Manual de supervivencia de Seguridad de la Información

Episodio 1:

Fundamentos

Juan Ignacio Trentalance

Manual de supervivencia de Seguridad de la Información.
Episodio 1: Fundamentos.

(c) Juan Ignacio Trentalance, 2009, 2010, 2011.
Todos los derechos reservados.

Cualquier comentario que el lector desee sobre este libro será bienvenido en la siguiente dirección de correo electrónico:

jtrental@gmail.com

Se permite citar partes del libro, enviarlas por email a terceros, imprimirlas y publicarlas en blogs y otros medios, con la condición de que no se modifique ni edite el texto, y se incluya el nombre del autor y la dirección de internet para descargar el material. El derecho de encuadernar este material y venderlo en forma de libro está estrictamente reservado.

Este libro es una obra en progreso y el presente documento data del 30 de noviembre de 2011. La última versión se puede descargar en:

http://www.portoyasociados.com.ar/manual_seginf_episodio1.pdf

Agradezco especialmente a Karina Macció y a Marcelo Mastromarino, quienes soportaron la lectura de esta obra y me hicieron una detallada devolución con sus mejoras y aportes.

Índice

1 Por qué este libro 5
1.1 Tres episodios para un recorrido personal 6
1.2 Episodio 1 – Fundamentos para el iniciado 6
2 La Seguridad de la Información 8
2.1 Por qué protegemos la información: datos, información y sistemas 9
2.2 Qué significa proteger la información 10
2.3 Las buenas prácticas en Seguridad de la Información 11
2.4 Política y Dirección 14
2.5 Activos de información 16
2.6 Clasificación de la Información 18
3 Gestión de Riesgos 19
3.1 Análisis de Riesgos 21
3.2 Análisis de Riesgos Cuantitativo 22
3.3 Análisis de Riesgos Cualitativo 23
3.4 Valoración de Riesgos 26
3.5 Tratamiento de Riesgos 29
4 Controles Administrativos 33
4.1 Aspectos Organizacionales 34
4.2 Roles y Responsabilidades 35
4.3 Documentación 36
4.4 Gestión de Incidentes 39
4.5 Gestión de la Continuidad del Negocio 41
4.6 Cumplimiento (*Compliance*) 43
5 Controles Tecnológicos y Físicos 45
6 Epílogo 47
A. Anexos 49
A 1. Bibliografía utilizada 49
A 2. Acerca del Autor 50

1 Por qué este libro

Durante una de las primeras clases del posgrado que cursé en la Universidad de San Andrés (Gestión de Servicios Tecnológicos y de Telecomunicaciones) nuestro profesor de Introducción al *Management* nos comentó "¿ustedes piensan que el negocio de[l principal grupo empresario industrial de la Argentina] Tenaris es la manufactura de caños sin costura? Piensen de nuevo, el 80% lo constituye la capacidad de la empresa para *entregar en tiempo y forma* ese caño en algún lugar remoto del mundo, ya sea en una plataforma petrolera del Mar del Norte, o en el medio del desierto en Arabia Saudita".

A principios de la década del '70, los países centrales iniciaron una transformación donde dejaron paulatinamente de ser sociedades industriales para convertirse en **sociedades de la información** o **del conocimiento**[1]. La generación de la riqueza dejó de estar tan vinculada a la producción de bienes tangibles para dar paso, cada vez más, a la prestación de distintos tipos de servicios: diseño, entretenimiento, educación, provisión de un producto, transporte, etc. El servicio de *delivery*, o entrega de un producto, es más trascendente que su manufactura.

Esta transformación fue posibilitada por el explosivo avance, difusión y abaratamiento de la tecnología informática subyacente (el *hardware*, el *software*, las redes de comunicación, etc.), hasta tal punto que la **generación**, **almacenamiento** y **transmisión** de la información, se ha vuelto un aspecto fundamental en la economía de la mayoría de las naciones.

Hoy en día es difícil concebir un trabajo de oficina sin el uso de una extensión telefónica personal, una computadora con correo electrónico corporativo, la posibilidad de compartir documentos en formato digital y el acceso a Internet. Atrás han quedado los memos mecanografiados. De hecho, a pesar de haber trabajado durante 6 años en una oficina en una empresa de más de 3000 personas sólo en la Argentina, sólo hace relativamente poco entendí a qué se refieren en las películas cuando un empleado le dice al otro "¿acaso no leíste el último *memo*?" Nunca tuve que *usar* un memo. Levantaba el teléfono para comunicarme y en todo caso enviaba un correo electrónico (corporativo) para "dejar algo por escrito". Todavía me sorprende que determinados campos de un *mail*, como "destinatario", "copia de carbón" o "asunto" se hubieran usado antes en los *memos* ("uy, como si fuese un mail", pienso yo en el cine).

