

EXPERTOS EN SEGURIDAD Y LÍDERES DE LA INDUSTRIA DE TI

Situación de la Seguridad en Informática en México, frente a otros países del mundo.

De manera general, se percibe que México aún se encuentra rezagado, principalmente frente a los países más tecnificados. Este atraso, es reflejo de dos circunstancias principalmente:

- 1) Se conoce la tecnología, pero no se implementa. Las razones que en mayor medida determinan este comportamiento, son:
 - a) Una falta de conciencia en los niveles directivos, acerca de que la seguridad de la información tiene que formar parte de la estrategia de negocios y abordarse de manera global (con todos sus componentes, como son: Personas, Procesos y Tecnología), no aislada.
 - b) No se le da prioridad a este rubro, en las asignaciones presupuestales de la organización.
- 2) El retraso industrial que persiste en el país, ocasiona que en México no se desarrollen soluciones tecnológicas para este ramo.

A nivel de América Latina, se considera en un nivel estándar o incluso un poco arriba de la media.

En general no existe una cultura de Seguridad a nivel organizacional, lo que hace que las medidas, a nivel país, sean ejecutadas de manera parcial. A nivel sectorial, son pocas las organizaciones con un alto nivel de conciencia al respecto (como el sector financiero). En cuanto a tamaños de empresa, es claro que las grandes empresas y corporativos destinan recursos específicos para seguridad, mas en empresas medianas y pequeñas, al igual que en la mayoría de las instituciones gubernamentales, el rezago es muy alto.

A nivel de usuarios en general, algunos expertos mencionaron que México se registra como uno de los países más afectados por código malicioso, así como uno de los principales generadores de ataques a la infraestructura de Internet en la región.

Principales retos

Entre los retos más importantes que enfrenta México como país y las principales responsabilidades de los diferentes sectores que lo conforman (usuarios de la tecnología, proveedores de la industria, instituciones educativas, medios de comunicación, gobierno, cámaras y asociaciones), se mencionaron los siguientes:

- Promover la educación, así como el desarrollo de una mayor conciencia de Seguridad a todos los niveles (sociedad en general, organizacional, etc.)
- Crear una verdadera cultura de Seguridad en Informática.
- Combatir el letargo histórico que se tiene para realizar acciones. Pasar de una cultura reactiva y correctiva, a una cultura proactiva y preventiva, por parte de quienes toman las decisiones.
- Lograr una legislación expedita, con leyes claras que realmente castiguen a los infractores.
- Creación de estándares a nivel nacional.
- Una mayor difusión, de manera objetiva.
- Mayores y mejores controles en la infraestructura de comunicaciones de las empresas, dependencias de gobierno y los hogares, con énfasis en las redes inalámbricas.
- Profesionalización, tanto de los proveedores como de los compradores de tecnología.
- Fomentar una cultura de la legalidad, a nivel educativo. Apoyar esto, difundiendo las desventajas de la piratería, desde la perspectiva del daño directo (código malicioso incluido en el medio) y de las vulnerabilidades crecientes que implica el no tener acceso a versiones actualizadas de las herramientas de seguridad.
- Creación e implementación de políticas claras y bien diseñadas, al interior de las organizaciones.
- Promover el desarrollo tecnológico a nivel nacional.
- Ofrecer al mercado productos integrales, en donde la seguridad esté implícita y no tenga que ser un elemento adicional.
- Hacer la tecnología de seguridad más accesible a todas las personas y organizaciones.
- Que los proveedores de tecnología hagan que la utilización de las herramientas de seguridad sea fácil y transparente para el usuario.
- Mayor capacitación y especialización por parte de los proveedores de tecnología, consultores e integradores.

- Adaptar las soluciones a la idiosincrasia del país en el que se vendan.
- Como fabricantes de productos, buscar la estandarización y una mayor compatibilidad con soluciones de otros proveedores.
- Manejar y desarrollar esquemas de licenciamiento más flexibles, que faciliten la implantación de programas de seguridad informática, de acuerdo a las condiciones de cada organización.
- Construir sobre plataformas listas para crecer conforme lo vaya requiriendo el usuario.
- Mayor participación conjunta entre fabricantes, integradores y usuarios finales
- Buscar la mayor rentabilidad para las organizaciones usuarias, en la implementación de soluciones de seguridad.
- Difundir el concepto de Seguridad de la Información entre los estudiantes de cualquier carrera, no sólo en las relacionadas con tecnología informática.
- Brindar servicios públicos vía Internet, con alto grado de seguridad.