

Conferencias

Inseguridad de los sistemas de información (Conferencia Internacional)

Jesús Vásquez (México)

Los sistemas se han desarrollado durante décadas y en el mejor de los casos la seguridad se ha considerado en las etapas finales del diseño: en la mayoría de estos casos la seguridad es considerada como una corrección a los desarrollos en operación, después de detectarse algún problema. Entre estos figuran desde el viejo "stack overflow", el manejo de información confidencial en sistemas no confidenciales, uso de protocolos de comunicación inseguros, hasta la ausencia total de consideraciones de seguridad en el ciclo de vida de desarrollo de software.

El oficial de seguridad informática:

Coordinador de la gestión de seguridad de la información.

Andrés Almanza

La seguridad y protección de la información requiere de esfuerzo, disciplina, dedicación y constancia, para darle un orden lógico y engranar todas las piezas. El oficial de seguridad de la información será pieza clave para que nos ayude a articular un programa de seguridad y protección de la información dentro de la organización.

El análisis de riesgos: La base para el Sistema de Gestión de la Seguridad de la Información. Caso Magerit

Armando Carvajal

Los riesgos son la base misma de la gestión de seguridad de la información. Establecer estrategias metodológicas para adelantar su identificación, análisis y tratamiento es factor fundamental para una adecuada gestión de los mismo. Esta charla presentará un caso práctico de este tipo de análisis utilizando el discurso metodológico MAGERIT.

Gestión de Vulnerabilidades Informáticas

Astrid Pereira

La gestión de la seguridad de la información exige la validación permanente de la inseguridad de la información y el seguimiento de las fallas. Se presentará una reflexión sobre cómo se adelanta una gestión de vulnerabilidades, puntos críticos y riesgos propios de esta labor inherente a la gestión de seguridad de la información

Gestión de la inseguridad de las aplicaciones: Un enfoque práctico

Felipe Silgado Quijano

Un sistema de gestión de seguridad de la información (SGSI), debe abarcar la gestión de seguridad de las aplicaciones, como otro proceso core. Esta presentación muestra la problemática actual de la gestión de seguridad de aplicaciones y expone una propuesta innovadora y práctica para mitigar esta problemática.

Gestionando una Plataforma de VoIP Segura

Giovanni Cruz

Las plataformas de Voz sobre IP establecen un nuevo elemento para incorporar dentro de la gestión de seguridad. Esta charla presenta los elementos clave de la gestión de una plataforma de VoIP y las acciones que se deben adelantar para su aseguramiento.

ITIL: Un soporte para el SGSI basado en ISO 27001

Javier Díaz Evans

Esta presentación busca explorar y analizar las buenas prácticas de ITIL como apoyo a la gestión de seguridad de la información, basada en las buenas prácticas sugeridas por el ISO27001.

Métricas en Seguridad Informática: Una revisión académica.

Jeimy J. Cano

El medir generalmente es una necesidad en las organizaciones para establecer directrices y decisiones. Esta presentación revisa tres propuestas internacionales sobre métricas de seguridad, para concluir con sugerencias prácticas y orientaciones para adelantar el desarrollo de mediciones e informes de gestión de seguridad de la información

ISM3, Aplicado a la Implantación de ISO27001.

Juan Carlos Reyes

Marco general de madurez de la seguridad informática en las organizaciones alineada con las estrategias de negocio. ISM3, es una iniciativa en la cual se suman muchos esfuerzos de profesionales de la seguridad, académicos y la industria para proponer alternativas que procuren una mejor gestión de la seguridad de la información.

CobiT como promotor de la seguridad de la información. Hacia el Gobierno de TI.

Lucio Molina

Dentro de las buenas prácticas internacionales en gestión de TI, COBIT se resalta como una de las más referenciadas y utilizadas. En esta presentación se desarrollará una estrategia que permita promover la gestión de la seguridad de la información a partir de las características y procesos detallados en esta buena práctica.

