

PRIMER CONVERSATORIO NACIONAL EN SEGURIDAD DE LA INFORMACIÓN

Se consolida la carrera de Seguridad y Auditoría Informática



Ing. Hernán Salas Asencios; Ing. Raúl Silva; Lic. Alejandro Guerrero; Christopher Hafer; Dr. Erick Iriarte; Ing. Antonio Santiago; Ing. Frano Capeta Mondoñedo; Jaime Honores; Ing. Omar Neyra; Nancy Vilchez, e Ing. Yvanna Quijandria.

La necesidad de establecer una política nacional de seguridad de la información y de aplicar un plan de contingencias sobre la base de una toma de conciencia de los riesgos por intrusiones, virus y hackers, señalaron expertos, investigadores y especialistas durante el Primer Conversatorio Nacional en Seguridad de la Información.

Este evento académico y científico fue organizado en forma conjunta por la Facultad de Telecomunicaciones y Telemática de la Universidad Tecnológica del Perú, UTP, y la empresa Information Security Inc, ISEC, y se desarrolló en el auditorio "Madre de Dios" de la universidad el jueves 19 de febrero. En la reunión participaron el ingeniero Frano Capeta Mondoñedo, director regional de ISEC; el ingeniero Raúl Silva, funcionario de la División Nacional de Alta Tecnología del Ministerio del Interior, DIVINDAT; el funcionario Jaime Honores, director

general de Tecnologías de la Información del Ministerio de Vivienda; el experto Christopher Hafer; el ingeniero Omar Neyra, instructor de ISEC, el doctor Erick Iriarte, representante de la ONG Alfa Redi; y el ingeniero Jaime Suárez, representante del Ministerio del Interior.

La cita fue presidida por el rector de la UTP, doctor Enrique Bedoya Sánchez; el vicerrector Académico, magister Marcial Solís Vásquez; el decano de la Facultad de Ingeniería de Telecomunicaciones y Telemática, ingeniero Hernán Salas Asencios, y el decano de la Facultad de Ciencias de

la Comunicación, licenciado Alejandro Guerrero. Al inaugurar el evento el ingeniero Hernán Salas manifestó que la seguridad de la información es un tema sumamente importante porque implica la garantía y la protección de esos contenidos y que por ello se ha querido reunir a especialistas, investigadores y expertos para tratar esta materia.

Anunció que precisamente la creación de la nueva carrera de Ingeniería de Seguridad y Auditoría Informática, que ha puesto en marcha la universidad, tiene como soporte un convenio que se acaba de suscribir



con la empresa ISEC, que tiene gran prestigio y experiencia internacional en este campo. Fue moderador del evento el licenciado Alejandro Guerrero e intervinieron como panelistas el ingeniero Omar Neyra, el ingeniero Javier Suárez, el doctor Erick Iriarte y el ingeniero Antonio Fernández.

Buenas prácticas en seguridad

El primer tema del conversatorio fue ofrecido por el ingeniero Frano Capeta y se refirió a las "Buenas Prácticas de la Seguridad de la Información"

En su exposición, el ingeniero Capeta manifestó que la seguridad informática implica tres conceptos básicos que son: la integridad de la información que significa no poder modificarla, la confidencialidad que supone que solo puede ser modificada por la persona autorizada, y la disponibilidad para que pueda ser utilizada cuando sea necesario.

Entre las buenas prácticas para proteger la información recomendó no dar el "password" a ninguna otra persona, guardar la información importante en "back-up" y sobre todo tomar conciencia del gran valor de la

información más significativa de una

empresa frente a riesgos o uso indebido por parte de terceros.

Sin embargo, señaló que las amenazas a la confidencialidad y seguridad de la información generalmente provienen de los mismos empleados disconformes de la empresa, la baja concientización de la seguridad y el crecimiento de las redes.

En tal sentido, indicó que a través del Google encontramos un Manual del Hacker que puede ser operado por cualquier persona medianamente capacitada que puede vulnerar los sistemas de seguridad y protección.

Frente a este problema, manifestó que es necesario reconocer que no existe seguridad absoluta porque hay métodos muy extendidos como el "Trashing" o búsqueda en la basura y la ingeniería social, que es la forma ingeniosa de obtener por relaciones o peticiones sorpresivas para romper la confidencialidad en las comunicaciones.

Como conclusión, señaló que lo más importante es tener siempre presente la importancia de la seguridad de la información y tomar conocimiento de los nuevos métodos de intrusión en las telecomunicaciones para aplicar las medidas necesarias de protección.

Penas por delitos informáticos son muy leves

En diálogo con los panelistas, el ingeniero Capeta dio a conocer que los países que han avanzado más en la seguridad informática en esta región son Brasil, Argentina y Chile y que en segundo término se encuentran Perú y Colombia, donde falta un largo trecho para alcanzar un nivel óptimo. Señaló que los sectores empresariales que ofrecen mayores garantías de seguridad en el Perú son la banca, los seguros y los registros públicos.



También insistió que mantener la información importante y confidencial en un lugar seguro o "back-up". Es una medida de garantía que libró a muchas empresas de pérdidas y riesgos significativos.