La información ha cobrado un rol preponderante para nuestra vida en general (y para las organizaciones en particular), cuidarla es una tarea que se vuelve cada vez más relevante. Dicha problemática ha sido tratada por Scott Adams,

[1] La sociedad de la información es un término popularizado por el autor Fritz Machlup, en su trabajo "La producción y distribución del conocimiento en los Estados Unidos" de 1962. Los términos sociedad de la información y sociedad del conocimiento no significan exactamente lo mismo, pero su discusión excede el objetivo del libro.

autor de la tira cómica Dilbert[2], basada en un ingeniero homónimo que trabaja en una gran corporación de productos y servicios de tecnología. Las tiras cómicas de Dilbert expresan de una manera muy inteligente las relaciones humanas en el contexto de una gran organización, y el impacto de sus productos y servicios en las personas. En una de las tiras aparece la mamá de Dilbert, donde la computadora le indica que el software de seguridad se ha desactualizado y le presenta dos opciones:

> ¿Desearía pasar el resto de su vida natural tratando de entender cómo actualizarlo?...
> ... ¿o preferiría dejar que los hackers le roben la identidad, vacíen su cuenta bancaria, y destruyan su disco rígido?[3]

1.1 Tres episodios para un recorrido personal

Este manual forma parte de una **trilogía** sobre el proceso de implementación de las buenas prácticas de Seguridad de la Información en una organización. Su contenido está inspirado en la recopilación de una serie de conferencias que presenté en diversos ambientes a lo largo de los últimos 6 años[4]. El recorrido de los temas sigue mi propia evolución como profesional de la Seguridad de la Información. Los tres episodios son:

1. **Fundamentos:** cuáles son las actividades, recursos y técnicas que debemos gestionar según las buenas prácticas de Seguridad de la Información.
2. **La organización y la seguridad:** cuáles son los desafíos a la hora de pasar de la teoría a la práctica, cuáles son los "cuellos de botella" y los problemas con los que nos encontramos.
3. **Sistemas de gestión:** cómo superar en la práctica los desafíos planteados implementando un Sistema de Gestión de Seguridad de la Información[5].

1.2 Episodio 1 **–** Fundamentos para el iniciado

[2] También es autor de varios libros cómicos que en algunas librerías los he visto en la sección "Management". Ver por ejemplo, Adams, Scott: *The Dilbert principle*, Nueva York, Harper Collins, 1997.

[3] La fuente de esta tira cómica es http://www.dilbert.com, la fecha de publicación es 12 de abril de 2006.

[4] Entre otros, en eventos organizados por ISSAArBA (Information Systems Security Association, capítulo de Buenos Aires, Argentina) junto con Microsoft, Universidad de Buenos Aires (UBA), Universidad Tecnológica Nacional y el capítulo argentino de AFCEA (Armed Forces Communications and Electronics Association); en eventos de la industria como Infosecurity y Segurinfo; y como docente de posgrado de la Especialización en Servicios y Redes de Telecomunicaciones de la Facultad de Ingeniería de la UBA.

[5] En el contexto de este libro, el término **Sistema de Gestión** no se utiliza para denotar un **Sistema Informático** (en el sentido de un *software* que corre sobre un determinado *hardware*), sino todos aquellos elementos (*personas*, *procedimientos*, *políticas*, *tecnología*, etc.) utilizados para dirigir o gobernar una organización.

Hace unos meses, durante una consultoría en una empresa de desarrollo de *software* que quería implementar seguridad en sus productos, me topé con la siguiente inquietud del CEO y fundador: “ya me leí tres libros de Seguridad Informática, y todavía no logro entender la diferencia entre *vulnerabilidad* y *amenaza*”. Se trata de una empresa dedicada al rubro del *marketing online* que empezó como un emprendimiento y terminó posicionada como uno de los líderes de esa industria. Quienes conocen del tema de *entrepreneurship* (¿emprendedorismo?) aseguran que hay un momento crítico para la supervivencia de una empresa, que es cuando la demanda aumenta abruptamente (durante lo que se conoce como período ventana). En ese momento, el emprendedor debe hacer *escalar* el negocio. Esto es, principalmente, invertir para agrandar la capacidad de la organización y cubrir dicha demanda, pero también, ordenar todos sus procesos de negocio para conservar la homogeneidad de la calidad del servicio o producto. No es de sorprender, entonces, que un buen emprendedor (sobre todo en la industria de servicios tecnológicos) haya considerado a la Seguridad de la Información de su empresa como uno de las claves de su supervivencia.

Mi respuesta fue: “la explicación detallada de esa sutil, pero importante diferencia la vas a encontrar en un libro que estoy escribiendo” y acto seguido produje el borrador de este trabajo (quienes se estén preguntando por esta diferencia, pueden consultarla en el capítulo 3). Posteriormente, las oportunidades de “quedar bien con clientes” se empezaron a multiplicar, hace unas pocas semanas, la flamante Gerente de Seguridad Informática de una importante empresa multinacional financiera me dijo “la verdad es que tengo más de 20 años de experiencia en Tecnología, y hasta hace 3 meses era la Gerente de Tecnología, pero por estos cambios organizacionales de las grandes empresas me tocó formar un área casi desde cero, ¿existe un curso elemental o bibliografía para que en no más de 15 días yo pueda estar preparada para enfrentar este desafío?”

Si bien yo ya tenía la decisión tomada de publicar un libro de Seguridad de la Información, fue durante estas experiencias que fue madurando en mi cabeza la idea de volcar en un **manual** (de supervivencia, agregaría posteriormente) mi experiencia aplicando en la práctica los conocimientos teóricos sobre la *gestión* de la Seguridad de la Información. Los primeros capítulos introductorios del libro se transformaron entonces en el primer episodio de la serie, una suerte de compilación de “preguntas frecuentes” (o FAQ por sus siglas en inglés) con un enfoque gerencial, pensadas para un público sin demasiados conocimientos en la disciplina. Para quienes tengan ya algunas nociones, es recomendable leer el capítulo 2 completo y continuar con una lectura salteada de las secciones que siguen, hasta llegar a los capítulos 5 y 6 donde se presentan las conclusiones del episodio 1.

