Introducción a Riesgo Informático

Leonardo Sena y Simón Mario Tenzer

Agosto 2004

INDICE

Prefacio

Este documento se relaciona fuertemente con otros documentos de la Cátedra. Las referencias precisas a estos y otros documentos se señalan oportunamente en el texto. Por ejemplo: Virus Informático, Seguridad Informática, etc. Todos ellos abordan el tema de riesgos desde distintas ópticas.

Estos documentos tratan algunas de las amenazas más comunes y explican la manera de minimizar ciertos riesgos, incluidas herramientas concretas para ello.

Por lo tanto este documento puede ser interpretado como un articulador que permitirá comprender más cabalmente los conceptos abordados en otros documentos, así como permitirá que estos conceptos puedan ser aplicados de una mejor manera.

Por la relevancia práctica del tema, este documento está dirigido a las tres opciones del curso de Introducción a la Computación de Facultad, a saber: a) Administrativo / Contable, b) Economía y c) Licenciatura en Estadística. Para estas dos últimas, las referencias a paquetes contables y al informe COSO deben ser ignoradas.

Introducción

El acelerado crecimiento de la tecnología de la información (TI)[1] [2] en los últimos 15 años ha generado creciente número de oportunidades así como un creciente número de amenazas.

Un alto nivel de inversión en tecnología, tal cual existe hoy día, produce un efecto multiplicador importante en caso que dichas amenazas se materialicen, dado que las pérdidas posibles se ven incrementadas en igual proporción al aumento de la inversión.

[1] También se suele referir en plural: Tecnologías de la Información.
[2] Es mejor referirse a las Tecnologías de la Información y las Comunicaciones (TIC).

Pero no solamente ha cambiado el volumen del uso de la tecnología. También ha cambiado la forma de su utilización. Hoy día el acceso a los recursos de TI no está restringido a los profesionales en informática, sino que es accesible para la casi totalidad de la población. A su vez, el acceso a las TIC no se realiza únicamente a los recursos propios, sino que se extiende a otros organismos, sin frontera física. Esto es gracias a Internet y a la apertura de las redes corporativas, en una magnitud inimaginable años atrás.

A su vez el grado de complejidad de la tecnología utilizada ha aumentado considerablemente, tornándola cada vez más difícil de administrar adecuadamente, lo cual incluye el control de riesgo, para proteger la seguridad.

En este entorno creciente y complejo es que los responsables de gestionar las herramientas tecnológicas deben poder diagnosticar adecuadamente los riesgos a los cuales se ven expuestos para poder mitigar de manera oportuna las pérdidas que puedan generase (que como se ha dicho están relacionadas al monto de la inversión, o pueden superarla).

Anteriormente, los responsables de manejar los recursos de tecnología eran solamente profesionales de tecnología. Actualmente esto ha cambiado, llevando a profesionales en otras áreas a tener que comprender razonablemente las herramientas y recursos tecnológicos con los cuales cuentan, dado que pueden ser responsables tanto por la gestión integral de TI en su organización, como de la gestión de algún componente específico que soporta el proceso de negocio por el cual ellos son responsables.

Este texto trata de realizar una aproximación al tema de riesgo informático, con el objetivo de brindarle al estudiante de Ciencias Económicas, los conceptos básicos necesarios para poder comenzar a transitar de manera exitosa el camino de la administración de riesgos en el contexto actual, enmarcado en la actividad profesional del egresado de Facultad.

Definición de riesgos

Riesgo se puede definir como aquella eventualidad que imposibilita el cumplimiento de un objetivo. De manera cuantitativa el riesgo es una medida de las posibilidades de incumplimiento o exceso del objetivo planteado. Así definido, un riesgo conlleva dos tipos de consecuencias: ganancias o pérdidas.

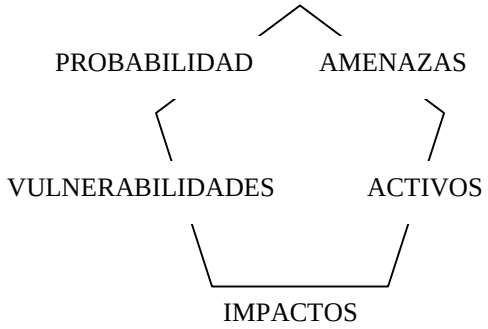
En lo relacionado con tecnología, generalmente el riesgo se plantea solamente como amenaza, determinando el grado de exposición a la ocurrencia de una pérdida (por ejemplo el riesgo de perder datos debido a rotura de disco, virus informáticos, etc.).

