

PLAN DE ALCANCE

CLAVE DEL PROYECTO: **CAPACITACIÓN**

NOMBRE DEL PROYECTO: **PROGRAMA DE CAPACITACIÓN INTERNA PARA EL GRUPO RESCCO**

FECHA DE ELABORACIÓN: **ENERO 2008**

ELABORADO LIDER DE PROYECTO: **ARTURO GÓMEZ GARCÍA**

V_o. B_o. COORDINADOR RESCCO: **ARTURO GÓMEZ GARCÍA**

1. DESCRIPCIÓN DEL PROYECTO

Desarrollo e implementación de un programa de capacitación continua en seguridad de cómputo dirigido a los integrantes de la Red de Seguridad en Cómputo Región Centro Occidente, con el objetivo de proporcionar las metodologías y herramientas necesarias para generar una base de conocimiento homogénea y aplicable en los diversos proyectos institucionales.

2. JUSTIFICACIÓN DEL PROYECTO

Ante el dinámico desarrollo de las TIC en las áreas de redes y telecomunicaciones, la seguridad se ha convertido en un punto estratégico a reconocer, para el aseguramiento de la efectividad en los procesos informáticos de nuestras instituciones. Ante tal reto las IES deben permanentemente actualizarse en los temas de seguridad que exigen sus infraestructuras tecnológicas actuales, mediante el uso de conocimientos, métodos, herramientas y mejores prácticas.

3. ALCANCE

Consolidar el grupo de trabajo de la red regional con el fin de estandarizar los conocimientos, compartir experiencias y lograr la implementación de soluciones eficaces en los siguientes aspectos o temas de interés común (ejes propuestos):

- Infraestructura de redes y cómputo
- Antivirus
- Políticas de seguridad
- Seguridad física
- Monitoreo
- Capacitación
- Servicios a través de la red
- Firewall
- Detección de intrusos
- Acondicionamiento de sites
- R&S(Routing & Switching)

PLAN DE ALCANCE

4. OBJETIVO DEL PROYECTO

Consolidar un esquema de seguridad para las redes en cómputo en la región, que nos permitan garantizar su integridad, disponibilidad y la confidencialidad de la información de nuestras instituciones.

5. REQUISITOS

La metodología de seguridad está diseñada para ayudar a los profesionales de la seguridad a desarrollar una estrategia para proteger sus activos primarios.

El proyecto debe contemplar los diferentes servicios de TI que ofrecen las IES de RESCCO, además de incluir claramente ámbito de aplicación, definiciones claras de términos utilizados, esquema de revisión del documento, seguridad física, seguridad humana, seguridad lógica, seguridad logística, sanciones a aplicar en cada caso, salvedades, listado de procedimientos a los que hace mención y los anexos que sean necesarios.

6. FASES DEL PROYECTO

Fase 1:

Planeación: Investigación de los servicios de seguridad en TI ofrecidos en las IES.

Fase 2:

Implementación: Determinar recursos necesarios para ofrecer el curso de capacitación (gestión de hardware, software, etc.)

Fase 3:

Desarrollo: Asegurar la puesta punto de los procedimientos necesarios para la realización de los cursos.

7. ESTRATEGIAS SELECCIONADAS

Diseñar e implementar sistemas estratégicos que incluya la procuración en los siguientes temas:

- Diseño del curso
- Temas a impartir
- Aplicación de conocimientos
- Prácticas
- Instructores
- Participantes

PLAN DE ALCANCE

- Fecha de inicio y duración del curso
- Lugar
- Infraestructura y requerimientos de equipo de cómputo
- Costos
- Manuales y material didáctico
- Diplomas o constancias

8. RESTRICCIONES DEL PROYECTO

Limitaciones para la implementación de este proyecto sería la falta del factor humano, infraestructura o recursos.

9.

