Introducción a la seguridad de la información

Un mundo de cambios

La vertiginosa velocidad con que van evolucionando las tecnologías informáticas y de comunicaciones genera un desafío sin precedentes al momento de garantizar la preservación de un nuevo activo para las organizaciones como lo es la información.

por Gustavo García Enrich*

Al ritmo de la *Ley de Moore*, la capacidad de procesamiento sigue duplicándose cada 18 meses, las redes se proyectan hasta el infinito sin diferencias entre un entorno local o global mostrando que la sociedad de la información se ha instalado para no marcharse. Los requerimientos de almacenamiento crecen a ritmo exponencial aumentando la densidad de información en los medios/soporte a niveles impensados.

Éste que vivimos, es un mundo frágil. Los riesgos abundan en la selva tecnológica y se acrecientan día a día anticipándose a las tecnologías defensivas. Hackers, ingeniería social, ciberterrorismo, robo de información, virus, negación de servicio, troyanos, *phishing*, incendios, sabotajes, catástrofes y otras contingencias acechan todos los días conspirando contra el *uptime* o tiempo disponible de sistemas, vital para las organizaciones modernas. El mundo está *online* y del otro lado de la línea tiene que haber respuesta 24 horas, siete días a la semana, con una efectividad del 99.99 %.

A la vista de todo esto el desafío de los CEO de hoy es hacer las cosas bien o por lo menos todo lo bien que el estado de las tecnologías actuales lo permitan. No hay margen para el error porque no hay certeza de que la sombra de Murphy no se proyecte: si algo puede fallar, fallará. La única alternativa es estar preparado.

Hoy en día nadie vinculado a las áreas de *management* de una organización desconoce el siguiente postulado:

Información = activo

Podemos clasificar la información por sus dos estados característicos: circulación y elaboración. La información en circulación es aquella en contacto directo con los usuarios finales y que interviene como soporte a los procesos de decisión en una compañía. Es aquella que circula por las redes privadas y públicas, accediendo a ella en forma local o remota, es la que alimenta un ERP o que se almacena parcialmente en redes de almacenamiento o en discos locales en máquinas de escritorio. Es aquella que se traslada físicamente en un *notebook* y que circula por redes Wi Fi en el espacio público sin demasiado control y también es aquella que se muestra tentadora a agentes inescrupulosos para robar, manipular, y modificar, en beneficio de terceros. Pero además de todos los riegos que acechan a la información en su estado elaborado, esta no es indivisible y puede escindirse en sus dos componentes más puros:

Información = datos + capacidad de procesamiento
Estos elementos primordiales son la génesis de todo el proceso, sin datos o sin la capacidad de procesarlos, no hay información.

Seguridad de la información

Ahora y, tal como dijimos antes, los datos y/o la información no son estáticos sino que obedecen a la dinámica de los tiempos que corren. Esto significa que alcanza el mismo grado de importancia la capacidad de transmitirlos en sentido bilateral, o sea la capacidad de emitir o recibir a través de las redes globales en forma segura. Hay que tener en cuenta, por ejemplo, que según las últimas estadísticas el 75% de las informaciones vitales y confidenciales de una organización viajan por e-mail. Sin lugar a dudas el riesgo generado por esta aplicación podría hacer tambalear más de una compañía si esa información cayera en manos equivocadas.

La seguridad de la información se logra implementando un conjunto adecuado de controles que abarca políticas, prácticas, procedimientos, estructuras organizativas y funciones de software que aseguran una garantía razonable o suficiente de que se lograrán los objetivos del negocio.

Es comúnmente difundido que lo que no se puede medir no se puede mejorar y es mucho más problemático en el campo de seguridad de la información la existencia de una falsa percepción de la seguridad. Esto hace difícil medir y poner parámetros al estado real de la información además de proyectar cambios alineados con un proyecto de mejora.

Dentro de las organizaciones, es común encontrar pensamientos como los que siguen:

Por lo tanto la seguridad de la información protege a ésta de una amplia gama de amenazas, a fin de garantizar la continuidad del negocio, minimizar el daño al mismo y maximizar el retorno sobre las inversiones y las oportunidades.

Podemos entender la seguridad de la información como la preservación de las siguientes características:

1. Confidencialidad: garantiza que la información sea accesible sólo a aquellas personas autorizadas a tener acceso a ella.