La Organización Internacional por la Normalización (ISO) define riesgo tecnológico (Guías para la gestión de la seguridad de TI /TEC TR 13335-1, 1996) como:

> "La probabilidad de que una amenaza se materialice, utilizando vulnerabilidad existentes de un activo o un grupo de activos, generándole perdidas o daños".

En la definición anterior se pueden identificar varios elementos que se deben comprender adecuadamente para, por ende, comprender integralmente el concepto de riesgo manejado.

Estos elementos son: probabilidad, amenazas, vulnerabilidades, activos e impactos.



A continuación se analiza cada uno de ellos:

Probabilidad: establecer la probabilidad de ocurrencia puede realizarse de manera cuantitativa o cualitativa, pero siempre considerando que la medida no debe contemplar la existencia de ninguna acción paliativa, o sea, debe considerarse en cada caso qué posibilidades existen que la amenaza se presente independientemente del hecho que sea o no contrarrestada.

Existen amenazas, como por ejemplo incendios, para las cuales hay información suficiente (series históricas, compañías de seguros y otros datos) para establecer con razonable objetividad su probabilidad de ocurrencia. Otras amenazas presentan mayor dificultad en establecer cuantitativamente la probabilidad. Por ejemplo, el acceso no autorizado a datos; dónde se hacen estimaciones sobre la base de experiencias. Siguiendo con el ejemplo, para el personal interno del Centro de Cómputos (CPD), la probabilidad puede ser el 70%, para el personal de la organización, externo al CPD, del 45%, y para personas de fuera, el 80% (a través de acceso por Internet).

Amenazas: las amenazas siempre existen y son aquellas acciones que pueden ocasionar consecuencias negativas en la operativa de la empresa. Comúnmente se indican como amenazas a las fallas, a los ingresos no autorizados, a los virus[3], uso inadecuado de software[4], los desastres ambientales como terremotos o inundaciones, accesos no autorizados, facilidad de acceso a las instalaciones, etc.

Las amenazas pueden ser de carácter físico o lógico, como ser una inundación en el primer caso, o un acceso no autorizado a una base de datos en el segundo caso.

Vulnerabilidades: son ciertas condiciones inherentes a los activos o presentes en su entorno que facilitan que las amenazas se materialicen llevan a esos activos a ser vulnerables.

Mediante el uso de las debilidades existentes es que las amenazas logran materializarse, o sea, las amenazas siempre están presentes, pero sin la identificación de una vulnerabilidad no podrán ocasionar ningún impacto.

Estas vulnerabilidades son de naturaleza variada. A modo de ejemplo se citan las siguientes: falta de conocimiento del usuario, tecnología inadecuadamente probada (“testeada”), transmisión por redes públicas, etc.

Una vulnerabilidad común es contar con antivirus no actualizado, la cual permitirá al virus actuar y ocasionar daños. Si el antivirus estuviese actualizado la amenaza (virus) si bien potencialmente seguiría existiendo no podría materializarse.

Activos: Los activos a reconocer son aquellos relacionados con sistemas de información. Ejemplos típicos son los datos, el hardware, el software, servicios, documentos, edificios y recursos humanos.

Impactos: las consecuencias de la ocurrencia de las distintas amenazas son siempre negativas. Las pérdidas generadas pueden ser financieras, no financieras, de corto plazo o de largo plazo.

Se puede establecer que las más comunes son: la pérdida directa de dinero, la pérdida de confianza, la reducción de la eficiencia y la pérdida de oportunidades de negocio. Otras no tan comunes, felizmente, son la pérdida de vidas humanas, afectación del medio ambiente, etc.

[3] Ampliar en el documento “Virus informáticos”
[4] Ampliar en el documento “Aspectos legales del software”

Administración y análisis de riesgos

Como herramienta de diagnóstico para poder establecer la exposición real a los riesgos por parte de una organización se recurre a lo que se llama Análisis de Riesgos. Este análisis tiene como objetivos identificar los riesgos (mediante la identificación de sus elementos) y lograr establecer el riesgo total (o exposición bruta al riesgo) y luego el riesgo residual, tanto sea en términos cuantitativos o cualitativos.

Cuando se refiere al riesgo total, se trata de la combinación de los elementos que lo conforman. Comúnmente se calcula el valor del impacto promedio por la probabilidad de ocurrencia para cada amenaza y activo.