Razones por las cuales se debe contar con una planeación adecuada de Continuidad de Negocio

Pedro Romero

El tener un plan adecuado asegura que su negocio ante un evento sufra un impacto mínimo de interrupción y tenga la capacidad de seguir operando. No sólo se trata de proteger los datos y la infraestructura tecnológica, sino también la integridad de sus empleados en caso de un desastre y que estén capacitados para garantizar la reanudación de sus tareas.

Leyes y contratos: Son útiles frente a una inseguridad informática?

Rafael Gamboa

¿Qué pasa cuando la inseguridad se materializa? La charla busca presentar al auditorio las herramientas legales y jurídicas que hay, haciendo énfasis en la utilidad o efectividad de las normas en el mundo de la inseguridad Informática.

Modelos de Madurez para seguridad informática

Roberto Arbeláez

Los modelos de gestión de seguridad informática evolucionan y está en cada gerente o responsable de seguridad hacerlo madurar conforme a la realidad de su organización y las tendencias internacionales. Esta charla revisará modelos actuales de madurez en seguridad informática, para establecer puntos de diagnóstico y control en el proceso de gestión.

Protegiendo Sus Ingresos Con Protección de Software y Licenciamiento

Tom Ybarra (México)

Se mostrarán las nuevas tendencias en licenciamiento de software, asegurando que cada copia de software que exista, sea legal y controlada. La charla se dirige a quienes deseen conocer sobre las últimas y más avanzadas técnicas de protección y activación de software; así como de las mejores prácticas para salvaguardar la propiedad intelectual.

Planeación Estratégica de Seguridad

Wilmar Castellanos

Esta charla busca establecer referentes básicos de planeación estratégica de la seguridad alineada con las exigencias del negocio, sustentado en experiencias aplicadas de uso con el fin de sugerir elementos prácticos que permitan adelantar este proceso en las organizaciones.



Introducción

La inseguridad informática como propiedad inherente de los diferentes elementos que conforman los diseños de seguridad de la información, es un referente necesario, pero nunca suficiente para comprender que tan seguros podemos llegar a ser. Sin un conocimiento detallado de cómo surge la inseguridad, cómo se diagnostica y cómo se gestiona, pocas oportunidades tendremos para avanzar en la búsqueda de propuestas y alternativas ajustadas y coherentes con la dinámica misma de los desarrollos tecnológicos, la evolución de las vulnerabilidades y con el ambiente globalizado del cual somos partícipes.

En este escenario, las Jornadas Nacionales de Seguridad Informática ACIS 2008 abren un espacio para la reflexión y análisis de experiencias, ideas, prácticas y actividades relacionadas con la gestión de la seguridad de la información, como una excusa académica y un ejercicio corporativo para avanzar en una cultura de seguridad informática más sólida, en un compromiso más serio y formal de todos nosotros y sobre manera, en un mensaje alineado y común para todos aquellos que buscan respuestas prácticas para descubrir los mitos y realidades de la Gerencia de la Seguridad de la Información.

Andrés R. Almanza, M.Sc. (c)

Jeimy J. Cano, Ph.D, CFE

Coordinadores Académicos

VIII Jornada Nacional de Seguridad Informática

Juni o 18, 19 y 20 de 2008

Centro de Convenciones

Biblioteca

Luis Ángel Arango

Cal le 11 No 4-14, Bogotá, D.C.



Conferencistas

Jesús Vásquez (México)

Egresado de la ESIME-IPN en la Especialidad de Electrónica. Maestro en Ciencias en Ingeniería Electrónica del CINVESTAV-IPN. Especialista en Redes de Computadoras en la Escuela Superior de Electricidad en Francia. Doctor en Informática de la Universidad de Rennes I, Francia. Profesor del CINVESTAV-IPN en la sección de computación y Profesor Asociado en la UAM-Azcapotzalco, así como Catedrático del ITESM. Actualmente es el titular de la Oficina de Seguridad Informática del Banco de México.

