Plan de Entrenamiento en Productos Sonicwall

BOGOTA
Octubre 2007

TABLA DE CONTENIDO

1. PRESENTACIÓN DE LA SOLUCIÓN

A continuación, se presentan los temas más relevantes para la organización de la propuesta del entrenamiento en seguridad de la Información de acuerdo con los requerimientos propuestos para la capacitación en productos Sonicwall**:**

- *Dar a conocer conceptos básicos de seguridad de la Información.*
  - *Seguridad en TCP*
  - *Tipos de firewall*
  - *Consideraciones para el diseño de una arquitectura de seguridad*
  - *Concepto de UTM*
  - *Inspección profunda de paquetes (deep packet inspection)*
  - *VPN(IPSEC)*
  - *Sistemas de detección y prevención de intrusos*
- *Presentar temas relacionados con la administración de plataformas tecnológicas y mostrar la importancia del rol de administrador de plataforma en el modelo de seguridad de la entidad, con el fin de garantizar la confidencialidad, integridad y disponibilidad de la información, además de familiarizar al estudiante con los equipos de la solución Sonicwall.*
- *Entrenamiento sobre la importancia de asegurar el correo electrónico.*
- *Entrenamiento sobre soluciones que utilizan aceleradores para aplicaciones tipo WEB utilizando el protocolo SSL.*
- *Conceptos básicos relacionados con firewall y sistemas de detección de intrusos.*
- *Control de contenido y Gateway Antivirus.*
- *Gestion de la plataforma Sonicwall desde browser utilizando http o https.*

1.1 ALCANCE

Duración: *32 Horas*
Dirigido a: *Personal del área de tecnología de la información.*

Cupo máximo: 7 *personas.* (Este es el número recomendable para este tipo de cursos que poseen teoría y practica, y que se quiere generar un cambio en el comportamiento y la forma de realizar las actividades diarias)

Información complementaria*:* Para este curso se entregara una lista de artículos disponibles en Internet, con el fin de familiarizar al estudiante con este tipo información y complementar algunos temas del curso, los cuales serán de lectura obligatoria.

Se busca así a futuro, facilitar el realizar actividades concretas en el área de seguridad informática, tales como procesos de detección y análisis de problemas, análisis de vulnerabilidades, y en general, tener un criterio de decisión, cuando se nos plantee como

implementar controles para mejorar lo que ya se tiene, o el visualizar el mejor camino a seguir, en caso de no presentarse algún incidente de seguridad.

Entonces, resumiendo el curso de seguridad de la información, plantea un análisis crítico de la tecnología (pasado y futuro) junto con una compresión global de los elementos que conforman la arquitectura de los sistemas de seguridad de la información. No siempre los problemas o las soluciones son de tipo tecnológico; este será un tema recurrente durante el recorrido o viaje por el curso propuesto.

Como todos sabemos la tecnología la utilizan seres humanos, y muchas problemas en el tema de seguridad provienen de una falta de conciencia sobre la implicaciones que puede tener el no tener un proceso dentro de la organización orientado a generar un cambio en la conducta, con el fin de lograr unos procesos apoyados por unos procedimientos mas seguros.

Otro tema importante en el desarrollo del curso será el tema asociado a la organización internacional:**Internacional Information Systems Security Certification Consortium (ISC)[2],** y su correlación con el estándar internacional ISO 17799[1]. Este último tema le permitirá a los estudiantes tener una visión total del ambiente informático, considerando las tres variables fundamentales que son: Confidencialidad, Integridad y disponibilidad, con el fin de mejorar el cumplimiento de los objetivos planteados al inicio de este párrafo.

Por ultimo, en la solución Sonicwall se hará un entrenamiento en los comandos principales con el fin de activar funciones asociadas al firewall, IPS, CFS y Gateway Antivirus, Mail security, SSL, con el fin de que el entrenamiento garantice que los futuros administradores de los equipos de seguridad puedan realizar configuración que estén de acuerdo con las condiciones siempre cambiantes propio de los entornos de la red en la actualidad.