De esta manera tendremos, para cada combinación válida de activos y amenazas:

RT (riesgo total) = probabilidad x impacto promedio

Por ejemplo, si la probabilidad de incendios en el año es de 0.0001 y el impacto promedio en términos monetarios de los activos amenazados por un incendio es $600.000, la exposición al riesgo anual es de 60 (ver explicación más adelante).

A este cálculo se debe agregar el efecto de medidas mitigantes de las amenazas, generándose el riesgo residual. El riesgo residual es el riesgo remanente luego de la aplicación de medidas destinadas a mitigar los riesgos existentes.

Las medidas mencionadas son aquellas que generalmente se conocen como controles. (Se aborda este tema más adelante.)

De hecho, el riesgo residual es una medida del riesgo total remanente luego de contemplar la efectividad de las acciones mitigantes existentes. De esta manera, siguiendo con el ejemplo planteado, si el riesgo total de la amenaza incendio es 60, luego de contratar un seguro sobre la totalidad de los activos, el riego residual resultante sería igual a cero. Por otra parte si se asegurara por la mitad del capital, el riesgo residual sería igual a 30.

Obviamente, este ejemplo está simplificado, con el único objetivo de ayudar a comprender los conceptos vertidos. En la realidad no es nada sencillo cuantificar adecuadamente los riesgos. Por lo anterior es que usualmente se utiliza un enfoque cualitativo, expresando los riesgos en altos, medios y bajos, o en niveles similares.

El proceso de análisis descripto genera habitualmente un documento que se conoce como matriz de riesgo. En este documento de ilustran todos los elementos identificados, sus relaciones y los cálculos realizados. La sumatoria de los riesgos residuales calculados es la exposición neta total de la organización a los riesgos.

La afirmación anterior fue efectuada con el supuesto de que el resultado obtenido es positivo. En caso que el resultado sea negativo se establece que la organización se encuentra cubierta de todos los riesgos analizados, pero, sin embargo, es ineficiente porque tiene más controles que los necesarios.

Realizar el análisis de riesgos es indispensable para lograr administrar adecuadamente los mismos.

Administrar el riesgo refiere a gestionar los recursos de la organización (empresa, organismo, institución, etc., sea pública, privada, etc.) para lograr un nivel de exposición determinado. Este nivel es generalmente establecido por tipo de activo, permitiendo menor exposición cuanto mas crítico es ese activo.

El ciclo de administración de riesgo se cierra (luego de efectuar las tareas referentes al análisis) con la determinación de las acciones a seguir respecto a los riesgos residuales identificados.

Estas acciones pueden ser:

Controlar el riesgo: Se fortalecen los controles existentes o se agregan nuevos.

Eliminar el riesgo: Se elimina el activo relacionado y por ende el riesgo.

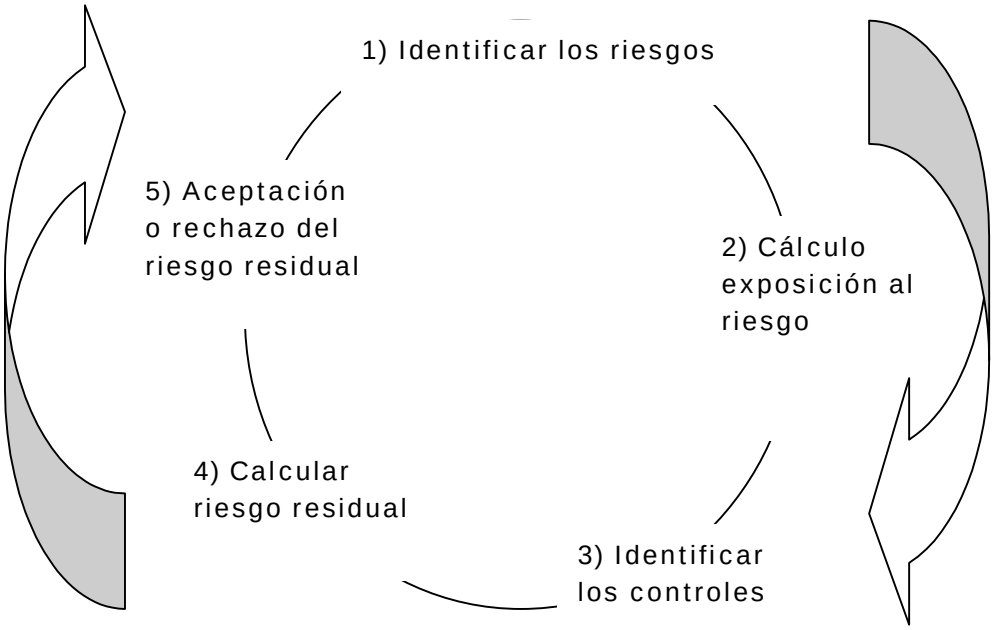
Compartir el riesgo: Mediante acuerdos contractuales se traspasa parte del riesgo (o su totalidad) a un tercero (un ejemplo son los seguros).