En este episodio se desarrolla, con cierto detalle, el contenido de las buenas prácticas de Seguridad de la Información, qué implicancias tienen éstas sobre las organizaciones, y qué elementos debemos gestionar (con la conclusión implícita de que *no son pocos*) para dar una idea de la magnitud del esfuerzo.

2 La Seguridad de la Información

Hace unos años se decía que los profesionales en el área de “Seguridad Informática” debíamos preocuparnos sólo por la seguridad, y que de la funcionalidad se preocuparan los usuarios. Desde el punto de vista de lo actitudinal, éramos “profundamente paranoicos” y “restrictivos” para con los “malditos usuarios”. Para nosotros, la seguridad era lo contrario de la funcionalidad, y nuestra misión consistía en buscar los medios para impedir que la tecnología fuese usada de manera “insegura” en la organización. Nunca nos habíamos puesto a analizar en detalle cuál era la **información** que debíamos proteger, ni cuál era su importancia para el negocio, ni por qué era tan importante protegerla. Tratábamos de proteger *toda* la información que encontrábamos, con la misma intensidad y esfuerzo.

La imagen del analista de seguridad paranoico ha sido retratada en varias oportunidades por Scott Adams en la tira de Dilbert a través del personaje Mordac (quien, cada vez que aparece en escena es descripto como el "impedidor de Servicios Informáticos"). En una reciente tira, Mordac define:

> La seguridad es más importante que la usabilidad.
> En un mundo perfecto, nadie debería ser capaz de usar nada.[6]

Este enfoque se ha demostrado poco útil por varios motivos. Para empezar, es ineficiente, porque al proteger la información “por la información misma” se gastan los recursos de manera arbitraria, llegándose a casos en los que lo que se protege vale mucho menos que lo que cuesta protegerlo. Es ineficaz, porque si no entendemos cuál es la función que cumplimos para el negocio de nuestra organización, corremos el riesgo de olvidarnos de las amenazas más importantes. En un ejemplo de mi experiencia profesional, recuerdo que protegíamos con celo la seguridad de la red mediante reglas del firewall, pero omitíamos involucrarnos en el proceso de desarrollo (y adquisición) de los sistemas comerciales (ERP, CRM, etc.), donde se almacenaba buena parte de la información del negocio.

En el largo plazo, esta actitud genera una suerte de “resistencia biológica” en los usuarios, que se convierten en “hackers por necesidad”, porque las trabas impuestas para que puedan desarrollar sus actividades son tan grandes (a ellos se les paga por *usar* la información, no por protegerla) que terminan encontrando los medios para, o bien “bypassear” los controles, o peor, evitar a que la gente de seguridad participe de los nuevos proyectos. Esto vuelve imposible la toma de conciencia de los usuarios, porque ¿cómo van a apoyar una iniciativa que les impide llevar a cabo el negocio de la organización?

En este capítulo cubriremos los aspectos estratégicos de la gestión de la Seguridad de la Información. La estrategia se fija de acuerdo con una serie de directrices o ideas fuerza hacia las que la organización quiere avanzar, tales

[6] La fuente de esta tira cómica es http://www.dilbert.com, la fecha de publicación es 16 de noviembre de 2007. El personaje es "Mordac, the preventer from information systems".

como gestionar los riesgos del negocio, aprender de los incidentes, identificar controles técnicos, administrativos y físicos, entre otras. Muchas de las directrices que una organización debe considerar para su estrategia de Seguridad de la Información son recopiladas en las llamadas **buenas prácticas** (o "la teoría"), que serán el principal foco del episodio 1. Otro aspecto importante es la identificación de los activos relacionados con la información que se quieren proteger, y con qué prioridad o clasificación.

2.1 Por qué protegemos la información: datos, información y sistemas

Volvamos brevemente a la introducción del capítulo 1 y preguntémonos por qué, (o para qué) necesitamos proteger la información. La madre de Dilbert se enoja porque no tiene suficientes conocimientos para tomar una decisión (proteger su vida personal) y necesita "más opciones". El sistema le ofrece una cantidad de datos que ella es incapaz de manejar.

Para contestar la pregunta, debemos considerar las siguientes definiciones:[7]

- **Dato:** es una forma abstracta de representar un aspecto de la realidad, por ejemplo, una cantidad de algo.
- **Información:** son los datos previamente seleccionados, o procesados de alguna manera que ayudan a alguien en la toma de decisiones.

Un dato puede o no ser información, en función de quién lo utiliza. La misma *información* que a un especialista en computación le permite actualizar su antivirus y proteger su computadora, para la madre de Dilbert son *datos* abstractos e inentendibles. De igual manera, muchos datos no necesariamente equivalen a mucha información. Para ilustrar esto de una manera muy sencilla, tomemos la definición que da la norma ISO 9001:

Información: datos que poseen significado[8].

Los datos son convertidos en información, y la información es adquirida, procesada, almacenada, transmitida, y presentada por sistemas (informáticos, de comunicaciones, lingüísticos, etc.). Existe toda una Teoría de Sistemas de principios del siglo XX[9]. Un **sistema** es una entidad compuesta por un conjunto de partes interrelacionadas que, por lo general, tiene un objetivo; toma una entrada, realiza un proceso y se obtiene una salida; tiene demarcado un límite (afuera y adentro del sistema); su comportamiento es

[7] Estas definiciones están tomadas de Saroka, Raúl Horacio: *Sistemas de la Información en la Era Digital*, Buenos Aires, Fundación OSDE, 2002.
[8] *ISO 9000:2005 - Sistemas de Gestión de la Calidad - Fundamentos y Vocabulario*, Suiza, ISO, 2005 (traducción certificada), sección 3.7. La familia de normas ISO 9000 (ISO 9000, ISO 9001 e ISO 9004) son una compilación internacional de buenas prácticas de gestión de la calidad, ampliamente utilizadas, validadas y actualizadas a lo largo de varias décadas, en varias organizaciones a lo largo del mundo. Los estándares ISO se tratan con más detalle en el episodio 3.
[9] Saroka, ibid.

difícil de explicar considerando sus componentes por separado; y puede estar contener subsistemas o ser parte de un sistema más grande en una jerarquía de sistemas (por ejemplo, un planeta y sus lunas es un sistema dentro del sistema solar).