FECHA DE INICIO	FECHA DE FIN
Febrero 2008	

NOMBRE Y FIRMA RESPONSABLE DEL PLAN LÍDER DEL PROYECTO	ACEPTACIÓN PARTICIPANTES EN RESCCO LISTA ANEXA	NOMBRE Y FIRMA VoBo COORDINADOR RESCCO

10. ANEXOS

GUADALAJARA, JAL., ENERO DE 2008

PLAN DE ALCANCE

CLAVE DEL PROYECTO: **POLÍTICAS.**

NOMBRE DEL PROYECTO: **CREACIÓN DE DOCUMENTO GUIA PARA LA CREACIÓN DE POLÍTICAS INSTITUCIONALES DE SEGURIDAD EN
CÓMPUTO RESSCO.**

FECHA DE ELABORACIÓN: **DICIEMBRE 2007**

ELABORADO LIDER DE PROYECTO: **PATRICIA MUÑOZ ROMERO**

Vo Bo COORDINADOR RESSCO: **ARTURO GÓMEZ**

1. DESCRIPCIÓN DEL PROYECTO

Generar un documento que sirva a las IES de la región como guía para crear e implantar Políticas Institucionales de Seguridad en Cómputo dentro de las instituciones integrantes de RESSCO.

2. JUSTIFICACIÓN DEL PROYECTO

Gran parte de la base en los trabajos de seguridad en cómputo son las normas que indiquen alcances y limitaciones de la seguridad, buenas prácticas; es importante que quede estipulado lo que se puede hacer en la red y lo que no tanto por parte de los usuarios como por parte de los administradores de la red. Se desea implantar en cada IES la normatividad necesaria para incrementar el nivel de seguridad y que dicho trabajo esté avalado por RESSCO. De esta forma se espera incrementar el grado de sensibilización tanto de los usuarios como directivos de las instituciones respecto de la importancia de la seguridad en cómputo así como con las actividades y planes necesarios para llevarle a cabo.

3. ALCANCE

Se desea obtener un documento normativo básico que contemple los diferentes servicios que las IES ofrecen por medio de la infraestructura en TI. Se contempla también presentar este documento para que lo avale la Secretaria Técnica de Anuies-RCO y presentarlo posteriormente en cada una de las IES buscando la autorización de la aplicación del mismo. Cada IES dará seguimiento al mantenimiento y actualización periódica dentro de su institución con posibles revisiones regionales.

4. OBJETIVO DEL PROYECTO

Lograr la unificación de la normatividad en seguridad en cómputo aplicada en todas las IES participantes de RESSCO como base de los trabajos de seguridad que se realicen tanto a nivel institucional como regional, nacional e internacional.

5. REQUISITOS DEL PRODUCTO PLAN DE ALCANCE

El documento debe contemplar los diferentes servicios de TI que ofrecen las IES de RESSCO, además de incluir claramente ámbito de aplicación, definiciones claras de términos utilizados, esquema de revisión del documento, seguridad física, seguridad humana, seguridad lógica, seguridad logística, sanciones a aplicar en cada caso, salvedades, listado de procedimientos a los que hace mención y los anexos que sean necesarios.

6. ENTREGABLES DEL PROYECTO

Fase 1: Investigación de los servicios de TI ofrecidos en cada IES, investigación de las actividades de riesgo identificadas en las IES = Listado de servicios, por qué y cual es su valor, de quien se desea proteger, y riesgos básicos a nivel regional.

Fase 2: Determinar recursos necesarios para ofrecer cada uno de los servicios listados: hardware, software, recurso humano, \$pólizas/subscripciones/licenciamiento, capacitación, espacios, mobiliario, instalaciones eléctricas, instalaciones de red, instalaciones ambientales, control de uso y acceso, procedimientos de protección contra desastres, obra civil, herramientas necesarias para su construcción y mantenimiento (escalera, taladro, etc.), = Listado de activos generales a proteger, valor intrínseco, costos derivados de su pérdida.

Fase 3: Proponer lineamientos para cada servicio que indique la política necesaria para asegurar la puesta a punto, buenas prácticas, mantenimiento, registro y control del servicio, procedimientos relacionados. = Lineamientos por servicio y listado de procedimientos que han de crearse para ello.