En relación con los delitos informáticos, el doctor Erick Iriarte señaló que la ley considera penas que van de cuatro a ocho años según la gravedad. Pero estimó que resultan muy benignas ya que casos tan graves como el del "chuponeo" o de los llamados "petroaudios" podrían tener sanciones leves. Agregó que a pesar de la ley, en el Perú no hay ningún sentenciado y en Brasil, sin ley sobre seguridad informática, hay ocho mil sentenciados.

El ingeniero Capeta opinó que el mundo virtual, por el acceso libre a Internet, no tiene fronteras y no está limitado y que en el ejercicio de la libertad de información frecuentemente se incurre en excesos y delitos a través de este medio universal de comunicación.

"Clonación" y "Fishing" por Internet

La segunda conferencia fue sustentada por el ingeniero Raúl Silva, experto de la Policía Nacional, quien desarrolló el tema titulado: "¿Cómo evidenciar el mal uso de la información?".

Manifestó que este es un asunto que tiene que ver con la seguridad de la información y que el punto más débil resulta siendo el propio usuario quien muchas veces no se da cuenta hasta el final que es víctima de un engaño o una estafa.

Afirmó que si bien el código penal peruano tipifica tres tipos de delitos informáticos, el uso de códigos maliciosos de todo tipo, la "clonación" de tarjetas de crédito, las ofertas de equipos como laptops por un depósito bancario y el "fishing", método por el que se pide el número de la tarjeta de crédito por un supuesto premio, son algunas formas de uso malicioso de la información.

En el diálogo con los panelistas el ingeniero Silva reconoció que muy pocos casos de delitos informáticos se judicializan y que por el secreto de las comunicaciones es difícil muchas veces llegar a los autores por lo que recomendó tomar conciencia de la real importancia que tiene la seguridad de la información en estos nuevos medios virtuales de la información.

La tercera conferencia sobre "Seguridad en redes inalámbricas", estuvo a cargo del experto y empresario Christopher Hafer, quien ofreció una serie de ejemplos de los trabajos realizados en diferentes empresas. Dijo que estas son abiertas en un 96 por ciento por lo que señaló la necesidad de establecer una plataforma de seguridad para las comunicaciones inalámbricas.

Afirmó, sin embargo, que las señales inalámbricas son más fáciles de capturar y vulnerar, pero en general consideró que hasta la seguridad en los bancos es realmente muy baja para los



Alumnos de la UTP, empresarios y autoridades durante el Primer Conversatorio de Seguridad de la Información.



Ing. Frano Capeta; Ing. Raúl Silva; Dr. Enrique Bedoya Sánchez; Jaime Honores, y Christopher Hafer.

estándares en este campo por lo que recomendó tomar todo tipo de prevención para evitar los riesgos naturales en este tipo de operaciones.

Implementan Comités de Seguridad en Información

El ingeniero Jaime Honores, director general de Tecnologías de la Información del Ministerio de Vivienda, trató el tema titulado: "Iniciativas por parte del gobierno peruano en la seguridad de la información".

En forma general sostuvo que es necesario que todas las instituciones tomen conciencia de la importancia de establecer políticas nacionales de seguridad y que, al existir la norma 17799 del año 2004 que regula la seguridad de la información, se comience a implementar su contenido en forma práctica.

Al respecto, dio a conocer que en el Ministerio de Vivienda se ha constituido un Comité de Seguridad de la Información para establecer los riesgos. Dijo que como funcionario técnico de un organismo del Estado debe establecer una política de seguridad

y luego iniciar la sensibilización sobre este asunto con la persona de la más alta responsabilidad y decisión de su participación para comenzar a trabajar en ese campo. Señaló que el marco legal les obliga a implementar este sistema para establecer una política de seguridad de la información que contenía un plan de contingencias, un programa de capacitación y luego proceder a la organización del Comité de Seguridad para que lleve adelante las acciones concretas.

En diálogo con los panelistas se llegó a la conclusión que como consecuencia de la aplicación de estas acciones ya se están implementando normas de confidencialidad en los contratos y que otras medidas se aplicaran en general con el objeto de conseguir buenos resultados.

Tecnología con sentido humano y ético

El evento fue clausurado por el rector de la UTP, doctor Enrique Bedoya Sánchez, quien expresó su satisfacción porque el objetivo de este certamen se ha logrado plenamente al haber generado un espacio y la oportunidad de conocer en la opinión de

los expertos la trascendencia de la aplicación de normas de seguridad informática. Consideró que es sumamente importante crear conciencia y plantear alternativas de solución para el país en este campo. Dijo que el segundo objetivo del evento también se ha cumplido pues la universidad presenta su carrera de Ingeniería en Seguridad y Auditoría Informática.

Sostuvo que toda tecnología debe ser aplicada desde una perspectiva estrictamente humana ya que las soluciones se dan desde una gestión estratégica gerencial. Por lo tanto consideró, que la búsqueda de soluciones en la seguridad informática es un problema de hombres donde juega un rol importante no solo la capacidad sino la conciencia y la ética para aplicar las tecnologías más adecuadas.

Luego de clausurar el evento todos los expositores y panelistas recibieron sus certificados de participación con un agradecimiento especial de la universidad.