Los sistemas pueden usarse en varios contextos: sistemas de información (cuando las entradas y salidas del sistema son información), sistemas de comunicaciones, sistemas solares, un proceso de negocios, una organización, la sociedad (por ejemplo, el "sistema capitalista"). Tal vez la revolución producida por el abaratamiento de la electrónica (ya mencionado en el capítulo 1) hace que muchas veces se piense en un *software* corriendo sobre un *hardware* al referirnos a un sistema informático. Sin embargo, en lo que resta del capítulo, vamos a utilizar el significado más amplio posible (en especial más adelante, cuando hablemos de sistemas de gestión).

La información es importante en la organización porque nos permite tomar **decisiones** informadas -valga la redundancia- y en consecuencia, el flujo de intercambio entre los distintos componentes de la organización (el sistema) es vital para la realización de su **negocio**. Hablamos de cualquier tipo de organización, no sólo las comerciales, por lo que debe entenderse por "negocio" a su actividad, misión, o razón de ser.

2.2 Qué significa proteger la información

Cuando hablamos de Seguridad de la Información, nos referimos a la preservación de tres propiedades fundamentales[10]:

- **Confidencialidad:** propiedad por la cual la información se mantiene disponible y es divulgada sólo a individuos, organismos o procesos autorizados.
- **Integridad:** propiedad de proteger la precisión y la totalidad de la información.
- **Disponibilidad:** propiedad de que la información se mantenga accesible y sea utilizable a demanda por parte de un organismo autorizado en tiempo y forma.

Por otro lado, podemos referirnos a estas tres propiedades en función de sus principales amenazas:

- **Divulgación:** cuando se produce una pérdida o falta de confidencialidad en la información. Por ejemplo, cuando se hacen públicos los planos del prototipo de un producto nuevo que está por salir al mercado.
- **Alteración:** cuando se produce una pérdida o falta de integridad en la información. Por ejemplo, los datos de un balance comercial deben ser

[10] Estas definiciones están ligeramente modificadas de *ISO/IEC 27001:2005 – Information technology – Security techniques – Information security management systems – Requirements*, Ginebra, ISO, 2005. Ver la sección 2.3 para una breve explicación de esta norma.

apropiadamente protegidos de alteraciones para presentar a los accionistas el estado financiero de la empresa en forma confiable (recordemos el escándalo Enron).
- **Destrucción (o Denegación de Servicio):** cuando se produce una pérdida o falta de disponibilidad en la información. Una denegación de servicio puede impedir que se acceda a determinada información, a pesar de que su confidencialidad o integridad dentro del sistema no se hayan afectado.

Existen otras propiedades adicionales que nos interesa preservar en la información, como por ejemplo, la **Autenticidad** (que la fuente de la información sea identificada en forma confiable), el **No Repudio** (que existan mecanismos que impidan a la fuente decir posteriormente que no generó esa información), y el **Registro de la Responsabilidad** (o Accountability, que se puedan consultar las personas o entidades que modificaron, o accedieron a la información, junto con día, hora, etc.), entre otras. En general, no son propiedades de la información en sí, sino de las entidades que la generan, transmiten o manipulan, y que indirectamente preservan las tres propiedades fundamentales.

2.3 Las buenas prácticas en Seguridad de la Información

En la sección anterior se establecieron los objetivos de la Seguridad de la Información (las propiedades que debemos preservar y las amenazas que debemos prevenir). Pero desde el punto de vista de la gestión, se presentan grandes desafíos para mantener el esfuerzo a lo largo del tiempo. Para tal fin, distintos sectores de la sociedad han empezado a recopilar una serie de buenas prácticas, bastante alineadas entre sí:

- **Normas ISO/IEC 27001:2005 y 27002:2005:** son los requisitos para la implementación de un Sistema de Gestión de Seguridad de la Información (similar al Sistema de Gestión de la Calidad basado en ISO 9001) y el código de buenas prácticas de Seguridad de la Información, respectivamente.
- ***Common Body of Knowledge (CBK)* del *International Information Systems Security Certification Consortium* o (ISC)^2:** es el cuerpo de conocimiento mantenido desde hace varios años por (ISC)^2 como las buenas prácticas que un profesional de Seguridad de la Información debe manejar[11].
- ***COBIT (Control Objectives for Information and Related Technology)* del *Information Technology Governance Institute (ITGI):*** son las buenas prácticas relacionadas con la tecnología de la información desde el punto de vista de la gobernabilidad y el control interno.
- ***National Institute of Standards and Technology* (NIST) - *Information Technology Security and Networking* (ITSN) *Division*:** es un organismo gubernamental de Estados Unidos que provee buenas prácticas de

[11] Este consorcio es el que Certifica a los Profesionales de Seguridad de la Información (CISSP, *Certified Information Systems Security Professional*).