Andrés Almanza

Ingeniero de Sistemas, Universidad Católica de Colombia. Especialista en Seguridad de Redes de la Universidad Católica de Colombia. Candidato a Magister de Seguridad Informática de la Universidad Oberta de Cataluña, España. Certificación LPIC1, Linux Professional Institute. Oficial de Seguridad Informática de la Cámara de Comercio de Bogotá.

Armando Carvajal

Ingeniero de Sistemas, Universidad INCCA. Postgrado en Construcción de Software para redes, Universidad de los Andes. Maestría en Seguridad de la Información, Universidad Oberta de Cataluña, España. Gerente de consultoría de la empresa GlobaltekSecurity. Actualmente escribe artículos sobre seguridad de la información para la revista hakin9.

Astrid Pereira

Ingeniero de Sistemas, certificada MCSE + Security, CIW, CIW E-commerce designer, Comptia Security + Certified, Comptia Network+ Certified Trainer certified. Socio Fundador de Creangel Ltda. Consultor en la Superintendencia Financiera de Colombia, El Banco de la República, El DNP, La empresa de Acueducto, Compensar, El Espectador y "G4s" entre otras.

Felipe Silgado Quijano

Ingeniero de Sistemas, Universidad Javeriana. Certificado CISSP, CISM, Auditor Lider ISO 27001, ITIL Foundation y ABCP. Actualmente es Gerente de NOC-SOC en Desca Colombia. Oficial de Seguridad en compañías del sector financiero y Consultor en compañías que prestan servicios de seguridad de la información

Giovanni Cruz

Consultor experto con mas de 3 años de experiencia en pruebas de vulnerabilidad, hacking etico y análisis de riesgos y vulnerabilidades. Actual director de Digisert y Lider del proyecto Condor Labs. Certificado CEH en pruebas de penetración y hacking ético y GSEC en aspectos generales de seguridad. Docente de posgrado en la Universidad Católica.

Javier Díaz Evans

Ingeniero Electrónico y Especialista en Telemática, Universidad de los Andes. Certificación CISM Certified Information Security Manager ISACA. CISSP Certified Information Systems Security Professional ISC2. Auditor Lider BS7799 BSI. Consultor Lider del area de Technology Risk Services de PricewaterhouseCoopers.

Jeimy J. Cano

Ingeniero y Magister en Ingeniería de Sistemas y Computación, Universidad de los Andes. Doctor en Filosofía (Ph.D) de Newport University, USA. Examinador de Fraude Certificado (CFE) y Miembro de la High Technology Crime Investigation Association HTCIA. Profesor e investigador en derecho informático y evidencia digital de la Facultad de Derecho de la Universidad de los Andes.

Juan Carlos Reyes

Ingeniero de Sistemas, Universidad del Valle, ex-director del Centro Linux de la misma universidad. Actualmente es CCSA de CheckPoint, GCFA (GIAC Certified Forensic Analyst) del SANS Institute, iBS 7799 Lead Auditor del British Standard Institute especializándose en análisis de vulnerabilidades y computación forense.

Lucio Molina

Ingeniero de Sistemas, especialista en Auditoría de Sistemas, certificación CISA, acreditación Cobit, certificación de ITIL ESS y CISM. Experto en seguridad informática, auditoría de sistemas, gerencia de proyectos y diseño y desarrollo de sistemas. Fue vicepresidente internacional de ISACA y del ITGI. Actualmente es miembro del IT Governance Committee, miembro de ISACA, de la ISSA y de la ALIFC.

Pedro Romero

Administrador de Sistemas de Información de la Universidad Jorge Tadeo Lozano y posgrado en Alta Gerencia de la Universidad de Los Andes. Más de 20 años de experiencia, trabajando con Redes y Comunicaciones, Gerencia de Proyectos, Seguridad de la Información y Continuidad de Negocio. Consultor certificado por el DRIL y CISM por ISACA.