[1] . Recomendación Internacional sobre Seguridad informática dentro las organizaciones.

SESION NUMERO 1	
DURACION EN HORAS	**TEMA**
2	*Conceptos básicos en seguridad de la información.* ❖ *ISO 17799/27001* ❖ *COBIT* ❖ *Políticas de Seguridad*
2	*Protocolo TCP/UDP*
1	*Protocolo IPSEC* ❖ *Protocolo ESP, AH.*
1	*Protocolo SSL* ❖ *Ventajas* ❖ *Cifrado en SSL*
2	*Conceptos de: Firewall, IPS, CFS y Gateway antivirus y UTM*

SESION NUMERO 2	
DURACION EN HORAS	**TEMA**
2	*Configuración Firewall*
2	*Configuración Administración del equipo* ❖ *GUI* ❖ *Security Services* ❖ *NTP* ❖ *Packet capture* ❖ *Network* ❖ *WAN* ❖ *Zones* ❖ *Objects* ❖ *NAT* ❖ *DHCP* ❖ *DNS* ❖ *Logs*
1	*Configuración IP del firewall y reglas de seguridad*
1	*Configuración IPS*
2	*Configuración CFS, Gateway Antivirus.*

SESION NUMERO 3	
DURACION EN HORAS	**TEMA**
2	*Conceptos básicos en seguridad correo electrónico.* ❖ *Antispam* ❖ *Antiphising* ❖ *Auditing* ❖ *Antivirus* ❖ *Cumplimiento politicas*
2	*Comandos principales Mail Security* ❖ *CLI*
1	*Protocolos asociados*
1	*Conceptos sobre configuración de la solución SSL* ❖ *SSL overview* ❖ *Management interface* ❖ *Tab configuration* ❖ *Network tab configaration* ❖ *Portal tab configuration*
2	*Conceptos en la configuración de VPN*

SESION NUMERO 4	
DURACION EN HORAS	**TEMA**
2	*Configuración firewall* ❖ *Práctica con equipos*
2	*Configuración IPS* ❖ *Sesión práctica*
1	*Configuración Mail security* ❖ *Sesión Práctica*
1	*Configuración SSL VPN* ❖ *Sesión Práctica*
2	*Configuración VPN* ❖ *Sesión Práctica*

1.2 METODOLOGIA

Para el desarrollo del entrenamiento se tendrán conferencias magistrales, ejercicios prácticos y una evaluación al finalizar el entrenamiento con el fin de medir el nivel de conocimiento por parte de los asistentes.

1.3 ENTREGABLES

Los entregables del proyecto son los siguientes:

- Conferencias con los temas referenciados
- Material de las presentaciones en PDF
- Casos de estudio.
- Artículos sobre los temas propuestos.

2. CONDICIONES COMERCIALES

2.1 Precios

El costo del servicio se muestra desglosado para cada uno de los items.

Descripción	Precio $COL
Entrenamiento Seguridad 32 horas	
Preparación material curso para entrega cliente (se factura una vez)	

* Los precios anteriores no incluyen el IVA.

2.2 Forma de Pago

Cincuenta por ciento (50%) del valor total del proyecto a manera de anticipo apenas se firme y perfeccione el contrato, para iniciar la logística del curso relacionada con la preparación de los equipos para la sección práctica y preparación de material complementario, y material a ser entregado a los asistentes.

Cincuenta por ciento (50%) restante del valor total 5 días terminado el curso.

La preparación del material se debe contratar por adelantado y se requieren al menos 15 días para su impresión para los estudiantes.

2.3 Validez de la oferta

Sesenta (60) días a partir de la fecha de presentación.