"Seguridad Informática", relacionadas con la tecnología y las redes de comunicaciones, pero que no son ajenas a la evolución hacia el enfoque integral del que venimos hablando.

Si bien existen muchas escuelas y orígenes para las buenas prácticas, poco a poco, la industria de la Seguridad de la Información en su conjunto ha empezado a entender que lo importante para mantener en el tiempo el esfuerzo de protección es cómo *gestionamos* una amplia variedad de elementos (**procesos**, **personas** y **tecnología**) para proteger los activos[12] de información de las amenazas (ver esquema de la figura 2.1).

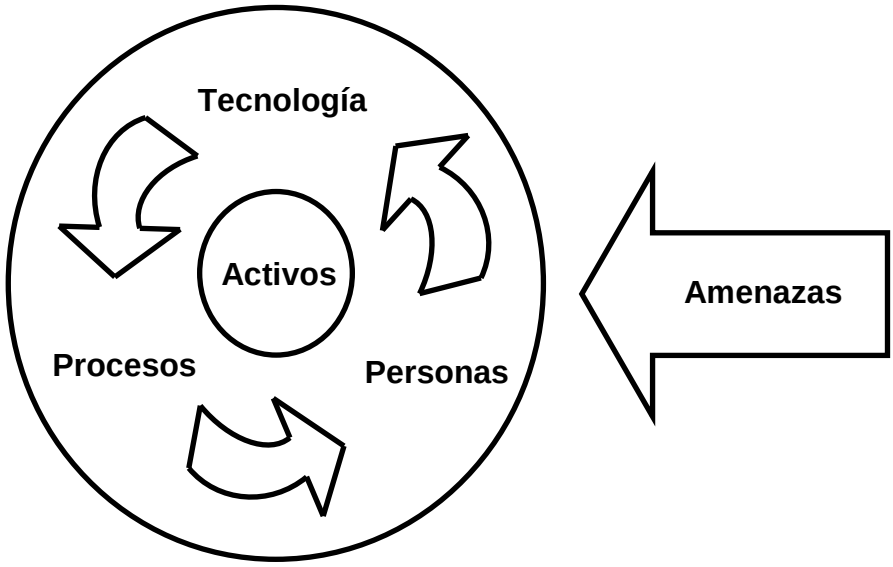

Figura 2.1. Cómo gestionamos la Seguridad de la Información.

Más específicamente, todas las buenas prácticas coinciden en lo siguiente:

- Se alinea la Seguridad de la Información con el **negocio,** y se reconoce que es una función estratégica del negocio, pero no un fin en sí mismo.
- Se agrega el apoyo de la **Alta Dirección** como factor clave de éxito.
- Se gestionan **procesos, personas y tecnología**.
- Se identifica qué información proteger, de qué amenazas y cómo hacerlo con una metodología de **gestión de riesgos**.
- Se habla el mismo lenguaje que "el Director de Finanzas", y cuando es posible, hasta se calcula el **retorno de las inversiones** en Seguridad de la Información.
- Se separa la función de Seguridad de la Información de las áreas de Tecnología o Sistemas y se la coloca como **área de staff** para que exista un control por oposición de intereses (seguridad versus funcionalidad).
- Se implementa un programa de **entrenamiento** y **toma de conciencia** en seguridad para usuarios, administradores, y otros involucrados.

[12] Los activos de información se verán con más detalle en la sección 2.5.

- Se **amplía el alcance** de la Seguridad de la Información para abordar otros temas como Seguridad Física, Continuidad del Negocio, Recursos Humanos y Cumplimiento.

El cambio cultural en los últimos años ha sido tan profundo en lo referido a las buenas prácticas, que en español hemos aceptado de buena gana reemplazar en nuestro vocabulario el término "Seguridad *Informática*" por "Seguridad *de la Información*". De esta manera se enfatiza la idea de que debemos proteger la información en cualquier medio en el que se encuentra, no solamente en los informáticos. Para ilustrar lo anterior, véase en la tabla 2.1 la comparación entre los *títulos*[13] en los que se organizan los controles de seguridad en la norma ISO/IEC 27001 y los capítulos del CBK del (ISC)^2.

ISO / IEC 27001	*Common Body of Knowledge* del (ISC)^2
A 5. Política de seguridad *(Security policy)*	Gestión de la Seguridad de la Información y del Riesgo *(Information Security and Risk Management)*
A 6. Organización de la Seguridad de la Información *(Organization of Information Security)*	
A 7. Gestión de Activos *(Asset Management)*	
A 8. Seguridad de recursos humanos *(Human resources security)*	
A 9. Seguridad física y ambiental *(Physical and environmental security)*	Seguridad Física (Ambiental) *(Physical (Environmental) Security)*
A 10. Gestión de las comunicaciones y operaciones *(Communications and operations management)*	Seguridad en Operaciones *(Operations Security)*
	Seguridad en Telecomunicaciones y Redes *(Telecommunications and Network Security)*
A 11. Control de accesos *(Access control)*	Control de Accesos *(Access Control)*
A 12. Adquisición, desarrollo y mantenimiento de sistemas de información *(Information systems acquisition, development and maintenance)*	Seguridad en Aplicaciones *(Application Security)*
A 13. Gestión de incidentes de seguridad de la información *(Information security incident management)*	

[13] En la tabla sólo hemos comparado los títulos, si además comparásemos el contenido, la correspondencia sería aún mayor.