Aceptar el riesgo: Determinar que el nivel de exposición es adecuado.

La opción elegida deberá ser adecuadamente fundamentada y autorizada por el nivel jerárquico correspondiente sobre la base del riesgo asociado.

Proceso de administración del riesgo

El proceso de administración de riesgos es un proceso continuo, dado que es necesario evaluar periódicamente si los riesgos identificados y la exposición a los mismos calculada en etapas anteriores se mantienen vigentes. La dinámica en la cual se ven inmersa las organizaciones actualmente demanda este esfuerzo día a día. Es por eso que ante cada nuevo emprendimiento se realice en tempranas etapas (recomendable luego de fijar los objetivos) un análisis de riesgo del referido proyecto así como su impacto futuro en la estructura de riesgos de la organización.



Ejemplo de matriz de riesgos

En la siguiente hoja se presenta una matriz simplificada, donde:

- En cada fila se presenta una amenaza identificadas
- En la columna de probabilidad se indica cuán probable es que esa amenaza actúe, con independencia de los controles que existan o que se establezcan. La certeza es el 100% y la imposibilidad es 0%. Cada porcentaje de cada fila es manejado en forma independiente.
- En las columnas siguientes se indica para cada uno de los activos a proteger cuál es el importe de la pérdida media estimada que ocasionaría esa amenaza en ese activo. Por ejemplo, por servidores se entiende las computadoras centrales que soportan las bases de datos, la gestión del correo electrónico, la red Internet y otros servicios. Las terminales son los puestos de trabajo computarizados. Los datos son la información de la organización. Instalaciones se refiere a toda la parte física, incluyendo edificio, mobiliario, componentes de red (cableados, “routers”, “bridges”, “switches”), etc. Personal son los recursos humanos.
- Los datos precedentes permiten calcular la columna siguiente, riesgo total, el cual sumariza los productos de la probabilidad de la amenaza por el impacto, de toda la fila.
- A continuación se presenta la efectividad del control actuante, o sea qué nivel del riesgo total se puede mitigar. Por ejemplo, la amenaza de inundación puede ser mitigada ubicando el Centro de Cómputos en un piso elevado. Por otra parte, también suele estar bajo tierra, por razones de seguridad. Otro ejemplo: los accesos no autorizados vía Internet pueden ser mitigados con un “firewall” (barrera de control de accesos desde fuera y hacia fuera) correctamente configurado.
- Finalmente, en la última columna, se indica cuál es el riesgo residual, que resulta de aplicar la efectividad del control al riesgo total.

		Grado de impacto (US$miles)							
Amenazas	**Proba-bilidad**	**Servi-dores**	**Termi-nales**	**Datos**	**Instala-ciones**	**Per-sonal**	**Riesgo Total**	**Efec-tividad del control**	**Riesgo Residual**
Incendio	1%	10	5	8	62	41	1,26	100%	0
Inundación	1%	10	1	8	22	8	0,245	90%	0.0245
Accesos no autorizados	20%	1	0	12	0	0	2,6	50%	1.3
Fallas	25%	0,5	0,5	2	0	0	0,75	50%	0.375
Virus	30%	2	3	1	0	0	1,8	80%	0.36

Esta matriz a sido presentada para ejemplificar y no debe ser considerada como la única manera de instrumentar este tipo de herramientas. Existen abundantes metodologías que abordan el tema de distintas maneras.

Así es que en este ejemplo se podría haber planteado como filas los activos y como columnas las amenazas y la misma seguiría siendo válida.

Algunas estadísticas

Se considera de interés presentar algunas estadísticas, para que se comprenda mejor la relevancia del tema de riesgo informático.

Sigue un cuadro con la distribución de contingencias ocurridas, ya hace un cierto tiempo atrás, en Centros de Cómputo en el mundo[5].

