FORMACIÓN DE UN COMPUTER SECURITY INCIDENT RESPONSE TEAM EN LA UNIVERSIDAD NACIONAL DE INGENIERIA CSIRT-UNI

FORMATION OF A COMPUTER SECURITY INCIDENT RESPONSE TEAM IN THE NATIONAL UNIVERSITY OF ENGINEERING CSIRT-UNI

Erik J. Borda Castillo[1], Cristhian Pacheco Castillo[1]

RESUMEN

El presente trabajo consiste en proponer la formación de un Equipo de Respuestas a Incidentes de Seguridad Informática en la Universidad Nacional de Ingeniería, que debiera responder de manera efectiva y oportuna a determinados incidentes de seguridad informática de nuestra universidad y algunos sectores de la sociedad. Asimismo, esta iniciativa denominada CSIRT-UNI busca impulsar activamente y formar parte del Centro de Coordinación Peruano de Respuesta a Emergencias de Seguridad Informática denominado PERUCERT/CC.

Palabras claves: CSIRT, CERT, Manejo de Incidentes, Seguridad Informática.

ABSTRACT

The present work consists of proposing the formation of a Computer Security Incident Response Team in the National University of Engineering, which had to respond of effective and opportune way to determined incident of computer security of our university and some sectors of the society. Also, this denominated initiative CSIRT-UNI looks for to impel actively and to comprise of the Peruvian's Coordination Center / Computer Emergency Response Team denominated PERUCERT/CC.

Keywords: CSIRT, CERT, Incidents Handling, Computer Security.

INTRODUCCIÓN

De acuerdo a un informe del SysAdmin, Audit, Network, Security (SANS) Institute: "más del 70% de los sitios con Firewall siguen estando vulnerables a ataques conocidos, más del 60% de los sitios están susceptibles a ataques de negación de servicio, más del 80% no saben que hay en su red ni qué está visible desde Internet y más del 80% tienen políticas de seguridad insuficientes".

Según un especial sobre Seguridad Informática publicado el año pasado en la revista especializada PC World Perú, sobre la base de un estudio de la empresa Dominio Consultores, en empresas e instituciones peruanas, sólo la mitad de los organismos encuestados tienen políticas de seguridad y las medidas de seguridad más comunes son aquellas que tienen un menor costo de mantenimiento y supervisión.

Siguiendo el informe, la mayoría de las empresas tiene una actitud pasiva y reactiva frente a la seguridad y su vulnerabilidad ante desastres es alta, pero, asimismo existe entre ellas una tendencia a incrementar las inversiones en seguridad.

Un Computer Security Incident Response Team (CSIRT) es una organización de servicios que es responsable de recibir, revisar y responder la actividad y reporte de los incidentes de seguridad informática. Sus servicios son usualmente realizados para una organización definida que debe ser una entidad padre como una corporación, gobierno u organización educacional; una región o país; una red de investigadores; o un cliente asalariado (1,2).

Este proyecto tiene como objetivo la creación de un Equipo de Respuesta ante Incidentes de Seguridad Informática en la Universidad Nacional de Ingeniería CSIRT-UNI, que debiera impulsar activamente y formar parte del Centro de Coordinación Peruano de Respuesta a Emergencias de Seguridad Informática (PERUCERT/CC), para responder de manera efectiva y oportuna ante determinados incidentes de seguridad informática de nuestra universidad y algunos sectores de la sociedad.

Como objetivos específicos el CSIRT-UNI pretende:

- Consolidar un Equipo de Respuesta a Incidentes de Seguridad con suficientes competencias para su desempeño en el CSIRT.
- Desarrollar trabajos preliminares de carácter formativo en seguridad informática sobre algunas áreas de la Facultad de Ingeniería Industrial y de Sistemas y la Universidad Nac. Ingeniería.
- Difundir intensamente la labor del CSIRT en los sectores académicos, profesionales y empresariales más importantes de la UNI y el país.
- Institucionalizar el CSIRT a través de Resoluciones Decanal y Rectoral, así como el establecimiento de la infraestructura, equipos, políticas y procedimientos.