ISO / IEC 27001	*Common Body of Knowledge* del (ISC)[2]
A 14. Gestión de la continuidad del negocio *(Business continuity management)*	Continuidad del Negocio y Planificación de la Recuperación de Desastres *(Business Continuity and Disaster Recovery Planning)*
A 15. Cumplimiento *(Compliance)*	Legislación, Reglamentaciones, Cumplimiento e Investigaciones *(Legal, Regulations, Compliance and Investigations)*
	Criptografía *(Cryptography)*
	Arquitectura y Diseño de Seguridad *(Security Architecture and Design)*

Tabla 2.1. Comparación entre los títulos de ISO 27001 y el CBK de (ISC)[2].

De la "Seguridad Informática tradicional" se encargan los controles en A.10, A.11 y A.12 de la norma ISO 27001 (en el CBK tiene más representación[14]: Arquitectura y Diseño de la Seguridad, Seguridad en Aplicaciones, Criptografía, Control de Accesos, Seguridad en Telecomunicaciones y Redes, y Seguridad en Operaciones). A estos componentes se han agregado una serie de controles administrativos para gestionar correctamente el inventario de activos de información (A.7), la seguridad del personal (A.8), los incidentes (A.13) y el cumplimiento (A.15). También se incorporan aspectos de seguridad física y ambiental (A.9), continuidad del negocio (A.14), junto con otros aspectos organizacionales, como establecer una política corporativa (A.5), y organizar las responsabilidades de la seguridad (A.6) (en el CBK estos contenidos se encuentran en el capitulo de Gestión de la Seguridad de la Información y del Riesgo).

2.4 Política y Dirección

"Alta Dirección" o simplemente "Dirección", es un término muy utilizado para referirse a los altos niveles jerárquicos de una organización, ya sea el "Dueño", el "CEO", el "Presidente", el "Directorio", los "Gerentes", etc. En cualquiera de sus facetas, la Alta Dirección tiene un eje común: la necesidad de tomar rápidamente decisiones trascendentes para mejorar el negocio. Casi siempre involucran algún tipo de **inversión**, ya sea en dinero, en tiempo, o simplemente asignando prioridades (qué tareas relegar cuando los recursos son escasos). Es por este motivo que sin el apoyo de la Alta Dirección, no es posible mantener a lo largo del tiempo -ni siquiera empezar, en verdad- el esfuerzo de seguridad.

[14] Esto es esperable, ya que el CBK apunta más a los conocimientos técnicos y de gestión que un profesional debe "conocer", mientras que ISO 27001 apunta a los controles que deben considerarse para mantener la Seguridad de la Información. Los alcances son claramente distintos.

La Seguridad de la Información no debe convertirse en un “proyecto” que una “oscura área técnica” dentro de una gerencia debe “vender” internamente en los niveles altos de la organización, sino un **concepto** que la Alta Dirección entiende, acepta y “baja” por el organigrama a las demás áreas. Tampoco puede ser un “proyecto asignado” a un área, sin la provisión de recursos adecuados, ni la alineación de los demás sectores de la organización.

La Alta Dirección tiene, sin embargo, ciertas responsabilidades que cumplir. Después de todo, frente a un incidente de seguridad, es ésta quien debe dar explicaciones a sus accionistas, clientes, público, y demás partes interesadas (o *stakeholders*). Debe establecer efectivamente la **intención** de implementar un programa de seguridad para que la organización en su conjunto sepa hacia dónde se dirige, y cuáles son los objetivos perseguidos.

En primer lugar, debe publicar y establecer una **Política Corporativa de Seguridad**. Se trata de una “expresión de deseo” de muy alto nivel que establece las directrices que se van a seguir en el esfuerzo de seguridad. Es concisa, resumida, y típicamente dice “el qué”, pero no “el cómo”. Es un documento que, si bien debe mantenerse actualizado y aplicable al negocio, no cambia con frecuencia.

Luego debe diseñar adecuadamente la **estructura organizacional** para que las responsabilidades de Seguridad de la Información puedan cumplirse realmente, por ejemplo, estableciendo un área de staff de seguridad, para mantener el principio de control por oposición de intereses (como ya dije, funcionalidad versus seguridad). El concepto de control por oposición de intereses no siempre es bien entendido por los administradores de seguridad. Muchas veces se traduce en una necesidad de “pelearse” con las “áreas controladas” y convertirse en una “máquina de impedir” (como Mordac en la tira de Dilbert). Es una actitud inútil, ya que a la larga va a prevalecer la necesidad de funcionalidad por sobre la seguridad que requieren tanto el negocio como la Alta Dirección. En definitiva, debe ser una característica del diseño de la estructura organizacional, más que una motivación de un área funcional.

Las responsabilidades de la Alta Dirección no terminan aquí. Debe evitarse que la Política se convierta en “letra muerta”, para lo que se requiere que las personas de la organización no solamente lean, sino que entiendan en qué medida sus funciones aportan al cumplimiento de los objetivos de seguridad (y en definitiva, a la Política). Asimismo, la Alta Dirección debe proveer los recursos suficientes para desplegar los lineamientos de la Política. Por ejemplo, invirtiendo dinero para adquirir tecnología, modificar procesos, y entrenar a las personas, pero también asignando responsabilidades y priorizando adecuadamente las tareas.

