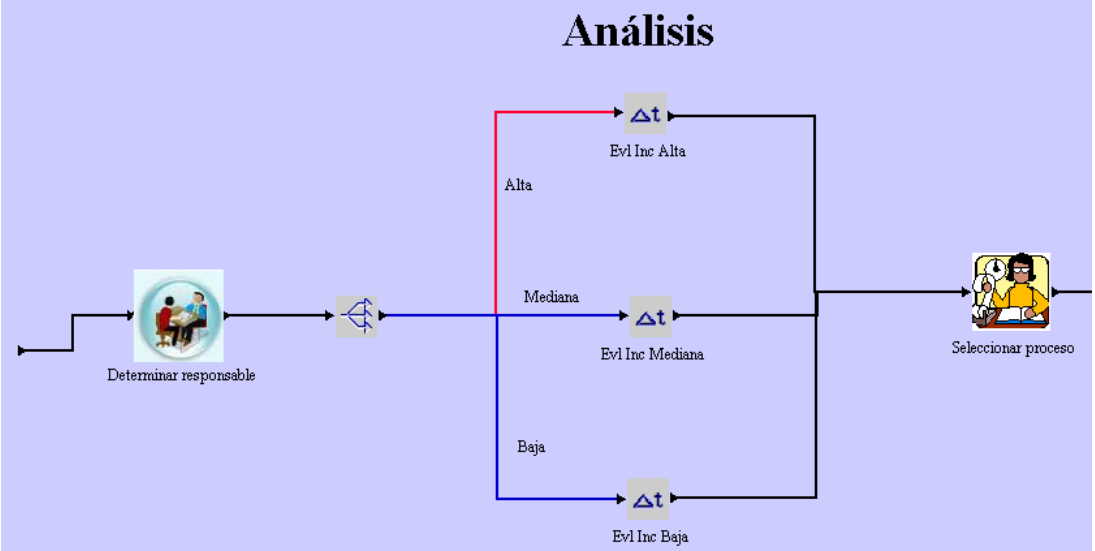

Figura 9. Definición de procesos de análisis de incidencias

Nota: *Evl Inc Alta incluye a personal del CSIRT, HELP DESK y Soporte de segundo y tercer nivel.*
Evl Inc Media incluye a personal del HELP DESK y Soporte de segundo y tercer nivel.
Evl Inc Baja incluye a personal del HELP DESK.

Las simulaciones realizadas permitieron determinar los siguientes resultados:

Número de incidencias resueltas: En los escenarios en los que no se contaba con personal experto en seguridad informática (*Incident Handler*), se presentó valores menores de incidencias resueltas; en el escenario 4, donde se consideró un experto de seguridad adicional el número de incidencias resueltas prácticamente se duplicó, especialmente en la categorizadas con ponderación Alta (ver Figura 10).

Porcentaje de ocupación del personal: En los escenarios en los que no se contaba con personal experto en seguridad informática (*Incident Handler*), se presentó mayor porcentaje de ocupación del personal del *Help Desk*, debido a que estos se encontraban recibiendo requerimientos y atendiendo incidencias. Adicionalmente el tiempo que el personal de *Help Desk* requiere para analizar una incidencia y ofrecer el tratamiento es mayor debido a que no cuenta con una especialización en seguridad informática.

En el escenario 3, donde no se contaba con documentación organizada se presentó un incremento en el grado de ocupación del personal de soporte de segundo nivel (GT2), debido a que a que se generó mayor escalamiento de incidencias por parte del *Help Desk*, al no tener procesos definidos para el manejo de incidentes.

En el escenario 4 se presentó un incremento en la ocupación del personal de las diferentes áreas, debido a que se resolvió un mayor número de incidencias en el mismo período de tiempo (ver Figura 11).

Costos: En los escenarios en los que se contaba con personal experto en seguridad informática (*Incident Handler*), se presentó un mayor costo del valor a pagar al personal por la resolución de incidentes, esto es debido a que el valor salario-hora del personal certificado es mayor. Si se analizan el número de incidencias de ponderación Alta resueltas y el costo de incidente que podría generarse debido al impacto de estas incidencias, se tiene una buena relación costo beneficio de contar con personal especializado.

