



**Proyecto AMPARO
INFORME DE AVANCE**

Identificación del Proyecto

Título:	Creación e Implementación de un CSIRT Académico para la Universidad Técnica Particular de Loja		No.	A000
Organización Proponente	Universidad Técnica Particular de Loja			
Jefe de Proyecto	Msc. María Paula Espinoza			
Período Informado	Septiembre-Enero/ 2011	Sitio Web	www.utpl.edu.ec/csirt-utpl	
Dirección del Proyecto	Msc. María Paula Espinoza			
Investigadores participantes	Rebeca Pilco Vivanco			
	Julia Pineda Arévalo			

Contenido

Contenido	1
1. Actividades Realizadas (Resumen de los avances)	2
2. Objetivo General.....	3
3. Objetivos Específicos.....	3
• Actividades del período Agosto/2010 – Diciembre/2010:.....	4
4. Indicadores de Avance: Verificación de Resultados	6
5. Participación efectiva de todos los intervinientes en el proyecto.....	10
6. Reuniones de Coordinación	10
7. Actividades de Difusión.....	10
8. Referencias	11
9. Anexos	12

1. Actividades Realizadas (Resumen de los avances)

El proyecto de Creación e Implementación de un CSIRT Académico para la Universidad Técnica Particular de Loja, tiene como objetivo fundamental, el construir y proponer una normativa de seguridad aplicable al entorno local, la implementación del equipo permitirá compartir la experiencia y resultados obtenidos con otras universidades a través de organismos como CEDIA¹ con el objetivo de proponer la creación de una red nacional de CSIRTs académicos y contribuir así a la investigación y desarrollo de metodologías y buenas prácticas que permitan mejorar la seguridad de las redes ecuatorianas.

La implementación del CSIRT-UTPL permitirá también:

- Contar con un equipo capacitado para la atención de incidentes brindando servicios proactivos, reactivos y de aseguramiento de la calidad en temas de seguridad de la información.
- Concientizar a la comunidad universitaria y usuarios finales sobre los riesgos y beneficios del uso de internet, pero, sobre todo de la importancia de tomar en cuenta las medidas de seguridad adoptadas en la Universidad.

Por otra parte como objetivo fundamental el construir y proponer una normativa de seguridad aplicable al entorno local, la implementación del equipo permitirá compartir la experiencia y resultados obtenidos con otras universidades a través de organismos como CEDIA con el objetivo de proponer la creación de una red nacional de CSIRTs académicos y contribuir así a la investigación y desarrollo de metodologías y buenas prácticas que permitan mejorar la seguridad de las redes ecuatorianas.

Los beneficiarios de la implementación de este proyecto serán principalmente la UTPL y con la implementación del proyecto:

- Otras Universidades
- Organizaciones públicas y privadas que mantienen Equipos de Seguridad.
- Empresas y profesionales que brindan servicios de atención de incidentes.
- CEDIA, y las universidades que forman parte de este organismo, con la finalidad de profundizar y proponer temas de investigación.

Debe indicarse, que durante el proceso de creación e implementación del CSIRT-UTPL se ha hecho conocer de esta iniciativa a CEDIA a través de la presentación del proceso de creación seguido, y con la emisión de un informe ejecutivo de las actividades que se han

¹ Consorcio Ecuatoriano para el Desarrollo de Internet Avanzado (<http://www.cedia.org.ec/>)

realizado, esto con la finalidad de compartir la experiencia del proceso de creación del CSIRT-UTPL.

Se conoce que la SUPERTEL² y las Fuerzas Armadas del Ecuador actualmente están implementando un equipo CSIRT, se han enviado comunicaciones a cada uno de ellos, informándoles del CSIRT-UTPL, para de esta manera establecer futuros vínculos de colaboración.

Se han establecido comunicaciones con UNAM-CERT de México, con quienes se ha compartido información en el tema de malware que podría afectar a organizaciones ecuatorianas.

El proyecto es propuesto por la Universidad Técnica Particular de Loja, bajo la dirección de Msc. María Paula Espinosa, tiene una duración de 12 meses.

Las actividades de proyecto se planificaron desde enero de 2010, pero por motivos de asignación de fondos se inició el 22 de febrero de 2010, el proyecto finaliza el 22 de febrero de 2011.