Esta iniciativa se encuentra directamente relacionada con las actuales necesidades de aseguramiento de información de nuestra institución académica y de las instituciones pú-

[1] Universidad Nacional de Ingeniería – Facultad de Ingeniería Industrial y de Sistemas

blicas y privadas de este país. Asimismo, se encuentra vinculada con la creación del Centro de Coordinación Peruano de Respuesta a Emergencias de Seguridad Informática (PERUCERT/CC), actualmente en formulación por parte de algunas instituciones del gobierno.

Antecedentes y motivaciones de la creación del CSIRT-UNI

De manera histórica los antecedentes se remontan al 4 de Noviembre de 1988 cuando un virus (gusano informático) invade miles de computadoras basadas en sistemas operativos Unix en universidades e instalaciones de investigación militares, donde las velocidades de tiempo de respuesta en acceso a la red fueron reducidas y en otros casos detenidas. También el virus se propagó a escala internacional.

Era el ataque del que fue llamado "Gusano de Internet", y la prensa cubrió el tema con frases como "el mayor asalto jamás realizado contra los sistemas de la nación". Erradicarlo costó casi un millón de dólares, sumado a las pérdidas por haberse detenido casi toda la red.

El autor fue Robert Morris Jr, un graduado de la Universidad de Harvard de 23 años en ese entonces. Creó un programa con gran capacidad de reproducirse, pero sin embargo jamás pensó que se propagaría tan rápida y extensamente. Él mismo calificó su "invento" como un "fallo catastrófico".

Luego del incidente del “Gusano Morris”, que logró inhabilitar cerca del 10% de las computadoras conectados a Internet en noviembre de 1988 (unos 60,000 ordenadores) afectando los sistemas informáticos de centros militares en los EE.UU., incluyendo la NASA, la Fuerza Aérea, el MIT, las universidades de Berkeley, Illinois, Boston, Stanford, Harvard, Princeton, Columbia y otras, la agencia DARPA (Defense Advanced Research Projects Agency) comisionó al SEI, Software Engineering Institute de la Universidad Carnegie Mellon, el configurar un centro de coordinación entre expertos para enfrentar emergencias de seguridad y trabajar en la prevención de futuros incidentes.

El resultado fue la inmediata conformación del Computer Emergency Response Team / Coordination Center, hoy CERT®/CC. Desde entonces CERT®/CC ha capacitado y apoyado la formación de la mayoría de Equipos de Respuesta a Incidentes más conocidos alrededor del mundo.

El Centro de Coordinación CERT® (CERT®/CC) es un centro de experiencia en Seguridad Informática y está ubicado en el Instituto de Ingeniería de Software, centro de investigación y desarrollo subvencionado por el gobierno de los EEUU, fundado y gestionado por la Universidad Carnegie Mellon en Pittsburgh, Pennsylvania.

El Proyecto de formación del CSIRT-UNI tiene como antecedentes inmediatos las iniciativas aisladas de alumnos, egresados y docentes, quienes desde su espacio académico o profesional constataron la necesidad de responder adecuadamente a los incidentes de seguridad que ocurren frecuentemente y que no pueden ser solucionados. Asimismo, se encontraron con la realidad de no ubicar muchos especialistas con conocimientos en el tema y menos aún con una institución imparcial que eduque sobre la normatividad, políticas, procedimientos y tecnologías en esta área.

Cuando llegan a ocurrir incidentes de seguridad informática, se hace crítico para una organización el contar con una manera eficaz de responder. La rapidez con la que una organización puede reconocer, analizar, y responder a un incidente podrá limitar el daño de un incidente y reducirá el costo de su recuperación.

El CSIRT-UNI debe operar sobre este terreno y conducir una respuesta rápida, eficaz y eficiente para contener el incidente de seguridad computacional y además conducir la recuperación frente al mismo. Las relaciones con otros equipos de respuesta y organizaciones de seguridad pueden facilitar el compartir estrategias de respuesta rápida y unificada, además de ofrecer alarmas tempranas a problemas potenciales.

