LADRONES VIRTUALES

La información electrónica corporativa y personal está más disponible que nunca para la audiencia mundial, y su seguridad es imprescindible en el mundo de hoy.

La información es poder. Eso nadie lo discute hoy. Por eso, se trata de uno de los activos más valiosos para una compañía y su custodia casi que una obligación.

La información puede ser definida como cualquier comunicación que incluya hechos, datos u opiniones, ciertas o no, bien sean números, gráficos o narraciones y que sean conservados en cualquier medio, incluyendo bases de datos computarizadas, papel, microfichas, CDs o las ya populares memorias USB. Algunos ejemplos de información clave en una empresa van desde el registro histórico de pagos, datos personales, información de precios para clientes en particular, hasta el registro histórico de desempeño, proyecciones, fortalezas y debilidades, pasando por alianzas estratégicas, proyectos específicos, problemas relacionados con los empleados, problemas administrativos, información de mercadeo, expansión, metas de mercadeo, contratación, nuevos productos y servicios, inventos y descubrimientos.

NO EXISTE UNA LEY QUE PROTEJA LA SEGURIDAD SOBRE LA INFORMACIÓN, A PESAR DE QUE HAY NORMAS SOBRE PROPIEDAD INTELECTUAL.

El problema es que actualmente no existe una legislación clara sobre el deber legal de proteger la seguridad de la información (accesos, modificaciones, uso y manejo), a pesar de que ya hay leyes sobre la propiedad intelectual y los derechos de autor, sobre el comercio electrónico y el Intercambio Electrónico de Datos (EDI). “En el área de la seguridad informática se está en espera de una legislación fuerte que abarque todos los campos de esta disciplina. Aunque el marco legal no cubre una gran variedad de aspectos (como el uso inadecuado de los computadores), el área que más llama la atención es el de protección de información”, señala el teniente coronel de I.M. (r) Guillermo Lara Páez, gerente general de Admejores Seguridad Ltda..

Sin embargo, cada día más empresas de seguridad se ponen en guardia en este campo. “En la medida en que las personas y empresas hacen un mayor uso de las Tecnologías de la información (TI) las necesidades de seguridad para garantizar la integridad y confiabi-

FOTOGRAFÍA: 123RF

lidad de las operaciones electrónicas también aumentan. El papel de una entidad de certificación digital como Certicámara es fundamental para proveer seguridad en la información electrónica", explica Erick Rincón Cárdenas, gerente general de Certicámara S.A., una entidad de certificación digital abierta que promueve el comercio y el gobierno electrónico confiable.

Para el experto, los riesgos más destacados en el uso de las tecnologías de la información son la suplantación de identidad, la alteración de la información electrónica, la falta de disponibilidad y la ausencia de confidencialidad de las operaciones electrónicas.

Agrega que la prevención de delitos relacionados incluye desarrollar procesos asegurando la información, pero no solo desde la perspectiva técnica o tecnológica, sino también desde el punto de vista jurídico (seguridad jurídica y probatoria), de la gestión documental (cumplimiento de las disposiciones técnicas en materia archivística) y de procesos. "Debe hacerse un análisis integral de riesgos que permita verificar cómo se controlan, mitigan o eliminan estos, dependiendo del impacto y probabilidad que tenga en una organización", señala.

Para esta entidad, la información debe ser protegida con mecanismos que garanticen su autenticidad, integridad y disponibilidad a lo largo del tiempo. Herramientas como las firmas electrónicas o firmas digitales, sellos digitales de tiempo, así como servicios de archivo confiable de la información electrónica, resultan indispensables en el desarrollo de la virtualización de procesos o documentos.

"El primer consejo para las empresas es invertir en buena seguridad, lo cual implica estructurar esquemas ajustados a su verdadera necesidad. Hay que encontrar un prestador de servicio con altos estándares de calidad", dice por su parte John Jairo Lozano, director nacional de ventas de Seguridad de Occidente.

LOS RIESGOS MÁS COMUNES SON: SUPLANTACIÓN, ALTERACIÓN DE INFORMACIÓN Y AUSENCIA DE CONFIDENCIALIDAD.

A su vez, para el presidente de la Federación Colombiana de Empresas de Vigilancia y Seguridad Privada (Fecolsep) Hernán González Pardo, el tema de la fuga de información y todo lo relacionado con formas delincuenciales de espionaje a nivel personal y empresarial es un tipo de delito que va mutando en su *modus operandi* y para combatirlo es importante contar con sistemas avanzados de seguridad de datos. "Se debe partir de una base: este tipo de delitos son invisibles por su naturaleza y la forma de enfrentarlos exige inversiones en tecnología –dice–. Un buen aliado privado en temas de seguridad recomendará la mejor forma de mantener seguras las redes y los sistemas de comunicación y generará mecanismos de control de datos basado en sus certificaciones de calidad. Este tipo de sistemas de gestión es hoy una norma en las empresas de vigilancia y seguridad privada y ayudan a prevenir el ser víctimas de delitos informáticos".

Una mención especial debe hacerse dentro de la protección de la información: la rápida expansión y popularización de internet hacen que la seguridad en redes sea indispensable en un esquema de defensa. Los virus y los *hackers* forman parte de los riesgos y, como no existe una solución universal para proteger una red, en la mayoría de los casos la mejor estrategia es pensar como un cibercriminal y "colarse" en la empresa para hallar las fallas y corregir luego los agujeros de seguridad. La estrategia es tan eficaz, que a veces se contratan *hackers* para que impartan cursos de seguridad a los responsables de las redes de las empresas. |D|