Hasta la presente fecha el proyecto se encuentra en el onceavo mes de ejecución, las diferentes actividades programadas se han realizado de acuerdo a lo planificado y hasta el momento se han cumplido las actividades propuestas, de acuerdo al cronograma planificado. (Ver Anexo 1)

El detalle de las actividades realizadas hasta la fecha se detalla a continuación:

2. Objetivo General

Construir y proponer una normativa de seguridad aplicable al entorno local mediante la implementación de un Equipo de Respuesta a Incidentes para la Universidad Técnica Particular de Loja.

3. Objetivos Específicos

Objetivo específico 3 (agosto – Diciembre)	Definir una metodología para la detección, la atención, manejo y respuesta de incidentes de seguridad adaptada al entorno local.
Objetivo específico 4	Convertirse en un grupo de investigación en temas de

² Superintendencia de Telecomunicaciones

(enero – 2011)	seguridad de la información que permita generar estadísticas de los principales incidentes y vulnerabilidades reportadas en los sistemas de la UTPL y que servirán como insumo para otros grupos e investigaciones a fines.
Objetivo específico 5 (febrero 2011)	Proponer la creación de Equipos CSIRT a nivel de Universidades a través de organismos como CEDIA para impulsar la creación de un CSIRT Nacional.

- **Actividades del período Septiembre/2010 – Enero/2010:**

Actividades para el cumplimiento del Objetivo Específico N° 3 Definir una metodología para la detección, la atención, manejo y respuesta de incidentes de seguridad adaptada al entorno local.	Plazo de ejecución planificado	Plazo de ejecución realizado
	Mes/Año	Mes/Año
	Mayo /2010	diciembre /2010
3.1 Proponer el uso de una metodología para la atención, manejo y respuesta de incidentes en base a la problemática de la UTPL.	Mayo /2010	Julio /2010
3.2 Evaluación y modificación de la metodología propuesta para la atención, manejo y respuesta de incidentes.	Agosto/2010	Agosto /2010
3.3. Presentación de la metodología y políticas que van a ser utilizadas en el CSIRT-UTPL.	Septiembre/2010	Septiembre/2010
3.4 Capacitación a los integrantes del equipo en el uso y manejo de la metodología realizada para la atención, manejo y respuesta de incidentes	Octubre/2010	Octubre/2010
3.5. Capacitación a los administradores de servidores en el uso de formularios para el reporte de incidentes y vulnerabilidades.	Noviembre /2010	Noviembre/2010
3.6. Evaluación a los administradores e integrantes del equipo en el tema de políticas de seguridad y de la metodología para la atención, manejo y respuesta de incidentes.	Diciembre /2010	Diciembre /2010

Actividades para el cumplimiento del Objetivo Específico N° 4 Convertirse en un grupo de investigación en	Plazo de ejecución planificado	Plazo de ejecución realizado
---	---------------------------------------	-------------------------------------

temas de seguridad de la información que permita generar estadísticas de los principales incidentes y vulnerabilidades reportadas en los sistemas de la UTPL y que servirán como insumo para otros grupos e investigaciones a fines..	Mes/Año enero /2011	Mes/Año enero /2011
4.1 Realizar el Monitoreo de las actividades que se registran en los servidores de la UTPL, y registrar los hallazgos presentados.	enero /2011	enero /2011
4.2 Realizar el Triage de la información recibida en el CSIRT en base a la metodología propuesta.	enero /2011	enero /2011
4.3. Consolidación de Resultados	enero /2011	enero /2011

Actividades para el cumplimiento del Objetivo Específico N° 5 Proponer la creación de Equipos CSIRT a nivel de Universidades a través de organismos como CEDIA para impulsar la creación de un CSIRT Nacional.	Plazo de ejecución planificado	Plazo de ejecución realizado
	Mes/Año febrero /2011	Mes/Año febrero /2011
5.1 Presentar la experiencia y resultados obtenidos de la implementación del CSIRT – UTPL a través del portal del equipo, de presentaciones y publicaciones..	febrero /2011	febrero /2011

4. Indicadores de Avance: Verificación de Resultados

Se recomienda crear un sitio Web del Proyecto, de ser posible, a fin de acceder a Indicadores y Medios de Verificación. Los indicadores deben estar muy precisados y los medios de verificación deben ser “verificables”.