El CSIRT-UNI debe trabajar proactivamente con otras áreas de la Institución para asegurar que nuevos sistemas se desarrollen e implanten con "seguridad en mente" y en conformidad con un conjunto de políticas de seguridad preestablecidas. El CSIRT-UNI debe ayudar a identificar las áreas vulnerables de la Institución y realizar la evaluación del riesgo, análisis de vulnerabilidades y hasta la detección de un incidente en curso.
Las motivaciones que guían el establecimiento del CSIRT-UNI comprenden:

- Un incremento general en el número de incidentes de seguridad informática que han sido reportados.
- Un incremento general en el número y tipo de organizaciones que han sido afectadas por incidentes de seguridad informática.
- Una mayor conciencia enfocada por las organizaciones en la necesidad por tener políticas y prácticas de seguridad como parte de sus estrategias globales de administración de riesgos.
- Nuevas leyes y regulaciones que impactan en cómo las organizaciones son requeridas para proteger sus activos de información.
- La comprensión de la insuficiencia en recursos técnicos y no-técnicos de los administradores de sistemas y redes los cuales no pueden proteger en forma aislada los activos y sistemas de su organización.

La demanda existente en el país sobre el tema de seguridad de la información está dado por organismos del Estado, organismos privados e instituciones académicas, que tienen o están implementando sistemas de red para su operatividad. Sin embargo, no es posible satisfacerla ya que no se cuenta con el personal calificado y con la experiencia requerida para la formación de equipos de respuesta ante incidentes de seguridad de carácter privado.

La principal motivación de la formación del equipo CSIRT-UNI es la activa participación en la formulación de un proyecto que permita una sólida creación de un Centro de Coordinación Peruano de Respuesta a Emergencias de Seguridad Informática (PERUCERT/CC), el cual tendría una estructura UNIVERSIDAD-ESTADO-EMPRESA y estaría orientado a la formación de nuevos CSIRTs en el Estado, asimismo una correcta coordinación entre todas éstas, con el objetivo general de salvaguardar la integridad y seguridad de los activos informáticos de la nación y demás organizaciones públicas y/o privadas.

PLAN DE TRABAJO

Se programó las siguientes actividades, planteándose metas por entregables en cada uno de los pasos descri-

tos en la siguiente tabla :

PASO	DESCRIPCIÓN
1	Obtener Soporte y Convencimiento de la Alta Dirección
2	Determinar los Lineamientos Estratégicos del CSIRT
3	Recoger Información Relevante
4	Diseñar la visión del CSIRT
5	Comunicar la visión y plan operativo del CSIRT
6	Empezar la implementación del CSIRT
7	Anunciar y empezar la operación del CSIRT
8	Evaluar la efectividad del CSIRT

Proyectos desplegados para la formación del CSIRT

Estos proyectos son iniciativas que se desprenden del plan de trabajo expuesto y que deben culminarse con algunos entregables hasta el inicio de operaciones del CSIRT-UNI. Luego, muchos de ellos se convertirán en funciones del CSIRT y aparecerán nuevos proyectos en cartera.

a) Capacitación Equipo CSIRT

Alcance

Llevar a cabo actividades de capacitación generales o especializados que tengan que ver con la actividad del CSIRT. Asimismo, se deben establecer convenios institucionales que permitan conseguir facilidades para el entrenamiento de los miembros del equipo. Los miembros del equipo CSIRT-UNI deberán responder a una amplia variedad de habilidades técnicas y de rasgos de personalidad.

El personal del CSIRT debe ser dedicado, innovador, detallista, flexible, analítico y con integridad a toda prueba. Son solucionadores de problemas, buenos comunicadores y capaces de manejar situaciones estresantes.

Entre los roles organizacionales que se pueden incluir se cuentan: gerentes o líderes del equipo, supervisores o líderes de grupos, staff de mesa de ayuda y coordinadores de emergencias, manejadores de incidentes y de vulnerabilidades, especialistas de plataformas, entrenadores de personal y analistas de tecnología (3).