2. Integridad: salvaguarda la exactitud y totalidad de la información y sus métodos de procesamiento y comunicación. Debe contener en forma completa lo que se espera que contenga. También implica que la información que se recibe en un punto remoto de una red debe ser exactamente igual a la que se emitió en un punto local.

3. Disponibilidad: garantiza que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con ella toda vez que se requiera, en el momento que se requiera y donde se requiera.

- Todas las fallas serán notorias en forma inmediata.
- Lo que hacemos no es importante.
- Las personas saben qué hacer ante una emergencia.
- Es fácil conseguir los elementos de reemplazo (insumos, aire acondicionado, servidores, etc.)
- Los clientes y otros receptores de nuestros servicios van a entender.
- Los sistemas de alarma son infalibles.
- Con la UPS y el Firewall es suficiente.
- A nosotros no nos va a suceder.

Pero sucede y mucho mas frecuente de lo que se supone. No siempre los problemas toman una dimensión pública porque suelen ocultarse y no se denuncian los incidentes de seguridad. Esto empeora las cosas porque los casos no se documentan y permite que causas que produjeron el problema queden latentes y el incidente pueda repetirse.

También es cierto que la seguridad de la información posee otras características propias que generan reticencias al momento de elevar los niveles de seguridad, casi siempre se vincula a ocurrencias hipotéticas; se tilda de abstracta y compleja; se dice que es

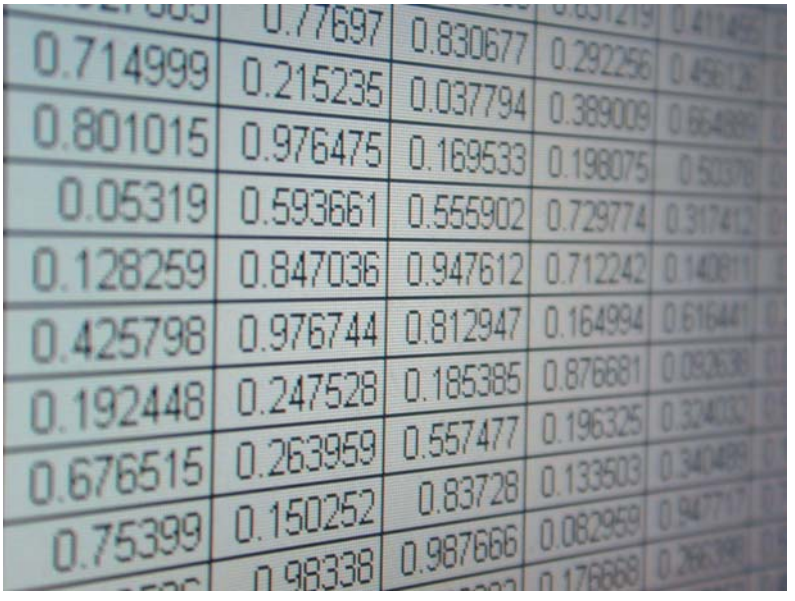
un problema del negocio, no técnico; implica mayores costos, reduce el desempeño y acarrea incomodidad; los gerentes preguntan: ¿cuanto más voy a vender si pongo más seguridad? Y a esto añadimos que no existen indicadores y prácticas universales para medirla.

Dentro de este marco general, los responsables de la seguridad deben luchar contra la cultura propia de la empresa para implementar un programa de seguridad de la información y es contar con el apoyo de la dirección de la empresa, lo que se transforma en un factor clave de éxito. Para ello los objetivos de seguridad deben soportar o reflejar los objetivos o misión de la organización a la vez que deben satisfacer distintos marcos regulatorios.

Legislaciones actuales

Existe un grupo de nuevas leyes que hacen legalmente responsables a los directivos de empresas si no protegen sus activos de información bajo amenaza de sanción. La diligencia razonable de los responsables o gerentes está en promover el interés y la prudencia necesaria en evaluar el riesgo y las medidas pertinentes para reducirlo o eliminarlo.

A partir de los escándalos fiscales de Enron, Global Crossing y World.Com, fruto de los defectos y lagunas de los sistemas de información empresarial financiera, la ley estadounidense Sarbanes-Oxley Act, conocida como SOX, se desarrolló teniendo como objetivo generar un marco de transparencia para las actividades y reportes financieros de las empresas que cotizan en bolsa, y darle mayor certidumbre y confianza a inversionistas y al propio estado.