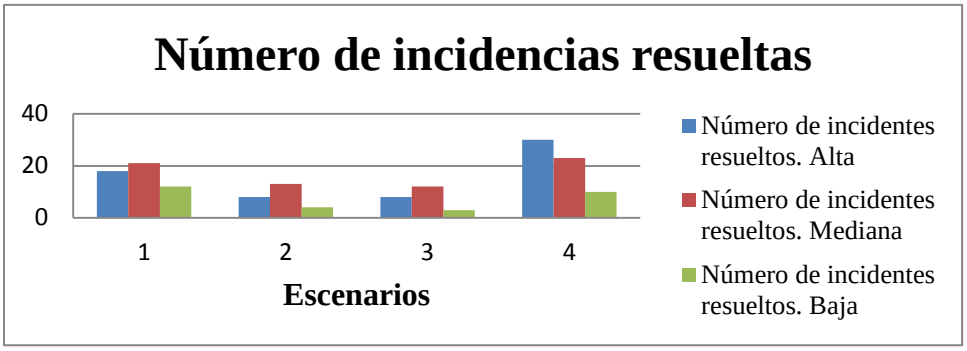

Figura 10. Simulación de número de incidencias resueltas.

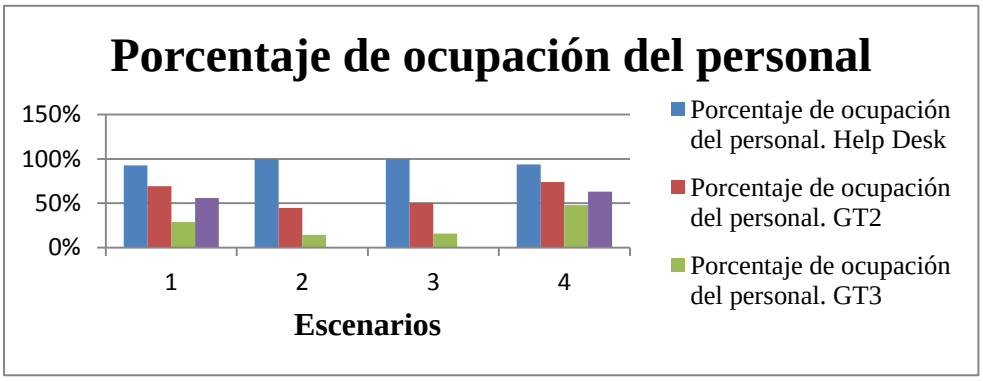

Figura 11. Simulación de porcentaje de ocupación del personal de la UTIC.

Un aporte adicional de las simulaciones realizadas, es la verificación de la importancia de contar con procesos de documentación de las incidencias presentadas y la capacitación del personal de tecnología en gestión de incidentes de seguridad, a fin de mejorar los tiempos de resolución y la reducción de escalamientos incorrectos a personal de mayor nivel de especialización.

5. Trabajos relacionados

Actualmente la implementación de CSIRT´s está enfocada a organizaciones con fines de lucro, en las cuáles se puede justificar la inversión financiera frente al costo de incidentes de seguridad informática, que afectan a la continuidad del negocio, la perdida de información o al deterioro de la imagen institucional. Por tal motivo existe limitada documentación sobre la implementación de CSIRT´s académicos, por lo cual esta tesis aporta a la evaluación de los mismos a nivel latinoamericano y aplicación de las etapas de implementación definidas en las publicaciones del CERT/CC, la guía NIST SP 800-61 y la norma ISO/27035 para el CSIRT académico. En este trabajo adicionalmente contribuye a establecer la justificación de la inversión económica en base a el análisis de costo beneficio, mediante la validación del modelo de costo de análisis de incidentes propuestos por el ICMAP-II, utilizando los valores de salarios aprobados por el Ministerio de Relaciones Laborales y el escalafón docentes fijado por Ley Orgánica de Educación Superior (LOES) del Ecuador, así como el costo de usuario calculado a partir del valor de la matrícula y duración del periodo académico de la ESPE para obtener una rentabilidad al implementar el CSIRT en una institución académica. Un aporte adicional de esta tesis al trabajo propuesto por el CERT UTPL es incluir en la propuesta de implementación, la utilización del estándar ISO/IEC 27035 la guía NIST 800-61, las directrices del CERT/CC y la validación de los procesos de manejo de incidentes mediante simulaciones con la herramienta SIMPROCESS.

6. Conclusiones y trabajo futuro.

Para el diseño y dimensionamiento de un CSIRT para la ESPE, se utilizó las directrices del estándar ISO/IEC 27035, la guía NIST SP 800-61, el modelo de gestión ITILv3 y el CERT/CC. La factibilidad financiera realizada en base al análisis de costo beneficio y la aplicación de la propuesta del proyecto ICAMP-II permite evidenciar una rentabilidad económica a la Institución, el aporte al fomento de investigaciones afines y el apoyo al mejoramiento de la cultura de seguridad informática de la sociedad. Mediante las simulaciones realizadas a los procesos de manejo de incidentes se validó la eficiencia y operatividad de los mimos, así como el incremento en el número de incidencias resueltas satisfactoriamente en menor tiempo.