N° Actividad	N° Resultado	Indicador	Medio de Verificación
3.1 Proponer el uso de una metodología para la atención, manejo y respuesta de incidentes en base a la problemática de la UTPL.	Metodología para el manejo de incidentes para la UTPL.	Versión 1 de la metodología propuesta para su revisión.	Metodología para el Manejo de Incidentes – CSIRT-UTPL versión 1.
3.2 Evaluación y modificación de la metodología propuesta para la atención, manejo y respuesta de incidentes.	Metodología aprobada por autoridades para el manejo de incidentes en la UTPL.	<ul style="list-style-type: none"> • Metodología para el manejo de incidentes aprobada. • 30% de la comunidad objetivo hacen uso de la metodología desarrollada para el manejo de incidentes del CSIRT-UTPL. 	Metodología Final (Actualmente en proceso de aprobación). <u>Ver anexo 2 y 3</u> <i>Nota: Actualmente a la interno del equipo, se está haciendo uso de la metodología.</i>
3.4 Capacitación a los integrantes del equipo en el uso y manejo de la metodología realizada para la atención,	Integrantes del área de Seguridad conocen de la metodología para el	<ul style="list-style-type: none"> • Uso de reportes para la respuesta de incidentes • Clasificación de la Información (Triage) 	Los integrantes del equipo conocen y hacen uso de la metodología para el manejo

<p>manejo y respuesta de incidentes</p>	<p>manejo de incidentes</p>	<ul style="list-style-type: none"> • Detección (Monitoreo de servicios críticos haciendo uso de herramientas de seguridad) 	<p>de incidentes.</p> <p>Uso de la metodología para el manejo de incidentes y de los procesos que son parte de la metodología para el proceso de manejo de incidentes en el CSIRT-UTPL</p>
<p>3.5. Capacitación a los administradores de servidores en el uso de formularios para el reporte de incidentes y vulnerabilidades.</p>	<p>Comunidad objetivo hace uso de formularios para el reporte y registro de incidentes y vulnerabilidades.</p>	<p>Disminución del número de incidentes en los usuarios finales porque hacen uso de políticas.</p>	<p>Cantidad de reportes recibidos.</p> <p>Nota:</p> <p><i>Mediante una reunión, se hizo conocer a los administradores de servidores sobre el uso de los reportes de incidentes y vulnerabilidades, las políticas para el reporte y respuesta de incidentes.</i></p> <ul style="list-style-type: none"> • <i>La última semana de enero se inicia con la campaña a lo interno de la UTPL para que los usuarios finales de la universidad conozcan del CSIRT.</i>

<p>4.1 Realizar el Monitoreo de las actividades que se registran en los servidores de la UTPL, y registrar los hallazgos presentados.</p>	<p>Contar con herramientas adecuadas para el análisis de incidentes y estudio de tráfico.</p>	<p>Reportes estadísticos de incidentes y vulnerabilidades de los primeros meses. Clasificación de los reportes recibidos en: incidentes y vulnerabilidades durante los primeros meses.</p>	<p>Reportes Estadísticos de incidentes y vulnerabilidades recibidas.</p> <p>Ver: Portal WEB</p> <p>www.utpl.edu.ec/csirt-utpl</p> <p>Sección: Estadísticas.</p> <p><u>Nota:</u></p> <p><i>Diariamente se realiza el monitoreo de los sistemas, se emiten reportes mensuales, si se detecta algún anomalía, esta es reportada al administrador del equipo, haciendo uso de los reportes establecidos para que el mismo sea atendido.</i></p>
<p>4.2 Realizar el Triage de la información recibida en el CSIRT en base a la metodología propuesta.</p>	<p>Contar con herramientas adecuadas para el análisis de incidentes y estudio de tráfico.</p>	<p>Reportes estadísticos de incidentes y vulnerabilidades de los primeros meses. Clasificación de los reportes recibidos en: incidentes y vulnerabilidades durante los primeros meses.</p>	<p>Reportes clasificados por categorías, y por incidentes, vulnerabilidades e información recibida.</p> <p><i>Ver portal: sección de estadísticas</i></p>
<p>4.3. Consolidación de Resultados</p>	<p>Resultados de las actividades realizadas</p>	<p>Implementación CSIRT-UTPL Procesos y metodologías</p>	<ul style="list-style-type: none"> • Metodología para el manejo de incidentes