Entregable

Equipo del CSIRT-UNI capacitado en Gestión de la Seguridad Informática, Operación multiplataforma, Implementación de la Norma ISO17799, Tecnologías de Redes, Manejo de herramientas de seguridad y auditoría Informática.

b) Difusión del CSIRT

Alcance

Difundir las actividades que desarrolle el CSIRT antes o durante su puesta en funcionamiento. Es decir, se deben contactar con medios escritos, radiales, televisivos y de Internet para difundir los resultados de nuestra actividad. Asimismo, se hará cargo de la realización de eventos relacionados con nuestra institución.

Entregables

- Información sobre el CSIRT en al menos un medio de comunicación escrita, un radial, un televisivo y uno de Internet.
- Eventos de presentación en la FIIS, en la UNI y para la comunidad en general.

c) Marco Legal CSIRT

Alcance

Estudiar y analizar el marco legal concerniente a nuestra actividad como CSIRT. Es decir, se deben recoger, sintetizar y dar a conocer todas las normas legales que afecten el inicio de nuestra operación.

Entregables

- Informe sobre el Marco Legal relacionado con la Seguridad Informática en el país y en el mundo.
- Informe sobre nuestra situación formal con el CERT Perú, el CERT®/CC del SEI de la Carnegie Mellon y el Forum of Incident Response and Security Team (FIRST)

d) Piloto en el Instituto Sistemas UNI y el Centro de Cómputo de la UNI

Alcance

Evaluar la situación actual de la seguridad informática en el Instituto Sistemas UNI y el Centro de Cómputo de la UNI, entregando además recomendaciones generales y especializadas.

Entregable

Informe con la descripción de la evaluación y las recomendaciones entregadas.

e) Gestión de la Información

Alcance

Recoger, analizar, sintetizar y difundir toda la información relacionada con la Facultad y la UNI. Es decir, se deberá estudiar su funcionamiento, su estructura organizacional, sus necesidades en el tema de seguridad informática y la manera en que actualmente afrontan este tema.

Entregable

Informe sobre la Facultad (FIIS-UNI) y la UNI que incluya en detalle información sobre como funciona, como está organizado, sus necesidades en el tema de Seguridad Informática y la manera en que se gestiona este tema en la actualidad.

f) Institucionalización CSIRT

Alcance

Formalizar la existencia del CSIRT en la Facultad y en la UNI, para ello se buscará la aprobación de las autoridades y los recursos que permitan iniciar la actividad del CSIRT.

Entregables

- Aprobación del funcionamiento de las Autoridades de la Facultad y de la UNI.
- Aprobación de la entrega de recursos financieros, materiales y tecnológicos para el funcionamiento del CSIRT.

g) Participación en Eventos Académicos

Alcance

Planificar la participación del equipo CSIRT en eventos relacionados con la seguridad informática, para ello se buscará asistir presentando artículos de investigación, exposiciones especializadas o como asistentes únicamente.

Entregable

Participación del equipo CSIRT en por lo menos un evento nacional y otro internacional, a través de artículos, exposiciones y asistencia.

h) Implementación CSIRT

Alcance

Implementar físicamente la infraestructura que necesitará el CSIRT. Es decir, la configuración de la red y los reglamentos que normarán su funcionamiento.

Entregables

- Implementar la infraestructura tecnológica necesaria que incluya reglamentos y procedimientos.
- Elaborar guías para la operación del CSIRT como reportes, recepción, análisis y comunicación de incidentes y notas técnicas.

i) Evaluación de la Actividad CSIRT

Alcance

Establecer procedimientos e indicadores que permitan evaluar nuestra actuación en un determinado periodo de tiempo. Asimismo, se deben elaborar recomendaciones para conseguir un mejor tiempote respuesta del CSIRT-UNI.

Entregables

- Elaborar un modelo de evaluación interna basado en indicadores.
- Elaborar un informe que incluya la evaluación y las recomendaciones para una mejor actuación del CSIRT.