RODRIGO FERRER VELÁSQUEZ

CISSP

BS 27001 LEAD AUDITOR

CISA examen aprobado

Carrera 24ª N° 152-42 APTO 209

Teléfonos: Celular: (310)2234533

Residencia 6153896

Bogotá, D.C.

e-mail: rferrer@cable.net.co

CONSULTOR EN TECNOLOGÍAS DE INFORMACIÓN

RESUMEN

Experiencia en el sector de las telecomunicaciones, trabajando con compañías lideres en fabricación de tecnología, como es el caso de 3Com Corporation, Sonicwall y Extreme Networks. Este desarrollo se ha hecho en un proceso de aproximadamente 10 años, donde he logrado adquirir experiencia tanto en el área técnica, como comercial y finalmente en procesos de Consultoría, experiencia tanto a nivel nacional, como internacional permitiéndome así, lograr un manejo integral de todo el proceso, que va desde la creación del negocio, hasta su implementación.

Entre los temas de interés que en este momento estoy investigando se encuentran:

- Metodologías de planes de continuidad del negocio.
- Manejo de incidentes
- Auditoria 27001
- Recuperación ante desastres.
- Gestión de redes.
- Seguridad Física.

EXPERIENCIA LABORAL

SISTESEG. 2002 – a la fecha

Gerente Técnico. 2002 – a la fecha

Sonicwall. (www.sonicwall.com) **2004-2005**

- *Diseño de Soluciones.*
- *Entrenamiento a canales.*
- *Manejo de Proyectos.*
- *Capacitación usuario final.*
- *Realización eventos en USA y Sur América.*
- *Implementación de Soluciones tipo VOIP.*
- *Proyectos de asesoría y consultoría a nivel regional en el área de infraestructura y seguridad informática.*

Extreme Networks. (www.extremenetworks.com) 2000 - 2001

2000 –2001

System Engeniering. 2000 –2001

- *Diseño Soluciones Grandes Proyectos*
- *Manejo de canales de distribución.*
- *Entrenamiento a Canales*
- *Manejo de Proyectos.*
- *Capacitación usuario final.*
- *Realización eventos en USA y Sur América.*
- *Recomendaciones diseño de algunos equipos.*

3Com Corporation. (www.3com.com) 1996- 2000

- *Diseño de Soluciones.*
- *Entrenamiento a canales.*
- *Manejo de Proyectos.*
- *Capacitación usuario final.*
- *Realización eventos en USA y Sur América.*
- *Implementación de Soluciones tipo VOIP.*
- *Proyectos de asesoría y consultoría a nivel regional en el área de infraestructura y seguridad informática.*

EXPERIENCIA EN CONSULTORIA Y ASESORIA

Diseño y Asesoría red Nacional Skandia.

Diseño y asesoría red Nacional ECOPETROL (Trabajo realizado en conjunto con 3Com Corporation).

Diseño y asesoría red EsSalud Perú (Trabajo realizado en conjunto con 3Com Corporation).

Diseño y asesoría red Poder Judicial Perú (Trabajo realizado en conjunto con 3Com Corporation).

Diseño y asesoría arquitectura de seguridad Agrícola de Seguros.

Diseño y asesoría arquitectura de seguridad SISTESEG.

SGSI Procuraduría General de la nación

SGSI Telefónica-Telecom

EXPERIENCIA DOCENTE

UNIVERSIDAD AUTONOMA BUCARAMANGA.
UNIVERSIDAD DEL NORTE.

- Profesor asignatura de la Especialización en redes.
- Gestión de redes.
- años en el proceso hasta la actualidad.

FUNDACION UNIVERSITARIA DE BOYACA.
UNIVERSIDAD DE ANTIOQUIA.
ASESOR PROYECTOS DE GRADOS UNIVERSIDAD DE LOS ANDES.

- Gestión y administración de redes.
- Software de apoyo al diseño de redes.
- Simulación en redes.
- Diseño de software de gestión en redes de alta velocidad.

ESTUDIOS REALIZADOS

Educación Continuada Universidad de los andes	*2004*
***Educación continuada (History of Science and technology**) Cambridge UK*	*2000*
***Especialista en Telemática**, Universidad de los Andes, Bogotá*	*1995*
***Gerencia de Sistemas de información**, Universidad de los Andes.*	*1999*
***Ingeniero eléctrico**, Universidad de los Andes, Bogotá*	*1987*
***Bachiller Académico**, Colegio Champagnat.*	*1981*