	hasta la fecha	establecidas y aprobadas	<p>(Anexo 2).</p> <ul style="list-style-type: none"> • Políticas para el reporte de incidentes y vulnerabilidades; y de manejo y respuesta de incidentes (Anexo 4) • Boletín para publicidad CSIRT-UTPL (Ver Anexo 5)
5.1 Presentar la experiencia y resultados obtenidos de la implementación del CSIRT – UTPL a través del portal del equipo, de presentaciones y publicaciones.	Universidades conozcan del equipo CSIRT-UTPL	Al menos una universidad toma la iniciativa de crear un CSIRT	<p>Documentación presentada</p> <p>Se realizó la presentación de un paper en el evento LACNOG 2010 - LACNIC XIV – 4º PTT Fórum realizado en Sao Paulo Brasil en Octubre de 2011.</p> <p>Ver portal WEB</p> <p><i>Nota:</i> Adicionalmente se envió un informe ejecutivo a CEDIA en el que se explicaba el proceso de creación del CSIRT-UTPL</p>

5. Participación efectiva de todos los intervinientes en el proyecto.

Hasta la fecha la participación de los integrantes del equipo se ve reflejada en el cumplimiento de las actividades, estas se han realizado acorde a lo planificado.

Se ha involucrado a personal de Marketing para la publicidad del CSIRT.

6. Reuniones de Coordinación

Se mantuvieron reuniones con:

- Grupo de seguridad para la presentación de la metodología para el manejo de incidentes.
- Grupo de Administradores para comunicarles la existencia del CSIRT-UTPL, uso de reportes de incidentes y políticas.

7. Actividades de Difusión

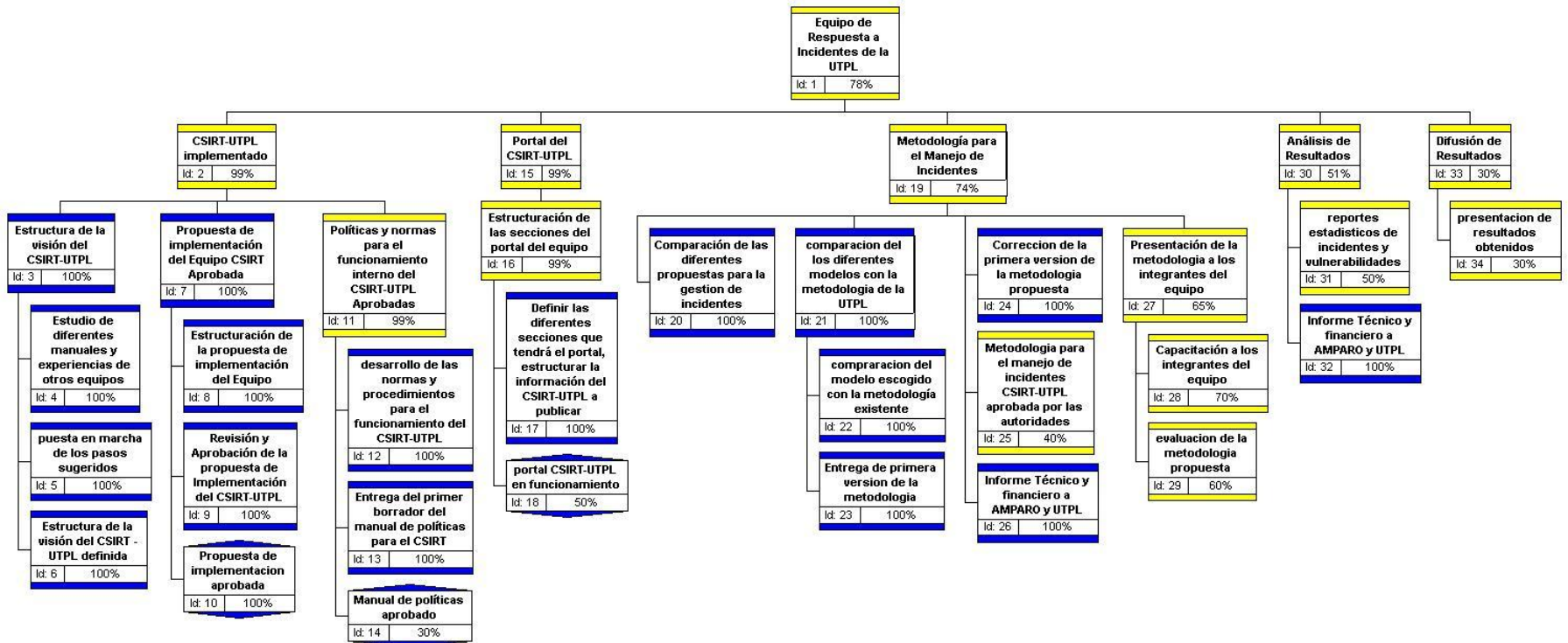
- Emisión de boletines con tips de seguridad para usuarios, los mismos que se emitirán mensualmente. Como estrategia de marketing, durante el primer mes se emitirán boletines semanalmente, con el objetivo de posicionar el CSIRT-UTPL en la comunidad universitaria.
- En conjunto con el área de marketing de la UTPL se está preparando una estrategia de comunicación para realizar la difusión del CSIRT-UTPL, lo que incluye boletines informativos, notas periodísticas, etc.
- Emisión de un boletín sobre el CSIRT-UTPL al área de marketing para que sea difundido a nivel interno en la UTPL.

