

# **PLAN DE TRABAJO DEL GRUPO “RED DE SEGURIDAD EN CÓMPUTO/ANUIES”**

## **1. DESCRIPCIÓN DEL PLAN DE TRABAJO**

La infraestructura de tecnologías de información y comunicaciones participan en un importante rol en nuestras instituciones académicas, y aún cuando no sean visibles o percibidas en su totalidad y vastedad por el usuario final. Asegurar y mantener esta infraestructura contra amenazas informáticas, accidentes y abusos es de importancia vital y objetivo para el plan de trabajo.

## **2. JUSTIFICACIÓN DEL PLAN DE TRABAJO**

La continua evolución de la tecnología computacional, móvil, y de telecomunicaciones tiende a ser ubicua en nuestras instituciones de educación como una herramienta imprescindible para el trabajo académico, administrativo y de investigación. Asegurar la tecnología de cómputo y comunicaciones permite la continuidad de la misión y objetivos de la institución; la disrupción y/o daño parcial o irreparable puede paralizar dicha continuidad natural de manera importante y en algunos casos de manera irreversible.

La función de la seguridad en cómputo es resguardar y mantener la continua operación de las tecnologías de la información y comunicaciones de la institución, que coadyuva en la misión de negocio, metas y objetivos del organismo.

## **3. ALCANCE DEL PLAN DE TRABAJO**

El alcance del presente plan de trabajo es aportar y apoyar que las Instituciones de Educación Superior (IES) registradas y activas dentro de la Asociación nacional de Instituciones de Universidades e Institutos de Educación Superior (ANUIES), en su región centro-occidente implementen las mejores prácticas y maduren en los procesos esenciales de seguridad como contar con centros de operaciones, monitoreo, evaluación del uso acceso y seguridad de sus redes.

## **4. SE PROPONEN LOS 4 PROYECTO SIGUIENTES**

1. Crear una red de monitoreo regional representativa de la actividad de amenazas informáticas.
2. Formar un centro de operaciones NOC (*Network Operation Center*) en cada IES con equipos especializados para respuesta a incidentes de seguridad en cómputo.
3. Asentar en las IES marco de políticas técnico, legal y administrativas que regulen y fomenten el buen uso de los servicios informáticos y contrarresten el mal uso y abuso de los mismos.

4. Instrumentar una herramienta de evaluación continua que cuantifique la gestión de seguridad.

## 5. REQUISITOS DEL PLAN DE TRABAJO QUE CONSTA DE 4 PROYECTOS

Las características del producto o servicio final son las siguientes:

1. **Red de Monitoreo.** Programa para la instalación de dispositivos en la red de datos local, que actúen como colectores de la actividad anómala, virus, ataques informáticos, etc. Para su registro estadístico, análisis y las contramedidas requeridas para su control de propagación y en coordinación con otros centros especializados en seguridad (ej. CERT-UNAM).
2. **Centro de Operaciones NOC.** Creación de una infraestructura física y lógica con recursos en hardware, software y personal dedicado al monitoreo permanente de los servicios informáticos para cada institución, neutralización de amenazas que pongan en riesgo sus activos informáticos y el manejo de incidentes de seguridad en cómputo.
3. **Políticas de seguridad en cómputo.** Creación de un marco común de políticas de seguridad en cómputo incluyendo los aspectos técnicos, legales y administrativos, para su adecuación y aplicación formal hacia el interior de la normatividad institucional de cada IES.
4. **Instrumento de evaluación continua de la gestión de la seguridad.** Actividad periódica (cada 4 meses) que actúe como un marco referente y representativo de la gestión de la seguridad que se tiene en cada IES, en sus etapas transitorias, avances y/o retrocesos importantes.