Fase 4: Organización de lineamientos por grupos para identificar los artículos necesarios en el documento. = Documento básico armado.

7. ESTRATEGIAS SELECCIONADAS

Interacción con los responsables técnicos de las IES participantes para obtener información vía correo, mensajero o teléfono en base al directorio actualizado de RESSCO.

Vaciado de información en una matriz, luego enviar a responsables a revisión a nivel regional como verificación.

Definir listado de servicios básicos con el cual se trabaje en el documento.

Interactuar con el equipo de trabajo de POLITICAS en la creación de los recursos en cada servicio para identificar lineamientos necesarios y bajarlos a papel.

PLAN DE ALCANCE

Realizar agrupación de lineamientos y definir organización del documento y listado de procedimientos necesarios.

Presentar término de cada Fase establecida en la lista de correo de RESSCO mediante la documentación de cada una de las fases.

8. RESTRICCIONES DEL PROYECTO

Retraso en la obtención de información de las IES o falta de participación.

9.

FECHA DE INICIO	FECHA DE FIN
Febrero 2008	Abril 2008

NOMBRE Y FIRMA RESPONSABLE DEL PLAN LÍDER DEL PROYECTO	ACEPTACIÓN PARTICIPANTES EN RESSCO LISTA ANEXA	NOMBRE Y FIRMA VoBo COORDINADOR RESSCO

10. ANEXOS

PLAN DE ALCANCE

CLAVE DEL PROYECTO: MONITOREO.

**NOMBRE DEL PROYECTO: CREACIÓN DEL DOCUMENTO GUIA PARA LA RED DE MONITOREO DE SEGURIDAD EN CÓMPUTO
RESCCO.**

FECHA DE ELABORACIÓN: DICIEMBRE 2007

ELABORADO LIDER DE PROYECTO: JAIME OLMOS

VO. BO. COORDINADOR RESCCO: ARTURO GÓMEZ GARCÍA

1. DESCRIPCIÓN DEL PROYECTO

Generar un modelo de referencia para las IES de la región para la creación e implementación de una red de monitoreo de seguridad de las TIC dentro de las instituciones integrantes de RESCCO como apoyo para el correcto funcionamiento de sus operaciones sustantivas.

2. JUSTIFICACIÓN DEL PROYECTO

La carencia de una base de datos informativa respecto al estado actual y futuro de la seguridad, implica que no se tomen las medidas de control correctas en cuanto a emisión de políticas, normatividad, justificación y adquisición de recursos que abonen a la seguridad en cómputo. El contar con una base de información actualizada y de primera mano permitirá una mejor toma de decisión en lo que respecta la gestión de la seguridad que afecten a los activos primarios de la institución.

3. ALCANCE

El alcance está definido en crear un sistema de monitoreo de actividad anómala (virus, malware, etc.) de manera complementaria y en coordinación con UNAM/CERT. Esto comprende la instalación y puesta a punto de un servicio de monitoreo para la región centro occidente. Específicamente en la participación del proyecto: Honeynet como parte de un sistema regional y nacional del registro e identificación de amenazas informáticas y de respuesta temprana.

4. OBJETIVO DEL PROYECTO

Lograr un sistema de captación que represente la actividad anómala de virus y ataques informáticos en la región centro occidente Y coadyuve a

PLAN DE ALCANCE

las IES tener una mejor base informativa para el análisis, control de riesgos y toma de decisión en adquisición y adecuación de su infraestructura de TIC.

5. REQUISITOS DEL PRODUCTO

Ser parte del proyecto honeynet UNAM/CERT <http://www.honeynet.unam.mx>

Un Hardware dedicado y de administración mínima para este proyecto.