8. Referencias

- [1] Defining Incident Management Processes for CSIRTs: A Work in Progress
www.cert.org/archive/pdf/04tr015.pdf
- [2] Computer Security Incident Handling Guide
<http://csrc.nist.gov/publications/nistpubs/800-61-rev1/SP800-61rev1.pdf>

9. Anexos

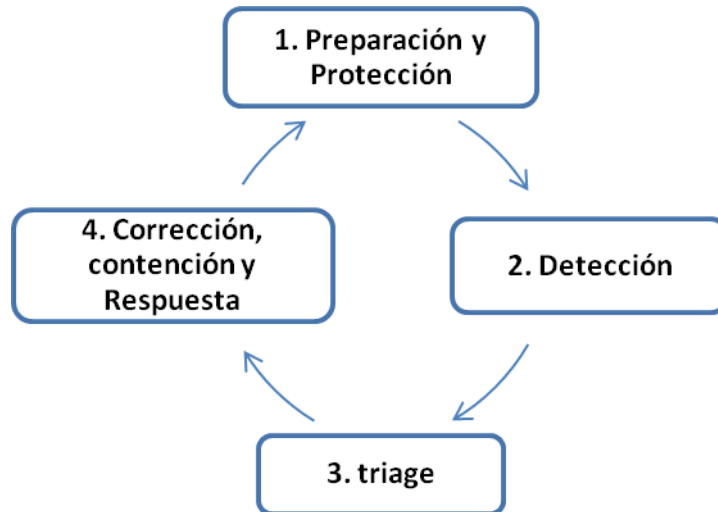
Anexo 1: Cronograma de Actividades



Archivo Adjunto: [Cronograma](#)

Anexo 2: Metodología para el Manejo de Incidentes CSIRT – UTPL

La metodología implementada se basa fuertemente en [1] y [2], básicamente se ha estructurado de acuerdo al siguiente esquema:



Cada uno de los pasos propuestos se describe a continuación:

1. Preparación y Protección

La fase de preparación consiste, principalmente, en la implementación de un equipo de Respuesta a Incidentes de Seguridad Informática³ (CSIRT), las actividades propuestas, que se deben realizar en esta fase son:

- Planificación del CSIRT – UTPL
- Implementación del CSIRT – UTPL
- Evaluación y funcionamiento del CSIRT
- Lecciones Aprendidas.

A más de definir un proceso de implementación de un equipo de CSIRT, es importante tomar en cuenta la Protección de la infraestructura de la Universidad para de esta manera asegurar que los

³ Computer Security Incident Response Team

sistemas, redes y aplicaciones tengan un nivel de seguridad adecuado. Las actividades de esta fase se realizan en conjunto con el área de Seguridad, pero básicamente el área de Manejo de incidentes tiene a su cargo la prevención de ataques, y si estos suceden mitigar el impacto. El área de seguridad realiza actividades de protección, en cuanto a configuraciones y garantiza la infraestructura informática de la Universidad.

2. Detección de Incidentes de Seguridad

Esta fase está compuesta de varias actividades (Ver: Fig. 4), tales como: detección de incidentes, análisis inicial y documentación del incidente y tiene como objetivo la búsqueda de toda posible señal de ocurrencia de un incidente. Todas las actividades e información generada en esta fase en enviada al proceso de Triage, haciendo uso de los reportes establecidos.

