vestigaconsultores.com

Newsletter

ENERO 2024, NÚMERO 6

SEGURIDAD DE INFORMACIÓN: NO BASTA LA TECNOLOGÍA

Usualmente, cuando una empresa sufre una pérdida o daño como consecuencia de un *hackeo* o de robo interno de información, sus altos mandos deciden que es prioritario invertir en la adquisición de un blindaje con las soluciones más modernas o recomendables por expertos en software y ciberseguridad. Y, sin duda, tener las mejores herramientas tecnológicas y digitales disponibles en el mercado es un paso muy importante para elevar el nivel de protección del mayor activo de uno de los principales activos de las empresas, su información.

No obstante, como lo señalan varios expertos y de acuerdo con la experiencia sufrida por miles de empresas, la inversión en infraestructura y soluciones digitales, apostando a un blindaje tecnológico cuya naturaleza se enfoca en la defensa contra ataques externos maliciosos, cuando al menos 80% de los incidentes de pérdida de información sufridos por las empresas obedecen ya sea a la negligencia (50%) o a la mala fe de empleados (30%) que roban información y/o se coluden con terceros para hacerlo.

Lo anterior se confirma con, por ejemplo, datos del monitoreo de percepciones empresariales de VESTIGA: de las empresas mexicanas que registraron sustracción de información, 49% lo atribuyeron a errores y/o negligencia de empleados y 35% a robo realizado por éstos también. Sólo 18% indicaron que dicha sustracción fue consecuencia de actos de *hackeo* efectuados por terceros sin el apoyo de empleados.

En ese sentido, dos factores clave que afectan sensiblemente el nivel de riesgo al que está expuesta la seguridad de la información de las empresas, más allá del también muy relevante factor tecnológico, están íntimamente ligados con la gestión de los recursos humanos de las empresas: un adecuado management y un proceso amplio y continuo de capacitación.

Así pues, las empresas no pueden con un grado de efectividad razonable mitigar los riesgos en seguridad de información gastando sólo en tecnología, por elevada que dicha inversión sea. Una estrategia adecuada para proteger la información de cualquier empresa debe incluir los aspectos de 1) definición clara de lo que incluye la idoneidad (características) de cuáles empleados, por perfil personal y naturaleza de sus roles, acceden a qué información y 2) programas de capacitación continua de manejo seguro de información para los empleados con acceso a la misma. De ese modo, es importante considerar, entre otros, los siguientes puntos:

I- Clasificar y compartamentalizar el acceso y manejo de la información, especialmente la más relevante para el negocio.

II- Definir e implementar políticas de acceso y protocolos de uso de información

III- Establecer / agregar cláusulas de responsabilidad de los empleados en el buen uso de información de la empresa.