6. ENTREGABLES DEL PROYECTO

Fase 1: Instalación de los equipos agentes en cada IES

Fase 2: Recolección de datos

Fase 3: Creación de las vistas de información colectada y procesadas para su consulta de manera total y por IES

Fase 4: Interpretación de datos, tendencias y programas de respuesta temprana a incidentes de seguridad.

7. ESTRATEGIAS SELECCIONADAS

Interacción con el grupo de seguridad de UNAMCERT.

Asesorías en la implementación de sus equipos agentes

Interpretación de datos y correlación de información.

8. RESTRICCIONES DEL PROYECTO

Retraso en la instalación de equipos agentes por parte de las IES o falta de participación.

9.

FECHA DE INICIO	FECHA DE FIN
Febrero 2008	Abril 2008

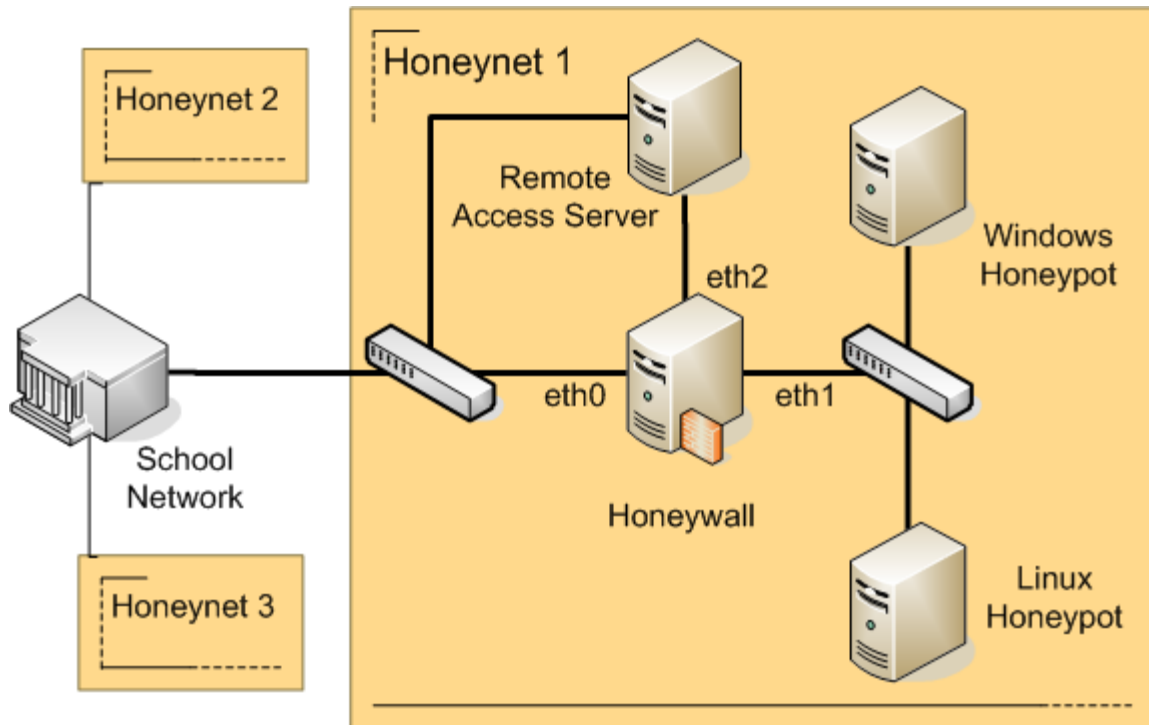
PLAN DE ALCANCE

NOMBRE Y FIRMA RESPONSABLE DEL PLAN LÍDER DEL PROYECTO	ACEPTACIÓN PARTICIPANTES EN RESCCO LISTA ANEXA	NOMBRE Y FIRMA Vo.Bo . COORDINADOR RESCCO

10. ANEXOS

DIAGRAMA BASE DEL SISTEMA DE MONITOREO DE SEGURIDAD.