Las nociones de **Responsabilidad de la Dirección** y **Política de Seguridad** sientan las bases para gestionar exitosamente un programa de seguridad. En ese sentido, constituye el primer hito, sin el cual carece de propósito seguir avanzando en técnicas y recomendaciones de seguridad. La experiencia demuestra que la Seguridad de la Información no existe fuera del negocio de

una organización. Sin éste, la seguridad carece de propósito. La seguridad *sirve* al negocio, y tiene sentido en la medida en que ésta proteja la información relacionada con el negocio. Esta visión, cada vez más aceptada por las buenas prácticas, es en realidad una obviedad para la Alta Dirección, y se aplica desde hace muchos años a todas las funciones de una organización, en especial, en aquellas actividades consideradas de soporte. La pregunta implícita en la mente de todo gerente general a la hora de invertir recursos es "¿Cómo va a mejorar esto nuestro negocio?".

Es en este punto donde se espera del responsable del área Seguridad de la Información que sea lo suficientemente inteligente como para justificar, en términos del negocio, los recursos requeridos. Si un oficial de seguridad empieza a hablar en términos absolutos (se convierte en una máquina de impedir) o trata de generar miedo, incertidumbre y duda (o FUD, por fear, uncertainty and doubt) puede pasar que se malgasten los recursos en actividades que no aportan al negocio, y/o que no se le asignen los recursos necesarios para protegerlo adecuadamente.

2.5 Activos de información

Normalmente, cuando pregunto en una organización "¿cuál es la información que es importante para el negocio que se proteja?" suelo obtener respuestas como las siguientes: "yo quiero que la gente no baje programas con virus de Internet", "me gustaría contar con una sala donde se pueda hablar sin miedo a que haya micrófonos" o directamente me responden con otra pregunta: "¿te estás refiriendo a que tenemos que encriptar los mails?". En muchos de los casos, la forma "natural" de abordar la Seguridad de la Información es pensando en amenazas que no queremos que ocurran, o directamente en controles que deberíamos aplicar.

Sin embargo, el primer paso debería ser abstraerse de las posibles amenazas y concentrarse en la relación que existe entre el negocio de la organización y su información. Un **activo de información** es, justamente, algo que surge de esa relación. Aquí se presenta un listado de los distintos tipos de activos que deben considerarse:

- **Información:** en cualquier medio, como bases de datos y archivos con datos, contratos y acuerdos, documentación impresa o en línea, información de investigación, manuales y material de entrenamiento, procedimientos, pistas de Auditoría.
- **Software:** de aplicación, de base, herramientas y utilitarios de desarrollo.
- **Activos Físicos:** equipos de computación, equipos de comunicaciones, medios de almacenamiento, centros de cableados.
- **Servicios:** de computación y comunicaciones, de soporte (electricidad, aire acondicionado, iluminación, calefacción).
- **Procesos:** pueden incluir a las actividades críticas del negocio, procesos estratégicos, o de soporte.
- **Personas:** junto con su experiencia, conocimiento, capacidades y competencias.

- **Activos Intangibles:** pueden incluir la reputación e imagen de la organización, o el valor (para los accionistas o el mercado) de su marca.

La información debe cuidarse a lo largo de su paso por los más variados medios: en el mainframe donde está almacenada, en el cable cuando es transmitida a la impresora, en la hoja impresa de la bandeja, en la propia mente de quien la leyó, y en el cesto de basura donde esa hoja fue descartada. Pero el listado de activos no se agota en los relacionados *sólo* con la información, sino también con el propio negocio de la organización, como es el caso de los activos intangibles o los procesos del negocio. Por ejemplo, la función principal de un Plan de Contingencias es asegurar la continuidad de los procesos del negocio, frente a una serie de amenazas disruptivas.

Las buenas prácticas definen algunos atributos importantes de los activos para establecer **prioridades** a la hora de protegerlos. Los tres atributos más destacados son:

- **Dueño:** es el responsable por el activo y las decisiones relacionadas con éste. No debe entenderse con el sentido de quien ejerce derechos de propiedad sobre el activo, ya que esto lo hace la propia organización (o los accionistas, socios, etc). Por ejemplo, es normal considerar al Gerente de Marketing como "dueño" de la base de clientes, pero esto no significa que pueda venderla a terceros (de hecho, sería causal de despido).
- **Custodio:** es el responsable de implementar la protección delegada por el dueño. Comúnmente, es una tarea que se delega a áreas de tecnología o de seguridad.
- **Clasificación:** es el grado de importancia definido por el dueño en función a diversos criterios, por ejemplo, qué tan confidencial, íntegra o disponible debe permanecer la información.

A partir de estos conceptos se escinden las decisiones sobre *por qué* proteger los activos de *cómo* hacerlo. El dueño define el por qué, ya que conoce claramente cuál es la información importante para el negocio. El cómo queda a criterio del custodio, quien entiende mejor qué tecnología, o procesos administrativos dan mejores resultados.

Esta separación de responsabilidades produce una **negociación** entre dueños y custodios que mejora la relación costo-beneficio de la protección de los activos. El dueño, muchas veces el propio generador y/o usuario, pretende que el activo sea protegido por todos los medios disponibles. Nadie conoce mejor que el dueño la real importancia de la información para el negocio. Por su parte, el custodio va a cuidar la carga operativa y el presupuesto asignado. Aquí se da un verdadero control por oposición de intereses, ya que el dueño va a exigir los controles adecuados para proteger "sus" activos, y el custodio, por su parte, que el dueño sea realista a la hora de definir prioridades. Una típica frase del custodio al dueño bien puede ser: "No vale que todos tus activos sean altamente críticos". Por ejemplo, ocurrió durante una consultoría que el dueño de una base de datos sostenía que la disponibilidad era un atributo crítico del activo, pero el custodio, al escucharlo, le contestó: "Eso no

es así, el mes pasado se cayó la base de datos durante tres días y ustedes ni se habían enterado, ¡fui yo quien se los comunicó!"

