# Los siete riesgos principales de TI para las empresas, de acuerdo con Zurich

El estudio revela que la mayoría de profesionales de seguridad no tienen claro cómo una falla tecnológica puede convertirse en un riesgo.

Muchos proveedores y consultores de TIC suelen emitir sus percepciones sobre las tendencias en el uso de TI por parte de las empresas, así como los riesgos que las compañías enfrentan cada año en materia de seguridad de la información y protección de datos. La gran mayoría de estas tendencias coinciden entre los diferentes fabricantes y consultores, lo que permite a las organizaciones prepararse para evitar caer en algún incidente que ponga en riesgo su operación.

Sin embargo, existen compañías capaces de detectar el número real de las organizaciones afectadas por alguna vulnerabilidad, además de conocer cuál es el impacto económico para estas organizaciones que han sufrido el ataque o la falla tecnológica. Estas empresas que parecen conocer la otra cara de la moneda, más allá de las previsiones de TI, son las aseguradoras, las cuales muchas veces deben hacer válidas las pólizas de sus clientes y, por ende, investigar las causas del incidente, las consecuencias y el costo final.

Esta recopilación de datos permitió a Zurich, una de las aseguradoras globales más importantes en el mundo, generar su Reporte de Seguridad Informática: un estudio global creado en colaboración con el centro de estudios Atlantic Council. En él, se encontró que las organizaciones deben mejorar su tiempo de respuesta a los riesgos informáticos a fin de evitar una conmoción en seguridad virtual.

El estudio revela que la mayoría de los profesionales de seguridad informática no tienen del todo claro la manera en que una falla

tecnológica podría evolucionar a convertirse en un riesgo a nivel organizacional.

**Los siete riesgos principales de TI para las empresas, de acuerdo con Zurich**

1. **Manejo de TI interno**. El tener toda la estructura de TI internamente, sin subcontrataciones, puede dar una acumulación de problemas difíciles de manejar para una sola organización.
2. **Asociaciones con contrapartes.** Al trabajar en un proyecto conjunto con una organización externa, ya sea un competidor o socio, pueden existir riesgos de una interconexión directa entre ambas partes y que compartan información.
3. **Subcontratación de servicios.** Se tiene que tomar precauciones al tener proveedores externos de servicios, como Recursos Humanos, Legal o de TI; hay que revisar que no se compartan datos de más entre las dos partes.
4. **Riesgos cibernéticos a cadenas de suministro.** Las cadenas de suministro y logística tradicionales pueden sufrir severas interrupciones con ataques cibernéticos.
5. **Tecnologías disruptivas.** Las nuevas tecnologías, como las redes inteligentes, traen consigo nuevos efectos inadvertidos, que todavía no están en la mira de los profesionales de informática.
6. **Infraestructura ascendente**. Actualmente hay sociedades y economías que son sustentadas por infraestructuras informáticas, ya sean sus sistemas de electricidad o telecomunicaciones, que de sufrir alteraciones, como una potencial regulación de Internet, crearían riesgos para cualquier organización.

7. **Crisis externas**. Los riesgos que están fuera del sistema, en los cuales la organización no tiene ningún control,  tal como una pandemia de malware, pueden tener un efecto cascada.

Zurich estima que una intensificación de estos riesgos podría crear una falla de escala similar a la crisis financiera de 2008. Por ello, la aseguradora recomienda a las organizaciones incorporar las mejores prácticas de regulación informática, incluyendo la creación de un Comité de Estabilidad Cibernética, a fin de optimizar el tiempo de respuesta a riesgos y amenazas informáticas.