Contingencia	Porcentaje
Incendios	17 %
Terrorismo	17 %
Huracanes y terremotos	25 %
Cortes de corriente	9 %
Errores de software	9 %
Inundaciones	7 %
Perforación de tuberías	5 %
Errores de Hardware	4 %
Cortes de comunicación	4 %
Otros factores	3 %
Total:	100 %

Según un estudio de Electronic Data Systems, sobre la capacidad de respuesta de las empresas de Manhattan, en Nueva York, frente a al corte de energía eléctrica ocurrido el 13/08/1990, se tiene: afectó a más de 1000 compañias, con 320 Centros de Cómputos, de los cuales 100 quedaron totalmente paralizados. Sólo 25% de estas compañías estaban preparadas frente al corte de corriente, con capacidad de recuperación del servicio informático inferior a 24 horas. El 75% restante tuvo un promedio de recuperación del servicio de 3 días!

Es obvia la relevancia de considerar planes de seguridad y para ello conocer el riesgo informático.

Controles

Los procedimientos efectuados para lograr asegurar el cumplimiento de los objetivos son definidos como controles.

El ayudar al cumplimiento de las metas indica claramente que estos procedimientos tienen un efecto directo mitigante sobre los riesgos existentes.

Como describimos en el punto anterior estas acciones mitigantes logran actuar sobre el riesgo total reduciendo la exposición al mismo a una medida menor (riesgo residual).

Por lo establecido anteriormente existe una relación biunívoca entre riesgo y control.

[5] Datos de Contingency Planning Research, Inc. Publicado en Sistemas y Tecnologías de la Información para la Gestión de Ignacio Gil Pechuán, 1996. Mc Graw – Hill. Págs 177 y 178

Es por ello intentamos cuantificar el riesgo al calcular el Riesgo Total (RT). El valor resultante nos indica cual debería ser el costo asociado al control que actúa sobre ese riesgo para ser eficiente.

Si bien al final volveremos sobre este tema, volveremos al ejemplo establecido en el punto anterior, para ilustrar mejor este concepto.

El RT calculado para un activo referente a la amenaza: incendio, es de $60, por lo tanto los costos anuales asociados al control que debo implantar no deben ser muy superiores a esa cifra, dado que si lo fueran estaría gastando más en la realidad que lo que eventualmente podría perder.

Los distintos procedimientos de controles pueden ser agrupados (sobre la base de los objetivos primarios que quieren satisfacer) en tres categorías, aquellos integrantes del sistemas de control interno, aquellos referidos a brindar seguridad y aquellos destinados a brindar calidad de las operaciones.

Estas categorías no son excluyentes, o sea existen procedimientos que se repetirán dentro de las tres categorías.

Como establecíamos anteriormente la agrupación se realiza sobre la base de objetivos de alto nivel que se quieren satisfacer, o sea estos procedimientos buscan que la información que procesan cuenten con cierta característica independientemente del objetivo específico por el cual fue creado (que como establecimos lo determinan los riesgos existentes).

De esta manera establecemos para cada grupo los objetivos a cumplir. Esta definición no es arbitraria sino que se basa en los marcos de referencia más recibidos, a saber COSO[6], ISO, SAC, etc.:

- **Control Interno** busca asegurar eficiencia y eficacia de las operaciones, cumplimiento de leyes, normas y regulaciones, y confiabilidad de la información (básicamente aquella publicable).
- **Seguridad** [5] busca asegurar la disponibilidad, confidencialidad e integridad de las operaciones.
- La **gestión de calidad** busca asegurar la adecuada calidad, entrega y costo de las operaciones.

El adecuado cumplimiento de los objetivos anteriormente detallados permitirá alcanzar una razonable seguridad en el cumplimiento de los objetivos planteados para los diversos procedimientos de TI.