Como trabajo futuro se prevé realizar la aplicabilidad del CSIRT en la ESPE, considerando que se ha elaborado en este trabajo las etapas I, II, III del proceso de implementación del CSIRT, que corresponden al diseño y dimensionamiento; y se han establecido los procedimientos que permiten ejecutar las etapas IV y V que se relación con la operatividad, revisión y mejoramiento del CSIRT.

6. Referencias bibliográficas

Alber, C. (2004). *Defining Incident Management Processes for CSIRTs:A work in progress.* Pensilvania: Universidad Carnegie Mellon.

CACI. (2012). *SIMPROCESS*. Recuperado el 27 de 10 de 2012, de http://simprocess.com

Caralli, R. (2004). *The Critical Sucess Factor Method: Establishing a Foundation for Enterprise Security Managment.* Hanscom, USA: Carniege Mellon.

Cisco Press. (2008). *End to End Network Security Defense-in-Depth.* Indianapolis: Cisco Press.

Cuadros, A., & Velásquez, G. (2011). *Análisis. Rediseño e Implementación de los procesos, basados en ITIL, para el área de gestión y soporte técnico de la Unidad de Tecnología de Información y Comunicaciones de la Escuela Politécnica del Ejército.* Sangolquí.

Dorofee , A., & Kilcrece, G. (2007). *Incident Managment Capability Metrics Version 1.0.* Hanscom: Software Engineering Institute.

Foro Mundial Económico. (2012). *Global IT Report 2012*. Recuperado el 20 de Julio de 2012, de http://www3.weforum.org/docs/Global_IT_Report_2012.pdf

Georgia, K. (2003). *Organizational Models for Computer Security Incident Response Teams (CSIRT´s).* Pensilvania: Universidad Carnegie Mellon.

Gonzáles, R. (2005). *Un modelo efectivo para la administración de incidentes de Seguridad de Información.*

Gonzáles, R. M. (2005). *Un modelo efectivo para la administración de incidentes de seguridad.*

Guangalango, R., & Moscoso, P. (2011). *Evaluación Técnica de la Seguridad Informática del DATA CENTER de la Escuela Politécnica del Ejército.* Sangolquí: ESPE.

Haller, J. (2011). *Best Practices for National Cyber Security.* Pensilvania: Carniege Mellon.

INEC. (2011). *Ecuador Estádistico Intituto Nacional de Estadísticas y Censos*. Recuperado el 20 de Julio de 2012, de http://www.inec.gob.ec/sitio_tics/internet.html

International Organization for Standardization. (2007). *ISO/IEC 27002 Security Techniques- Code of practice fpr information security managment.*

International Organization for Standardization. (2011). *ISO/IEC 27035:2011 Information Security Incident Managment.*

ISO/IEC 27032. (2012). *Information technology - Security techniques -Guidelines for cybersecurity.*

Killcrece, G. (2004). *Steps for creating National CSRT.* Pensilvania.

LACNIC. (2010). *Manual de Gestión de Seguridad Informática.* www.proyectoamparo.net.

Ministerio de Comunicaciones-República de Colombia. (2008). *Diseño de un CSIRT de Colombia.* Bogotá.

National Institute of Standards and Technology. (2011). *Computer Security Incident Handling.*

NIST SP 800-30. (2012). *Risk Managment Guide for Information Technology Systems.*

Pilco, R. (2008). *Creación de un Equipo de Respuesta a Incidentes de Seguridad Para la Universidad Técnica Particular de Loja.* Loja.

Rajnovic, D. (2011). *Computer Incident Response and Product Security.* Cisco Press.

Symantec. (2012). *Internet Security Threat Report*. Recuperado el 20 de septiembre de 2012, de http://www.symantec.com/threatreport/

TB-Security. (2008). Equipos de respuesta ante incidentes. *Equipos de respuesta ante incidentes*, (pág. 19). Montevideo.

United Kingdom´s Cabinet Office. (2011). *Information Technology Infraestructure Library.*

Universidad Carnegie Mellon. (2004). *Steps for creating National CSIRT* . Pensilvania.

US-CERT. (2011). *http://www.us-cert.gov.* Recuperado el 26 de 08 de 2012, de http://www.us-cert.gov/control_systems/csetdownload.html#i

USENIX. (2011). *Incident Cost Analysis and Modeling Project.*

West-Brown, M. (1998). *Handbook for Computer Security Incidente Response Team* . Pensilvania: Universidad Carneige Mellon.