Ing. Carlos Ormella Meyer y Asoc.
Gestión y Auditoría de Riesgos y Seguridad de la Información
Tel: +54-11-4371-4638 – Cel: +54-911-6513-2751
E-mail: ciprio@ingcomyasoc.com.ar

Preguntas y Respuestas
RIESGOS Y SEGURIDAD DE LA INFORMACIÓN

P: ¿De qué trata la norma ISO 27005?
R: La norma ISO 27005 de Gestión de Riesgos establece una serie de *recomendaciones* para la Gestión de Riesgos de Seguridad de la Información, necesarias por ejemplo para construir un Sistema de Gestión de Seguridad de la Información (SGSI) efectivo que involucra un proceso continuo.

P: ¿Cuáles son esas recomendaciones?
R: A grandes rasgos se refieren al contexto, valuación de riesgos, tratamiento de los mismos y su aceptación.

P: ¿Qué se puede decir del contexto?
R: El contexto de trabajo considera especialmente lo referido al propósito y criterios de la gestión de riesgos. En primer lugar corresponde aclarar que la ISO 27005 no es para uso exclusivo en Seguridad de la Información, sino que también puede dar soporte, entre otros, a un Plan de Continuidad de Negocios (BCP), o un Plan de Gestión de Incidentes (IRP), así como incluso para cumplir posibles imposiciones legales.
Adicionalmente, dentro del contexto que se comenta hay que establecer los criterios básicos para la evaluación y aceptación de riesgos, es decir, la consideración de los niveles de riesgo resultantes en función de los procesos y actividades de la empresa.

P: ¿Y siguiendo con la valuación de riesgos?
R: La valuación de riesgos consiste en la identificación y estimación de los riesgos, seguidas por la evaluación de los mismos conforme posibles umbrales y formas de consideración de los mismos.

P: ¿Y ahora viene la última parte?
R: Efectivamente. Una vez evaluados los riesgos deberán ser tratados adecuadamente sea para reducirlos, aceptarlos, evitarlos o transferirlos. Finalmente habrá que tomar las decisiones en cuanto a la aceptación o no de los resultados del tratamiento de riesgos.

P: ¿Eso es todo?
R: Hay que agregar que la aceptación de los riesgos deberá *comunicarse* adecuadamente así como *monitorearse y revisarse* cuando sea necesario dentro del proceso continuo del PDCA. Por lo demás en todo este proceso se destaca el tema de la estimación de riesgos ya mencionado.

P: ¿Qué se puede decir sobre la estimación de riesgos?
R: Uno de los aspectos más destacados lo constituye la estimación de los riesgos que puede realizarse con dos metodologías: ***cuantitativa*** (en valores monetarios) o ***cualitativa*** (bajo la forma de cierta cantidad de niveles). A su vez, en el análisis mismo se pueden usar dos aproximaciones: por las acciones o ***pérdidas*** y por las ***entidades*** que conforman el riesgo mismo.

P: ¿Qué se puede decir del método de estimación por las pérdidas?
R: El método por Pérdidas es el más conocido y se lo calcula multiplicando el **impacto** que un incidente puede causar en un activo de información por la **probabilidad de ocurrencia** de dicho incidente a lo largo de un año. El impacto en cuestión puede ser menor que el valor del activo afectado con un límite dado por dicho valor.
Para poder usar la variante cuantitativa, es decir donde se fijen valores monetarios, se necesita conocer el historial completo de todos los hechos similares ocurridos durante un tiempo considerable ponderados precisamente en las pérdidas en dinero, directas o indirectas.

Debido a las limitaciones que pueden aparecer en la práctica es usual “mapear” los posibles valores monetarios a niveles cualitativos descriptivos o bien identificables con números sucesivos desde 0 o 1 hasta el máximo que se considere.

P: ¿Y el método de las entidades?
R: El método de las Entidades, considera los **Activos** de información, las debilidades o **Vulnerabilidades** que puedan ofrecer, y las **Amenazas** que pueden aprovechar dichas vulnerabilidades para causar un daño en dichos activos. Este método sólo puede realizarse en forma cualitativa de nuevo asignando niveles con valores numéricos sucesivos.

P: ¿Se puede decir algo más de ambos métodos?
R: El método de Pérdidas arrastra un detalle negativo no menor. Al trabajar con valores numéricos (sean monetarios o asignados por niveles) el resultado de la multiplicación de impactos por probabilidad de ocurrencia puede arrojar resultados similares para situaciones muy diferentes como un incidente de ***bajo impacto y alta probabilidad de ocurrencia*** frente a otro de ***alto impacto y baja probabilidad de ocurrencia***. Y es fácil deducir que mientras los primeros podrían llegar a tolerarse, los de alto impacto y baja probabilidad pueden provocar situaciones insostenibles y aún catastróficas.
Este efecto también puede aparecer en el caso de Entidades para el caso que se multiplicaran simplemente los valores numéricos asignados. Por eso hay sistemas de determinación de riesgos que usan por ejemplo 10 rangos para los Activos, 5 para las Amenazas y 3 para las Vulnerabilidades, incluso con un algoritmo especialmente diseñado para el caso.

P: ¿Y cómo se determina el valor de un activo?
R: El valor de los activos físicos o contables generalmente no es el de compra o de libro. Un buen método es recurrir a un esquema multicapa a partir de los **procesos de negocios** que reciben un valor y/o ***nivel de criticidad***, por lo que representan para la empresa en cuanto a su importancia operacional, establecido por el personal comercial y de alta gerencia de una empresa. Como los procesos de negocios se ejecutan por medio de diferentes **funciones de negocio** (incluso en distintas áreas de una empresa) que se puede decir que heredan dicho nivel. A su vez, los **activos y recursos** que soportan dichas funciones heredan el mismo nivel.

P: ¿Alguna otra observación respecto de esta norma?
R: La ISO 27005 sólo ha sido adaptada a la ISO 31000 de Riesgos Corporativos (es decir de todo tipo) en cuanto al Proceso de Gestión de Riesgos, visión de alto nivel de la ISO 31000..
Esta faltando todavía la incorporación del concepto de Oportunidades, o sea de riesgos positivos en contraposición a los tradicionales riesgos negativos, característica que seguramente será incorporada en la próxima versión.
De cualquier manera el concepto de Oportunidades ya ha sido incorporado en la última versión 2013 de la ISO 27001.