FUENTE: [HTTP://WWW.HONEYNET.UNAM.MX/ES/PROJECT.PL](http://www.honeynet.unam.mx/es/project.pl)





PLAN DE ALCANCE

CLAVE DEL PROYECTO: **NOC**

NOMBRE DEL PROYECTO: **CREACIÓN DE DOCUMENTO GUÍA PARA LA INSTALACIÓN DE NOCS EN LA IES DE RESSCO**

FECHA DE ELABORACIÓN: **DICIEMBRE DEL 2007**

ELABORADO LIDER DE PROYECTO: **ANTONIO CHÁVEZ GARIBAY**

VO BO ADMINISTRADOR DE PROYECTO: **ARTURO GÓMEZ**

1. DESCRIPCIÓN DEL PROYECTO

Instalación de NOCs en las IES de la región Centro-Occidente de ANUIES

2. JUSTIFICACIÓN DEL PROYECTO

Las redes informáticas se han adquirido una importancia estratégica en las instituciones educativas debido a que a través de ellas se proporcionan los servicios de voz, datos y video, de manera que una falla en las mismas repercute enormemente en las actividades diarias de las áreas académicas y administrativas. La interrupción de las inscripciones, de los procesos financieros, de las actividades académicas y de investigación o de la telefonía pueden causar enormes pérdidas económicas a las IES e incluso originar problemas de tipo político. Por lo anterior es indispensable contar con herramientas que nos permitan minimizar las probabilidades de fallas en las redes, así como detectar oportunamente los eventos que puedan en un momento dado provocar una falla en las mismas.

Por lo anterior, es necesario la habilitación NOCs que cuenten de sistemas para monitorear el estado de la red, la detección y eliminación oportuna de virus, intrusiones y ataques informáticos, así como el consumo del ancho de banda entre otros.

3. ALCANCE

El sistema se instalará en el site principal de las IES y nos debe permitir:

- 1) Monitorear la red en tiempo real para detectar posibles fallas en los enlaces o en los dispositivos principales de la red.
- 2) Monitorear el ancho de banda de los enlaces, de acuerdo a las necesidades de cada IES.
- 3) Detectar y neutralizar amenazas informáticas (virus, ataques, intrusiones, etc.)
- 4) Compartir información con otros NOCs de las IES.



PLAN DE ALCANCE

4. OBJETIVO DEL PROYECTO

Instalar en las IES de RESSCO un sistema que permita monitorear, administrar y supervisar la operación de sus redes de telecomunicaciones y así facilitar la detección y corrección de los problemas físicos y lógicos que se presenten en la misma.

5. REQUISITOS DEL PRODUCTO

Mantener contacto con los otros NOCs de RESSCO a través de un sistema informático que permita compartir información importante.

6. ENTREGABLES DEL PROYECTO

Contar con el software y hardware necesario para monitorear el estado de los enlaces de la red y detectar fallas en el servicio, así como para analizar la utilización de los anchos de banda.

Contar con el software y hardware requeridos para detectar y neutralizar virus, gusanos y ataques informáticos, así como para reducir el nivel de SPAM. Se contará también con una herramienta que les permita a los NOCs de las IES compartir esta información.

7. ESTRATEGIAS SELECCIONADAS

Se sostendrán reuniones por videoconferencia y comunicación por e-mail con los responsables de las IES para conocer sus necesidades y problemática particular.

Los responsables de las IES deberán proporcionar información detallada sobre el avance que han logrado en este aspecto, así como de su red con la finalidad de conocer su estado actual y así poder definir las características que deberá tener el NOC

8. RESTRICCIONES DEL PROYECTO

Falta de interés de las IES, problemas para conseguir los recursos económicos.



PLAN DE ALCANCE

9.

FECHA DE INICIO	FECHA DE FIN

NOMBRE Y FIRMA RESPONSABLE DEL PLAN LÍDER DEL PROYECTO	NOMBRE Y FIRMA ACEPTACIÓN CLIENTE	NOMBRE Y FIRMA VoBo ADMINISTRADOR DEL PROYECTO

10. ANEXOS