## 6. ENTREGABLES DEL PRODUCTO

1. Creación de una red de monitoreo que concentre y represente la actividad de la región en cuanto amenazas informáticas se refiere.
2. Creación de un centro de operaciones de la red de cómputo (NOC), con una estructura de equipos locales para el manejo y respuesta a incidentes de seguridad.
3. Documento de registros de políticas en seguridad en cómputo aprobadas por la comunidad regional y aplicadas dentro de la normatividad de cada IES a través de sus cuerpos legislativos.
4. Un instrumento de evaluación continua para conocer y comparar los niveles de la gestión de seguridad en cómputo por IES.

## **7. ESTRATEGIAS SELECCIONADAS**

1. La estrategia principal a seguir es alinear las actividades de este plan de trabajo a las necesidades y proyectos compatibles en cada institución, y que de manera sincronizada y progresiva contribuya al trabajo de esta red en los esfuerzos de cada IES.
2. Asignación por parte de cada IES de un presupuesto para el desarrollo de las actividades de la red de seguridad en cómputo, con base en los insumos programados.
3. Los titulares deben ser designados y facultados por su actual rector a través de una carta compromiso con valides durante el periodo del proyecto o cambio del representante.
4. Coincidir en agendas por parte de los representantes de cada IES es un principal obstáculo para reunirse, y que sin embargo por la naturaleza de los trabajos y actividades se requiere un constante seguimiento. Por lo tanto las reuniones serán a través de telé-conferencias (voz/video) con una periodicidad mensual, y teniéndose una reunión presencial al año para la presentación de trabajos consolidados por cada IES.
5. El plan de capacitación y actualización continua es de suma importancia para la homologación en conocimiento y potenciación del mismo. La estrategia para esto será: gestionar los recursos necesarios para la participación y asistencia a estos foros capacitadores, que podrán ser de manera presencial o a distancia e impartidos por miembros de la red o externos. Así mismo la recolección de este conocimiento será puesta su consulta en sus diversos formatos originales: texto, video, etc.
6. La vinculación con organismos similares locales, nacionales o extranjeros, enriquece el trabajo de la red y mantiene su vigencia en el intercambio de experiencias. Se mantendrá una agenda de vinculación con estos organismos seleccionados de manera presencial y/o remota.

## **8. RESTRICCIONES DEL PLAN DE TRABAJO**

1. El trabajo realizado dentro de la red debe ser visible en resultados hacia el interior de cada IES. Dicho trabajo es responsabilidad y compromiso por cada representante de cristalizar los productos planteados.
2. El trabajo de la red estará limitado por nivel de compromiso y participación de la alta dirección en cada IES, que tiene como función el de promover e impulsar las iniciativas lanzadas por el grupo, trabajarlas y adecuarlas a la realidad de cada organización, para su concretización en resultados favorables para la misma.

## **9. FECHA DE INICIO Y FIN**

Periodo 2006-2008.

## **10. CALENDARIO BASE DE ACTIVIDADES:**

1. Red de monitoreo
  - a. Firma de acuerdo de confidencialidad e instalación de los sensores Honey-Net en coordinación con UNAM-CERT (Tiempo Aproximado: 2 meses).
  - b. Reportes continuos semanal y mensual de la actividad del sistema de monitoreo (tiempo: semanal y mensual)
2. Centro de operaciones
  - a. Instalación de hardware y software para (tiempo aprox.: 2.5 meses)
  - b. Capacitación básica de las herramientas a todas las IES (1 mes)
3. Políticas de seguridad en cómputo
  - a. Generación del documento básico y ad hoc para las IES (3 meses)
  - b. Aprobación y adecuación del documento por y para cada IES (2 meses)
  - c. Aprobación e implementación del documento de políticas dentro de cada IES (tiempo de espera 4 meses).
4. Instrumento de evaluación
  - a. Generación del documento base (2 meses)
  - b. Implementación del instrumento (cada 2 meses)
  - c. Reporte regional del nivel de gestión de la seguridad (cada 2 meses)
  - d. Revisión del contenido del instrumento (cada 4 meses)

Revisar posibles acuerdos de capacitación y colaboración con entes expertos en seguridad como: UNAM-CERT / CUDI-GRUPO de SEGURIDAD / CERT.org.

\*\*\*