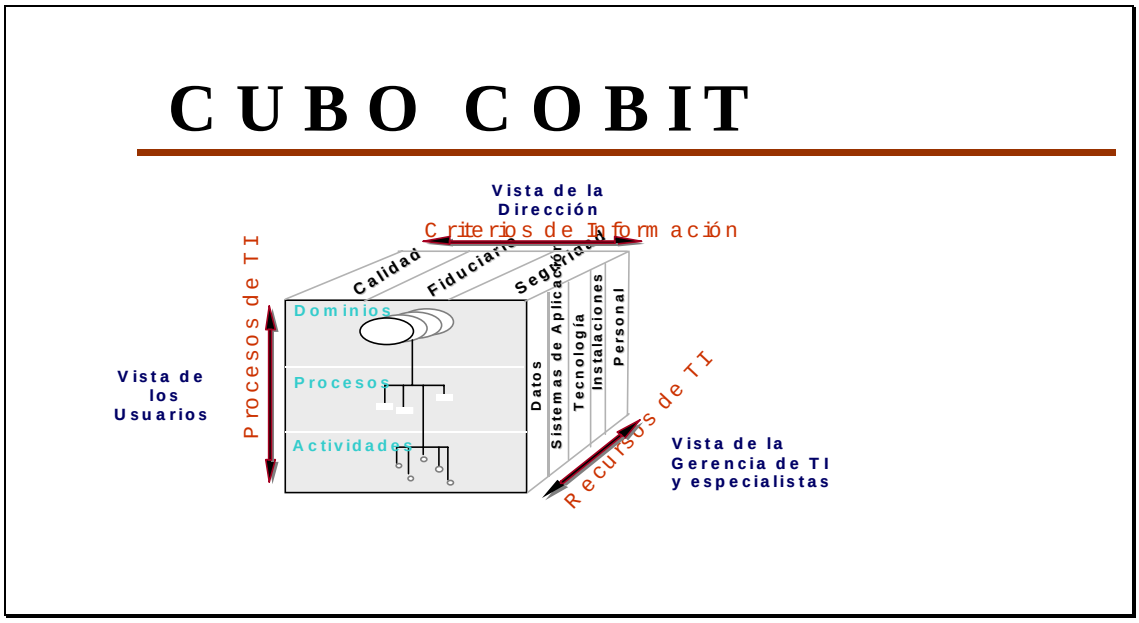
Existen marcos de referencia para una efectiva gestión de los recursos de tecnología, los cuales establecen los controles mínimos con los cuales debe contar una organización para lograr la misma.

Entre los marcos existentes mencionaremos especialmente el COBIT (Control Objectives for Information and Related Technology), el cual es un marco de referencia íntegro que incluye distintos aspectos de la gestión de TI, como ser el de los usuarios (estableciendo una estructura de controles aplicable a cualquier tipo de organización), el de los administradores de TI (estableciendo los indicadores de gestión aplicables a cada proceso vinculado a TI para lograr un cumplimiento eficaz y eficiente de las metas) y el del auditor (estableciendo guías de auditoría para una correcta evaluación de los procesos vinculados a tecnología).

Este marco de referencia ha sido elegido por el Banco Central del Uruguay para evaluar la gestión de tecnología de las empresas de intermediación financiera, a partir del año 2003.

COBIT define una serie de procesos relacionados con TI, los cuales agrupa en cuatro dominios (Planificación y organización, Desarrollo y adquisición, Soporte y Monitoreo), y los cuales estructura en distintas actividades. Estos procesos son adaptables a las distintas organizaciones y son la base para cualquiera de los enfoques utilizados para su implementación (usuarios, administradores de TI y auditores).

[6] Ampliar en el documento “Evaluación de paquetes contables”



Cuadro del "Cobit Framework" – ISACAF Information System Audit and Control Association Foundation

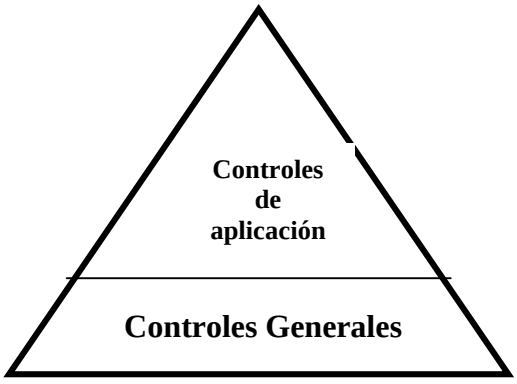
Los controles aplicables a los procesos vinculados a los procesos de TI se establecen en dos capas. La primera llamada de controles generales[7], contiene aquellos controles aplicables a los procesos que afectan a todo el procesamiento de información.

Y la segunda llamada de controles de aplicación4, que contiene los controles contenidos en las diferentes aplicativos que soportan determinados procesos del negocio y por ende procesan solamente determinado tipo de información.

