

## ¿Seguridad informática vs. Seguridad de la información?

© Ing. Carlos Ormella Meyer

La diversidad de ambientes que vienen formando experiencia especialmente desde principios de esta década, muestra algunas visiones diferenciales y en parte contrastantes en temas de gran importancia para una empresa.

### Seguridad Informática

Uno de esos temas, entre los más significativos, es que la mayoría de los "especialistas en seguridad" basan sus conocimientos y experticia solamente en el aspecto técnico tradicional de la seguridad, es decir del área IT, aunque una parte de ellos también consideran las cuestiones propias del "nuevo" aspecto de las comunicaciones y que ha hecho que hoy se hable de ICT o TIC.

Pero además del enfoque básicamente técnico, dichos especialistas en realidad sólo se manejan con **vulnerabilidades** y en parte también con **amenazas** bajo la forma de ataques, todo lo cual no es suficiente para hablar de los **riesgos** correspondientes.

Para un análisis o **valuación de riesgos** (*risk assessment*, RA) aunque se refieran a lo técnico, es necesario realizar también valuaciones de los **activos**, así como una identificación de las **amenazas** que puedan aprovechar y explotar las **vulnerabilidades** de esos activos. Recién entonces se pueden determinar los riesgos a partir de los tres factores mencionados, activos, vulnerabilidades y amenazas, cada uno medido en rangos apropiados de niveles (típicamente 3 para vulnerabilidades, 3 a 5 para amenazas, y 5 a 8 o aún más para activos).

Y si luego se trata de determinar qué se hace con los riesgos, en la mayoría de los casos corresponde mitigarlos a un nivel aceptable, para lo cual habrá que implementar determinadas medidas de seguridad.

El proceso es tal que, a partir de tales riesgos de características técnicas, el enfoque más eficiente es realizar un análisis gap contra por ejemplo estándares técnicos como los establecidos por NIST en su serie 800, o bien una norma de enfoque corporativo como la ISO 27002 (anteriormente ISO 17799), para establecer qué controles y a qué nivel se los debe implementar para reducir aquellos riesgos a niveles aceptables.

Hasta aquí se puede hablar de **seguridad informática**. Si bien este término es una buena traducción del correspondiente en inglés, **information security**, el sentido que se ha venido dando a esta problemática está mucho más cercano a algo como "computer security" o en todo caso "network security".

### Seguridad de la Información

Últimamente se viene dando el cambio a **seguridad de la información** como traducción más adecuada de **information security**. Pero peso a ello todavía hay muchos especialistas que siguen llamando así al puro enfoque técnico comentado antes.

En realidad la seguridad de la información es bastante más amplia, ya que no es simplemente una cuestión técnica sino responsabilidad de la alta gerencia y cuadros directivos de una organización.

En tal sentido hay que tener en cuenta que el ambiente ICT tiende a estar orientado al servicio y actuar como función habilitante de los procesos de negocios. En esto difiere de los procesos centrales mismos de una organización que constituyen el núcleo de los negocios de una empresa.

De hecho, sin el involucramiento activo de las unidades y líderes de negocio, ejecutivos, directorio y steering-committee, no puede existir un plan sustentable de seguridad de la información, a partir de los riesgos determinados. Y todo esto dentro del sistema de dirección y control propio de un adecuado **gobierno corporativo**, como define la OECD (Organización para la Cooperación y Desarrollo Económico, OCDE en español) al **corporate governance**.

Ahora se trata, entre otras cosas, de considerar también la gente, los procesos y funciones de negocio, la protección de todos los activos/recursos de una organización. Donde toda la empresa es la impulsora,

propietaria y beneficiaria de la seguridad de la información, en un marco de responsabilidades compartidas.

Lo comentado en los últimos párrafos implica entonces que para el marco de la seguridad de la información se requiere considerar no sólo los **riesgos técnicos de ICT**, sino también los riesgos de seguridad que se extienden a toda la empresa, es decir: **organizacionales, operacionales y físicos**.

Además, los **riesgos operacionales**-de singular trascendencia por ejemplo en el contexto del Nuevo Acuerdo de Capitales Basilea II para los bancos- son cada vez más cruciales en los escenarios de seguridad de la información. Y las vulnerabilidades de este tipo de riesgos, a diferencia de las vulnerabilidades ICT que responden más bien a un esquema blanco-negro, se extienden a lo largo de una amplia gama de grises, muy relacionada con el comportamiento humano y las opiniones subjetivas de las personas, la cultura empresarial, la forma de comunicación, la resistencia al cambio, etc.

La determinación de las vulnerabilidades organizacionales sigue un proceso muy diferente a las mediciones o lecturas tomadas sobre computadores, servidores, routers, switches, etc. Como generalmente no se disponen de datos históricos suficientes, un análisis exacto se hace imposible. Por eso el análisis se complementa con información que se puede recabar en tal sentido y que se corresponde con información subjetiva surgida de opiniones (generalmente de expertos o al menos de personal con conocimiento específicos del área que se analiza). Estas opiniones pueden identificarse y analizarse a partir de algún método de investigación prospectiva tal como Delphi, seguido por entrevistas personales para establecer el valor de dichas opiniones.

Por otra parte, la *valuación de activos* no está en la mayoría de los casos al alcance de los técnicos. El valor o nivel de un activo es un valor del negocio y para los negocios de una empresa. Esto señala que los propietarios de los **procesos de negocio** son quienes pueden establecer un valor adecuado de los mismos y de allí derivar los valores de los **activos/recursos** que manejan las diferentes **funciones** que componen cada proceso.

### Seguridad de la Información y Seguridad Informática

La extensión del concepto usual de **seguridad informática** al de **seguridad de la información**, implica un corrimiento y visión más amplia de un marco de riesgos de negocios respecto de la perspectiva tradicional de seguridad técnica, basada principalmente en vulnerabilidades. De acuerdo con lo visto anteriormente, tal extensión se da de dos maneras.

Por un lado, en el contexto de la seguridad de la información los riesgos de negocios incluyen no sólo las vulnerabilidades y un aspecto de las amenazas, sino el conjunto de los factores que determinan tales riesgos: **activos, vulnerabilidades y amenazas**.

Por otra parte, los riesgos de negocio que se consideran incluyen los **riesgos organizacionales, operacionales, físicos y de sistemas ICT**.

Una visión ilustrativa de tales conceptos puede visualizarse en la figura que se acompaña.



Finalmente surge también que un enfoque completo de seguridad de la información parte de considerar que los recursos necesarios para mitigar los riesgos dentro de un plan de seguridad, no son un gasto sino una inversión. Y que, como tal, se requiere el análisis y determinación cuantificable del retorno de las inversiones en seguridad, particularmente por medio de la determinación del **ROSI** (Retorno Sobre la Inversión en Seguridad) como extensión del conocido concepto financiero de **ROI** (Retorno Sobre la Inversión).