2.1. Detección de Incidentes

La Detección de incidentes es un proceso que permite identificar las actividades inusuales que pueden comprometer la misión del CSIRT, consiste en la detección y evaluación de posibles incidentes, determinar si un incidente ha ocurrido, y de ser así, el tipo, extensión y magnitud del problema.

Estas actividades se pueden identificar de manera reactiva y proactiva.

Los incidentes se pueden detectar a través de muchos medios tales como: IDS basados en red (NIDS) y en host (HIDS), software antivirus, software de control de integridad de archivos, sistemas de monitoreo de red, analizadores de logs, etc.

Los incidentes también pueden ser detectados por medios manuales, tales como reportes de incidentes de usuarios.

En el proceso de detección están involucrados: Área de Seguridad, CSIRT-UTPL, Gestión de Servicios TI, Infraestructura de TI, usuarios que han sido víctimas de algún ataque y otras áreas, incluye los siguientes aspectos:

- Señales de un incidente
- Detección de incidentes mediante la utilización de herramientas
- Detección de incidentes mediante el reporte de terceros.

2.1.1. Señales de un Incidente:

En el proceso de detección, la información sobre potenciales incidentes, vulnerabilidades, información de seguridad informática o de manejo de incidentes, puede ser obtenida de dos maneras:

- **Detección Reactiva**

Un incidente puede haber ocurrido o estar ocurriendo en este momento, puede ser detectado de varias maneras:

- ✓ El antivirus detecta que un equipo está contaminado con algún tipo de virus.
- ✓ Incidentes en el servidor web
- ✓ Envío de alertas y notificaciones por parte de otras organizaciones.

- **Detección Proactiva**

Involucra el monitoreo de posibles actividades sospechosas a través de:

- Reportes de IDS, pueden ayudar a la detección de actividades antes de que suceda un incidente.
- Monitoreo de Red
- Escaneo de vulnerabilidades
- Investigación
- Análisis de Riesgos

2.1.2. Detección de incidentes mediante la utilización de herramientas

La detección de incidentes es un proceso que permite saber si el sistema está en peligro o si los servidores corren el riesgo de detener sus servicios.

Esta actividad va de la mano con la detección proactiva, se debe tomar en cuenta el personal que se encargue del monitoreo y detección de actividad sospechosa, análisis de logs, uso de software de detección de intrusos, para cada una de estas actividades se deben tomar en cuenta los procesos establecidos en el Área de Seguridad para estas actividades.

Todos los datos analizados y los considerados sospechosos se envían al proceso de Triage.

2.1.3. Detección de incidentes mediante el reporte de terceros

Va de la mano con la detección reactiva, el usuario notifica del incidente al área de Gestión de Servicios, si el incidente se encuentra en la base de conocimiento de esta área, es atendido por

ellos, caso contrario se envía el reporte del incidente al equipo CSIRT – UTPL, en donde, primeramente se verifica que sea un incidente de seguridad (Fig.5).

Los incidentes que se envían al CSIRT-UTPL y los que se atienden, son los que constan en la categorización de incidentes del CSIRT-UTPL.

2.2. Análisis de Incidentes de Seguridad

En este proceso se busca analizar cada reporte de incidentes presentado, tanto por los usuarios y por los reportes obtenidos de las herramientas utilizadas, con la finalidad de verificar si realmente se trata de un incidente de seguridad, o son falsos positivos.

Se debe recalcar que el equipo CSIRT debe trabajar rápidamente en el análisis y validación de los incidentes, todas las acciones realizadas deben ser documentadas.

2.3. Documentación del Incidente

Uno de los mecanismos que sirve de soporte para Detección es la documentación del incidente, se han definido varios formatos para el reporte y respuesta de incidentes y vulnerabilidades, el uso de reportes ayuda a:

- ✓ Proveer información completa de un incidente al equipo
- ✓ Organizar la información recibida
- ✓ Priorizar reportes

La información que se solicita en el reporte de incidente es:

- ✓ Información de contacto
- ✓ Fecha de reporte
- ✓ Sistemas afectados
- ✓ Descripción del incidente
- ✓ Observaciones

A más de los reportes de incidentes, parte de la documentación incluye un documento en el que se detalla el cómo los usuarios deben realizar el reporte de los incidentes al equipo, etc.

