

HÉCTOR JARA

Sr. Security Consultant @ VerSprite

 @JaraHector

 <http://linkd.in/qfFC0m>

Por más de 12 años se ha desempeñado como Consultor en Seguridad de la Información, enfocándose en los últimos años en GRC (Gobierno, Gestión de Riesgo y Cumplimiento), con sólidas bases en el framework ISO 27.001, PCI-DSS y regulaciones de Privacidad de Latinoamérica.

Durante este tiempo ha prestado servicios a empresas de distintas industrias, entre las que destacan banca, finanzas, seguros, gobierno, educación, tecnología, salud y ONGs/sin fines de lucro.

Apasionado por la Educación, cuenta con más de 10 años de experiencia docente, dictando cursos en instituciones especializadas en tecnología y en carreras universitarias, siendo el profesor titular de la materia Seguridad de la Información en la Universidad Nacional de Quilmes.

Ha dictado diversas conferencias, tanto profesionales como académicas y ha escrito numerosos artículos para publicaciones nacionales e internacionales.

También es coautor de los libros Ethical Hacking, Hackers al descuberto y Ethical Hacking 2.0, todos publicados por Users entre 2009 y 2012.

Adicionalmente colabora activamente y forma parte del board del capítulo Argentino de la Sociedad de Educación del IEEE.

Héctor es Ing. En Telecomunicaciones por la Universidad Argentina de la Empresa, ha realizado un Posgrado en Desarrollo Gerencial en la Universidad de Palermo y una Especialización en Educación y Nuevas Tecnologías en FLACSO.

Adicionalmente ha obtenido las certificaciones CISSP, ISO 27.001 Leader Auditor, CEH y QCS.

También participa activamente como voluntario dando charlas sobre privacidad y concientización en el buen uso de Internet y Redes Sociales para niños, adolescentes y padres.

Actualmente reside en Panamá y presta servicios a la consultora norteamericana VerSprite, LLC como Sr. Security Consultant.

¿Por qué participar en el CIBSI / TIBETS?

Porque logra combinar un perfil académico y a la vez enfocado en la realidad del mercado de seguridad que lo diferencia de otros eventos.

En su opinión, ¿cuál es la relevancia

de su investigación en este Congreso?

El trabajo que realizamos es una extensión del proyecto MESI que se llevó adelante en España, pero hacia Centroamérica. Relevamos Universidades para identificar que contenidos de seguridad se están dando, donde, en que modalidad, etc. Si bien está en una etapa muy temprana de desarrollo, esperamos poder aportar a su evolución, de hecho ya entramos en contacto con gente de Perú para extender el proyecto también allí.

¿Cuál piensa que será el devenir de la Seguridad de la Información?

Las tendencias como IoT y Big Data, sumado al amplio desarrollo de las tecnologías y servicios basados en la nube, si bien ofrecen excelentes beneficios también incorporan nuevos riesgos relativos a la seguridad y a la privacidad. Hace tiempo que el concepto de perímetro de seguridad asociado a las redes de comunicaciones es difuso, la tendencia es que la gestión de la identidad y accesos de los usuarios sea el nuevo perímetro y es una de las claves para los próximos años.

Desde un punto de vista más general, creo que el avance de las regulaciones y la influencia sobre el gobierno corporativo también empieza a jugar un papel importante, dando lugar a la transición entre cumplir "para cumplir con las regulaciones" a una posición más madura de cumplir para tener gobierno y gestión de los riesgos en beneficio de la compañía.

¿Cuál es el mayor riesgo que tiene una sociedad como la Iberoamericana en materia de ciberseguridad?

Desde el punto de vista de las personas, la pérdida de privacidad y el robo de identidad son los mayores riesgos. Las herramientas tecnológicas para identificar a una persona con pocos datos que en

principio pueden parecer inofensivos son una realidad, mientras que la tecnología para proteger su privacidad no se desarrolla ni implementa al mismo ritmo. Conceptos como el "Privacy by Default" deberían ser tenidos en cuenta al momento de desarrollar nuevas regulaciones y actualizar las legislaciones existentes.

Desde el punto de vista de las organizaciones, los números del cibercrimen no dejan de crecer y desde hace varios años que no solo se enfocan en grandes empresas, sino también en medianas y pequeñas. Incluso las Start-Ups son objetivos cada vez más interesantes para ellos, en particular las de base tecnológica.

¿Cómo ve a Latinoamérica en materia de seguridad de la información frente al resto del mundo?

Gracias a Dios tengo la posibilidad de trabajar para empresas de los Estados Unidos, Argentina y Panamá, y la diferencia en el nivel de madurez de las empresas de los Estados Unidos y Latinoamérica es muy grande. Incluso dentro de Latinoamérica, dependiendo de los países e industrias, también hay brechas muy marcadas. Y si bien la obligación de cumplir con regulaciones ayuda a impulsar la seguridad de la información, muchas veces esto no es suficiente ya que se genera una cultura de seguridad basada en el cumplimiento y no como una herramienta de gobierno y gestión de riesgos que le puede agregar valor al negocio. La buena noticia es que con el tiempo, muchas compañías están viendo que los costos asociados a incorporar estas prácticas como parte integral de las compañías no son altos comparado a con lo que les puede pasar si son víctimas de un incidente o un ciberataque.

ARTÍCULOS PRESENTADOS EN CIBSI-TIBETS 2015

Proyecto MESI en Centro América: Los primeros pasos. *Full Paper*

Jueves, 12 Noviembre
Sesión 1 TIBETS