Rafael Gamboa

Abogado de la Universidad Javeriana de Bogotá, Master en Tecnologías de la Información y Privacidad, Master en Propiedad Intelectual. Miembro del Grupo de Estudios de Comercio Electrónico, Tecnología e Internet -GECTI- de la Universidad de los Andes. Actualidad ejerce como Abogado en Bernate & Gamboa Abogados y como Consultor del Banco Mundial.

Roberto Arbeláez

Ingeniero y Magister en Ingeniería de Sistemas y Computación de la Universidad de los Andes. Experiencia en Seguridad de la Información, Computación Forense, Administración de Riesgos, Operaciones de TI, Auditoría de TI y planeación estratégica de TI. Experto en Estándares y mejores prácticas de TI. Certificaciones CISSP, CISA, COBIT entre otras.

Tom Ybarra (México)

Administrador de negocios por la Universidad del Estado de California. Creador de una de las llaves de protección, lanzada al mercado en el año 2005 por la firma Safenet, también fungió como gerente de producto de Sentinel. Desde el año 2006 es gerente de cuentas mayores de la firma Safenet para las Américas, donde ayuda a identificar cuáles son las tendencias y el futuro del Digital Rights Management.

Wilmar Castellanos

Ingeniero de Sistemas, Universidad Nacional. Auditor Certificado CISA. Miembro de ISACA. Experto en evaluación de seguridad informática y riesgos de tecnología, generando recomendaciones de seguridad y control, considerando sistemas operativos, redes e Internet, bases de datos, sistemas de información y ERPs. Actualmente es Gerente ERS de Deloitte & Touche.

INSCRIPCIONES

		DESCUENTO POR PAGO HASTA MAYO 16
Miembros de ACIS al día en sus cuotas	\$555.000 + IVA	\$487.000 + IVA
Particulares	\$675.000 + IVA	\$590.000 + IVA
Estudiantes de Pregrado ACIS (cupó limitado)	\$370.000 + IVA	\$340.000 + IVA
Estudiantes de Pregrado (cupó limitado)	\$440.000 + IVA	\$370.000 + IVA

*IVA 16%.

Descuentos adicionales por grupos de la misma empresa, entre 3 y 6 participantes se otorga el 5% de descuento y 7 o más tendrán un descuento del 10%, quienes se encuentren interesados pueden diligenciar y enviar la siguiente información vía e-mail a: jornadaseguridad@acis.org.co ó al Tel-fax 6161407, 6161409, 6350745, 6350747, ó enviarla a la Calle 93 No.13-32 Oficina 102:Nombres, E-mail, Empresa, Cargo, Dirección, Teléfono, indicar si es miembro de ACIS, (Si el pago es corporativo enviar carta de presentación de la empresa).

FORMA DE PAGO:

Cancelar en efectivo o tarjeta de crédito en las instalaciones de ACIS (Proporcionamos mensajería sin costo.) ó consignar en la cuenta de ahorros Bancolombia Cta. No. 2098-4902095 ó de BBVA Cta. No. 025 0200213257. Enviar comprobante original a ACIS.

PREJORNADA Junio 17 de 2008

Tutorial " Gestión del Equipo Responsable de la Seguridad de la Información "

Instructor: *Jesús Vásquez (México)*

Duración: 8 horas

Contenido

1. Arquitectura de SI
2. Alcance y expectativas de SI
3. El enfoque de la ISO
4. El enfoque del NIST
5. Establecimiento de controles
6. Seguimiento

VALOR INSCRIPCIÓN

		DESCUENTO POR PAGO HASTA MAYO 16
Miembros de ACIS al día en sus cuotas	\$180.000 + IVA	\$170.000 + IVA
Particulares	\$290.000 + IVA	\$270.000 + IVA

*IVA 16%.



Calle 93 No. 13 32 Oficina 102
Teléfonos 6161407 - 6161409
Bogotá, Colombia
www.acis.org.co