Adicional al reporte de incidente enviado por el usuario, por parte del Equipo CSIRT-UTPL se debe enviar un documento de respuesta a incidentes, en el que se detalle la información relativa a la atención y respuesta del incidente reportado, dependiendo del tipo de incidente, esta

información será enviada a autoridades, y personal que requiera de esta información. (Esta sección, se detalla en la fase de la respuesta a incidentes).

Es importante la implementación de herramientas que permitan realizar el seguimiento de los incidentes, la información almacenada debe contener información sobre:

- El estado actual del incidente.
- Un resumen del incidente
- Las acciones tomadas en el manejo del incidente
- Información de contacto de las partes involucradas
- Comentarios del personal que atendió el incidente.
- Acciones a tomar, recomendaciones a administradores, parches, etc.

Algunas herramientas que se utilizan son:

- ✓ RTIR
- ✓ Request Tracker

3. Triage

En la metodología propuesta se ha incluido una nueva fase, el proceso del triage, esta fase reemplaza al apartado titulado: Preparación ante un incidente de seguridad, que consta de:

- Categorizar un Incidente
- Clasificar los incidentes.

El objetivo de la función de triage es: asegurar que toda la información destinada para el manejo de incidentes sea canalizada a través un único punto de contacto.

El Triage consiste en recibir la información, clasificarla y ordenarla con la finalidad de determinar si el reporte que se recibe está relacionado con eventos pasados, o con nuevos eventos, luego, asignar una prioridad que esté de acuerdo al esquema de prioridades definido y, asignar el reporte al experto para su respuesta.

3.1. ¿En qué consiste el Proceso de Triage definido para la UTPL?

El proceso de triage involucra la revisión de la información entrante, en determinar su validez y clasificar la información en Incidentes, Vulnerabilidades e Información general. Cuando la

información es recibida primero se envía un acuse de recibo de la información indicando que la información fue recibida, y que será atendida en el menor tiempo posible.

Luego, la información es clasificada, correlacionada y priorizada, la información que está catalogada como incidente es asignada al experto para su respuesta.

El proceso se realiza de acuerdo a los siguientes subprocesos:

3.1.1. Categorización y Correlación

Proceso que primeramente consiste en categorizar y establecer criterios para lo que se ha definido como incidente en la UTPL, por ejemplo: denegación de servicios, robo de identidad, etc.

Una vez definida la categorización de los incidentes, el proceso consiste en determinar el tipo de evento reportado, luego, en correlacionar esta información con otros incidentes atendidos, con el objetivo de determinar si es un incidente nuevo, si ha sido tratado anteriormente y está archivado en la base de conocimientos del CSIRT.

Si es un evento nuevo este es categorizado y enviado al proceso de priorización, para posteriormente enviarlo al proceso de respuesta.

Durante el proceso de Categorización y Clasificación de la información es importante hacer uso de una nomenclatura que permita un mejor manejo y clasificación de la información que es remitida al CSIRT.

Para un mejor manejo de la información, esta puede clasificarse en: reporte de incidente, reporte de vulnerabilidades e información general.

La nomenclatura propuesta para el CSIRT – UTPL es

- CSIRT#: para el seguimiento de incidentes.
- VUL#: es el prefijo utilizado para el seguimiento de vulnerabilidades.
- INFO#: prefijo usado para la identificación de otro tipo de información.

La información clasificada como incidente y luego de pasar por el proceso de triage, es enviada al proceso de respuesta para su atención.

3.1.2. Priorización

Consiste en determinar los incidentes que son de alta prioridad, las decisiones se realizan en base a la misión del CSIRT y sus políticas, por ejemplo: por tipo de incidente reportado y dependiendo de la persona que reporta el incidente, si un incidente es reportado desde el

Rectorado de la Universidad independientemente del tipo de incidente que sea tiene alta prioridad de respuesta.

La prioridad se establece en base a dos factores:

3.1.2.1. Efecto técnico actual y potencial del incidente.

Los encargados de la respuesta de incidentes deben considerar no sólo el efecto técnico negativo del incidente (por ejemplo, acceso no autorizado a nivel de usuario a los datos), sino también el probable efecto futuro del incidente, si no es contenido inmediatamente.

3.1.2.2. Criticidad de los recursos afectados.

Recursos afectados por un incidente, por ejemplo, firewalls, servidores web, conectividad a Internet, estaciones de trabajo de usuario y aplicaciones.