Los controles generales se dividen en controles de acceso al sistema[8], estructura organizacional adecuada[9], mantenimiento de la continuidad del procesamiento[10] y controles sobre cambios no autorizados.

Mientras que los controles de aplicación se dividen en controles de acceso a las aplicativos, controles de ingreso de datos a los aplicativos[11], controles de procesamiento de los aplicativos$_8$ y controles sobre rechazos de los mismos.

La relación existente entre estos dos grupos de controles puede establecerse como piramidal, donde los controles generales son la base y los controles de aplicación se distribuyen sobre esta base hasta el vértice superior de esta pirámide virtual.



De lo anterior podemos concluir que una inadecuada estructura de controles generales no puede ser mitigada por una adecuada estructura de controles de aplicación.

[7] Ampliar en el documento "Evaluación de paquetes contables"
[8] Ampliar en el documentos "Seguridad Informática"
[9] Ampliar en el documento "Administración Informática"
[10] Ampliar en el documento "Respaldo y recuperación"
[11] Ampliar en el documento "Seguridad Informática"

Evaluación de la estructura riesgos/ controles

Existen distintos enfoques para poder evaluar la estructura de controles existentes en mi organización. Sin embargo el enfoque más generalmente aceptado es el que plantea el informe COSO[12], el cual evalúa esta estructura sobre la base de los riesgos existentes.

Este enfoque establece los siguientes pasos:

- Identificar los procesos de TI (pueden adaptarse los procesos definidos por COBIT)
- Identificar las actividades que componen cada procesos (pueden adaptarse las actividades definidas por COBIT para cada proceso)
- Identificar los objetivos de cada actividad
- Identificar los riesgos asociados a tales objetivos
- Identificar los controles actuantes relacionados a cada riesgo
- Establecer la exposición al riesgo de cada actividad (ver Administración y análisis de riesgos)
- Analizar lo adecuado de los controles identificados sobre la base de los riesgos identificados

Como se puede observar este enfoque integra los conceptos de análisis de riesgos, evaluación de controles y evaluación de objetivos operacionales.

De esta manera puedo analizar:

- si los objetivos operacionales se encuentran alineados con los objetivos del negocio
- los riesgos asociados, para lograr una adecuada administración de los mismos
- la estructura de controles existentes, identificando vulnerabilidades o debilidades

El proceso de evaluación se plasmará en una matriz de riesgo donde se podrán visualizar los elementos identificados y sus relaciones.

Este documento deberá ser actualizado periódicamente para poder continuar siendo vigente y útil para la organización. Generalmente las actualizaciones son anuales, pero si los procesos normales de monitoreo existentes identifican cambios estos deben impactar rápidamente en la matriz para poder tomar decisiones eficaces y oportunas.

Conclusiones

Más allá de todo lo expuesto a lo largo de este documento, no se debe olvidar nunca que los riesgos cohabitan continuamente con el diario quehacer, siempre están latentes, aún cuando no se los pueda o no se los quiera identificar.

Es por esto, que, independientemente de las herramientas utilizadas para la administración de los riesgos, lo más importante es que exista conciencia que la administración del riesgo informático debe ser una actividad prevista y llevada a cabo al igual que la implementación y el funcionamiento de sistemas de información.

Recordar que la única manera que evitar un riesgo es eliminar la, o las actividades que lo genera. Hay actividades que pueden ser eliminadas y otras no, son necesarias. Por lo tanto, en el tema que se está tratando, es imprescindible la adecuada administración del Riesgo Informático.

[12] Ampliar en el documento “Evaluación de paquetes contables”

Textos vinculados

Todos los textosd están disponibles en la página Web de Facultad, bajo Cátedra Introducción a la Computación, del Departamentode Métodos Matemático – Cuantitativos. Además, están editadospor la Oficina de Apuntes del CECEA.

"Aspectos legales, derechos ded autor y piratería de software", Simón Mario Tenzer, 26 páginas.

"Elementos de Organización de la Función Informática" (Administración Informática), 19 páginas.

"Evaluación de paquetes contables" (sólo para Opción Administrativo / Contable), Beatriz Pereyra, 14 páginas. Incluye **"Integración de las actividades de control con la evaluación de riesgos."**

"Respaldo y Recuperación de Datos", Simón Mario Tenzer y Nelson Pequeño, Julio 2000, 17 páginas.

"Seguridad Informática", Leonardo Sena Mayans, Julio 2000, 11 páginas.

"Virus informático", Setiembre 2002, 21 páginas.