SOX contempla una revisión más rigurosa de los datos que los que una empresa declara en sus estados financiero–contables y de los que utiliza para sus controles internos. Esto no solamente abarca fraudes por falsedad en dichas declaraciones, sino también por inferencia y todos los casos de fraude en los que se desvirtúen de manera importante los estados financieros, como la malversación de activos y actos de corrupción, entre otros.

Las multas por proveer información falsa o incorrecta son muy severas y pueden llegar al extremo de encarcelar a los ejecutivos de la empresa o que ésta sea retirada de la bolsa de valores en que cotiza. Además exige contar con un canal de denuncias de irregularidades por parte de los empleados, accionistas, proveedores y demás, para que las mismas sean tratadas por el comité de auditoría.

En líneas más generales y según su área de aplicación podemos enumerar algunas de las regulaciones más importantes: (ver recuadro).

Gestión de seguridad y normas aplicables

Dado que mantener la seguridad es un problema y algo hay que hacer para solucionarlo, lo mejor es hacerlo teniendo en cuenta la guía de normas internacionales aplicables. No hace falta inventar la rueda, alguien lo hizo antes. Nuestro esfuerzo no debe estar centrado en el desarrollo de estándares sino en la implementación y capacitación.

Entre las principales normas y metodologías podemos citar:

- Information Systems and Audit Control Association – ISACA: COBIT
- ITIL (IT Infrastructure Library)
- British Standards Institute: BS 7799
- International Organization for Standarization: Normas ISO
- Departamento de Defensa de USA: Orange Book / Common Criteria
- ITSEC – Information Technology Security Evaluation Criteria: White Book
- Sans Institute, Security Focus
- Sarbanes Oxley Act, Basilea II, HIPAA Act,
- ISO17799:2005, ISO27001

Entre todas estas, la última es la que se va perfilando como un estándar de aplicación universal.

La Norma ISO 17799:2005 denominada Código de Práctica para la Administración de la Seguridad de la Información, es un estándar internacional de seguridad que provee las mejores prácticas para la definición de controles, proporcionando proactivamente soluciones para evitar interrupciones en las actividades y procesos del negocio, asegurando una protección adecuada para los sistemas de información contra amenazas internas y externas.

Debemos tener en cuenta que esta no es una norma certificable ya que se trata de recomendaciones. Para hacer una certificación deberá hacerse sobre la Norma BS 7799 parte 2 denominada

Legislación reciente	¿A quién se aplica?	¿Qué cubre?
Sarbanes-Oxley Act de 2002	A toda compañía registrada bajo el *Exchange Act* o que tiene una declaración de inscripción en espera bajo el *Security Act*.	Obliga a los jefes de dirección y a directores financieros a prestar juramento que sus declaraciones financieras son completas y exactas.
Gramm- Leach-Bliley Act de 1999	A las instituciones financieras.	Asegura la protección de las informaciones personales no públicas para la distribución fuera de la red de la institución financiera.
Health Insurance Portability and Accountability Act (HIPAA)	A toda entidad implicada en la información digitalizada por los cuidados de salud, incluyendo entre otros los proveedores, los empleados y los aseguradores.	Garantiza la portabilidad, la protección de la vida privada y la seguridad de la información médica de los individuos.
LOPD (Ley Orgánica de Protección de Datos) Ámbito europeo	Cualquier compañía que capture, guarde o trate datos de terceros.	Asegura la protección de la información personal (no pública) y el derecho a la rectificación y cancelación de los datos por el ciudadano.
Basilea II	A las instituciones financieras.	Calcula el riesgo operativo de negocio por motivo del mal funcionamiento o indisponibilidad de las TI.

Sistemas de gestión de la seguridad de la información. Cabe destacar que bajo los lineamientos de ISO, la última actualización de esta norma se ha transformado en la ISO 27001 denominándose: *Information Technology - Security Techniques – Information Security Management Systems – Requirements*.

Está conformada por diez secciones, tratando la primera parte los controles y la segunda la certificación del SGSI o Sistema de gestión de seguridad de la información.

La seguridad no es un proyecto sino un proceso que tiene un comienzo pero no tiene un final ya que es una actividad de mejora continua que requiere el compromiso y soporte de toda la organización para tener éxito. ■

** El autor es el gerente general de Area Data, una empresa argentina que prevee la infraestructura de seguridad para centros de datos de misión crítica. Puede ser contactado en el correo gge@areadata.com.ar*