Más Información: sección 1.2 del Anexo 3: [priorización](#)

3.1.3. Asignación

La asignación del incidente es el proceso que sigue a la priorización, este proceso tiene como objetivo asignar el incidente a un experto para su resolución, lo que significa que toda la información es enviada al proceso de Respuesta. La asignación se realiza en base al tipo de incidente y a la carga de trabajo de los expertos.

NOTA

Información adicional en el [archivo adjunto](#).

Anexo 3: Fundamentación

Para la estructuración de la metodología para la atención y manejo de incidentes, el estudio se basó en dos documentos, el uno publicado por la Carnegie Mellon [1] y otro por la SANS [2], en estos documentos se describen las diferentes fases para la gestión y manejo de incidentes, (Ver: fig. 2 y 3).



Fig 2: modelo presentado por SANS

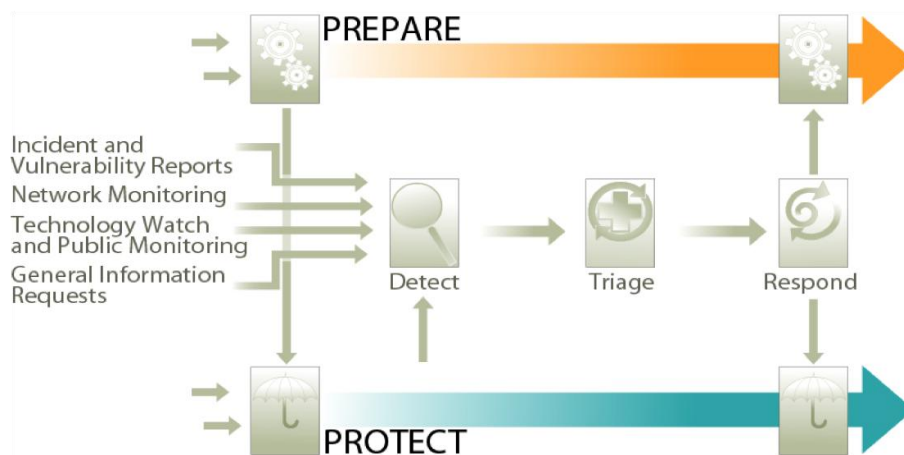


Fig 2: modelo presentado por Carnegie Mellon

Actualmente en base al estudio de los documentos mencionados y en base a la metodología para el manejo de incidentes elaborada en la UTPL se realizará la propuesta para la definición de la metodología que se utilizará en la UTPL.

NOTA

Se adjunta documentación de [\[1\]](#) y [\[2\]](#).

Anexo 4: Políticas para el reporte y manejo de incidentes

Nota: Documentación

- [Política para el Reporte de Incidentes y Vulnerabilidades](#)
- [Política para el Manejo y respuesta de Incidentes](#)

Anexo 5: Información enviada al Departamento de Marketing de la UTPL

El siguiente modelo de boletín se envió al Departamento de Marketing para la difusión del equipo.

EQUIPO DE RESPUESTA A INCIDENTES DE SEGURIDAD INFORMÁTICA
ÁREA DE SEGURIDAD DE LA INFORMACIÓN - UNIDAD DE GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN

¿QUÉ ES EL CSIRT - UTPL?
Es el equipo de respuesta a incidentes de seguridad informática de la UTPL, es el encargado de: brindar atención, soporte y respuesta a incidentes de seguridad que afecten a Autoridades, Docentes, Estudiantes, equipos y servicios de la Universidad.

SERVICIOS

- Alertas y Advertencias.
- Manejo de Incidentes.
- Detección de Intrusiones.
- Implementación y configuración de herramientas, aplicaciones, infraestructuras y servicios de seguridad.
- Estudio de tráfico malicioso.
- Educación y capacitación en temas de seguridad.

¿CUÁNDO CONTACTARSE CON EL CSIRT?

- Sospeche que ha sido víctima de suplantación o robo de identidad de correo electrónico.
- Cree que han accedido a datos privados, haciendo uso de medios electrónicos.
- Reciba correos electrónicos con contenido que desacredite su identidad.
- Detecte anomalías en los sistemas que usted maneja.

CONTACTOS
Unidad de Gestión de Tecnologías de Información
Área de Seguridad
CSIRT - UTPL
ext: 2543
email: csirtutpl@utpl.edu.ec

www.utpl.edu.ec/csirt-utpl