Servicios del CSIRT-UNI

El desarrollo de servicios por parte del CSIRT-UNI permitirá el autofinanciamiento de sus necesidades operativas. El CSIRT-UNI deberá, al finalizar su etapa formativa, cubrir de manera eficaz el funcionamiento de muchos de los siguientes servicios (4):

TIPOS DE SERVICIOS	SERVICIOS	
Servicios Reactivos	• Alertas y advertencias • Manejo de Incidentes • Análisis de incidentes • Respuesta a incidentes on-site • Soporte a respuesta de incidentes • Coordinación de respuesta a incidentes • Manejo de Vulnerabilidades	• Análisis de vulnerabilidades • Respuesta a vulnerabilidades • Coordinación de respuesta a vulnerabilidades • Manejo de artefactos técnicos de seguridad • Análisis • Respuesta • Coordinación de respuesta
Servicios Proactivos	• Publicaciones y anuncios • Observación tecnológica • Evaluación y Auditoría en Seguridad TI • Diseminación de información relacionada a seguridad TI	• Configuración y Mantenimiento de Herramientas, aplicaciones e infraestructura de seguridad TI • Desarrollo de herramientas de seguridad • Servicios de detección de intrusiones • Diseminación de información relacionada a seguridad TI
Servicios de Gestión de Calidad en Seguridad	• Análisis de riesgo • Continuidad del Negocio y Planeamiento de recuperación ante desastres • Consultoría en seguridad	• Concientización de temas en seguridad • Educación/Capacitación/Entrenamiento • Evaluación de productos y/o certificación

CONCLUSIONES

El crecimiento explosivo de las redes en Internet, la integración de las redes del Estado para el establecimiento de una futura implementación del e-goverment, el exponencial incremento del comercio electrónico, la diversidad de comunidades de usuarios, así como las inevitables amenazas a las que están expuestas estas redes, hace hoy en día impracticable el que una institución u organización, por sí sola pueda proveerse de un soporte universal para solucionar todo tipo de problemas de seguridad. Es bajo esta premisa que se enmarca la formación de equipos de respuesta ante incidentes de seguridad informática.

El presente trabajo consiste en la formación de un CSIRT en la Universidad Nacional de Ingeniería CSIRT-UNI, que debiera impulsar activamente y formar parte del Centro de Coordinación Peruano de Respuesta a Emergencias de Seguridad Informática (PERUCERT/CC), para responder de manera efectiva y oportuna ante determinados incidentes de seguridad informática de nuestra universidad y algunos sectores de la sociedad.
Este proyecto se justifica de acuerdo a los estudios internacionales y locales sobre el crecimiento de la inseguridad informática desde de la aparición de Internet. Asimismo, se sustenta en la experiencia personal y colectiva de algunos de los participantes de este proyecto quienes en su actividad laboral han debido enfrentar un sinnúmero de problemas y riesgos en seguridad informática y han formado parte en la evaluación de procedimientos y tecnologías para reducir la brecha de seguridad informática existente.

Una vez el CSIRT-UNI se encuentre en marcha, deberá convertirse en una institución que se sostenga económicamente por sí mismo en el tiempo. Asimismo, deberá consolidarse en una institución referente en los temas de Seguridad Informática en el Perú.

REFERENCIAS BIBLIOGRÁFICAS

1. West Brown, Moira; Stikvoort, Don; Kossakowski, Klaus; Killcrece, Georgia; Ruefle, Robin; Zajicek, Mark. Handbook for Computer Security Incident Response Teams (CSIRTs). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University; 2003.
2. Killcrece, Georgia; Kossakowski, Klaus Peter; Ruefle, Robin; Zajicek, Mark. Organizational Models for Computer Security Incident Response Teams (CSIRTs). Pittsburg, PA: Software Engineering Institute, Carnegie Mellon University; 2003.
3. Kossakowski, Klaus. Information Technology Incident Response Capabilities. Hamburg: Books on Demand; 2001.
4. CERT®/CC Carnegie Mellon University; Stelvio bv, The Netherlands; PRESECURE Consulting GmbH, Germany. CSIRT Services. Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University; 2002.

E-mail:
johnbordac@yahoo.com,
cristhian_pacheco@yahoo.com