2.6 Clasificación de la Información

La clasificación de la información es una actividad muy importante porque no toda la información tiene el mismo valor, ni está expuesta a las mismas amenazas, ni merece el mismo grado de protección.

La clasificación de los activos permite una mejor focalización de los controles en aquellas áreas que más los requieren. Estos activos son clasificados de acuerdo con su **valor** para la organización, directamente proporcional al impacto frente a una pérdida de confidencialidad, disponibilidad o integridad de la información relacionada. Clasificarlos puede ser tan sencillo como definir si la información es "confidencial", "de uso interno", "sensible", o "de acceso público". Lo difícil es mantener un inventario unificado y consistente en *toda* la organización, y con procedimientos para que *todo* el personal entienda los cuidados que se deben adoptar. Es decir, la gestión del inventario, y su posterior clasificación, etiquetado y manipulación.

Tradicionalmente, la clasificación se asociaba a los ambientes militares, donde les preocupaba la confidencialidad de la información que podía afectar gravemente la seguridad nacional. Lo usual es asignar una **etiqueta** (label) a cada activo con un nivel de clasificación (por ejemplo, "top secret", "secret", "sensitive", "unclassified"), y un **nivel de acceso** (clearance) a cada persona que deba acceder a la información, con la misma escala de las etiquetas. Esta visión de la clasificación ha sido superada con el tiempo, al tener las nuevas tecnologías de comunicaciones y redes cada vez más ingerencia en las fuerzas armadas. Hoy en día en los propios ambientes militares se consideran también requisitos de clasificación basados en la integridad y la disponibilidad[15].

Para ambientes no militares (comerciales, de gobierno u otras organizaciones), lo usual es asignar **etiquetas** a los activos (por ejemplo, "confidencial", "de uso interno", "sensible", "pública") y establecer **procedimientos** para que todo el personal entienda los distintos cuidados que debe adoptar de acuerdo con la clasificación. Es tan importante el procedimiento de clasificación de todos los activos críticos, como así también la toma de conciencia y entrenamiento para saber qué hacer (y sobre todo, qué *no hacer*) con la información clasificada.

[15] Como bien me lo hizo notar un militar durante una conferencia que estaba dando en el capítulo local de AFCEA *(Armed Forces Communications and Electronics Association)*.

3 Gestión de Riesgos

Los controles de seguridad (y más específicamente, la tecnología asociada) son el aspecto históricamente más visible de la Seguridad de la Información. Por ejemplo, la norma ISO/IEC 27002 (ex ISO/IEC 17799) es una guía de implementación de 133 controles de seguridad, agrupados en 39 objetivos de control pretendidos. El origen de esta norma fue la BS 7799 (del *British Standards Institution*) que recopilaba todas las buenas prácticas existentes en Reino Unido en lo referido a Seguridad de la Información. Estas normas también contenían lineamientos muy generales sobre el análisis y valoración de los riesgos como fuente para seleccionar las medidas a aplicar. Al principio, la interpretación de la industria de la seguridad era que se contaba con una serie de medidas que se habían descubierto eficaces para *controlar* la mayoría de las amenazas conocidas. Con el tiempo, y luego de varios proyectos fallidos de implementación de los controles de la norma ISO 17799, se comprendió la necesidad de determinar los pasos o requisitos previos para implementar estas técnicas de control de una manera **eficaz** (sabiendo *dónde* aplicarlas), **eficiente** (sabiendo *con qué intensidad* aplicarlas) y **continua** (asegurando su mantenimiento y *mejora* con el paso del tiempo). Dichos requisitos, que se recopilaron primero en la parte 2 de la BS 7799 (o BS 7799-2) y posteriormente en la norma ISO/IEC 27001, incluyen la gestión de riesgos, la gestión documental, la responsabilidad de la Dirección, las métricas de seguridad y la mejora continua.

La Gestión de Riesgos (o *Risk Management)* introduce el concepto de que nada es 100% seguro en materia de Seguridad de la Información -valga la redundancia. Se manejan conceptos como **probabilidad de ocurrencia** e **impacto**: no se sabe a ciencia cierta cuándo puede ocurrir un incidente, ni cuáles pueden ser sus consecuencias**.** Lo que sí sabemos es que existe un nivel de riesgos de seguridad relacionado con las condiciones particulares que rodean las actividades de la organización. Las buenas prácticas normalmente utilizan definiciones muy similares a las siguientes:

- **Gestión de Riesgos:** actividades coordinadas para dirigir y controlar una organización respecto de los riesgos de su negocio.
- **Amenaza *(threat)*:** un hecho potencial, que de ocurrir se traduce en un incidente que puede resultar en daño para la información o el negocio de la organización (normalmente, un factor externo).
- **Vulnerabilidad:** una debilidad en un activo, grupo de activos o controles de seguridad que lo protegen, que puede ser aprovechada por una amenaza para concretarse (normalmente, un factor interno).
- **Riesgo *(risk)*:** la combinación de la probabilidad de ocurrencia y el impacto o consecuencia de que una amenaza se concrete (normalmente, que se conjuguen el factor externo con el interno).
- **Control o Contramedida:** una técnica para manejar el riesgo, reduciendo la probabilidad de ocurrencia o el impacto de una amenaza.
- **Riesgo Residual:** el riesgo remanente luego de aplicar un control.

En la figura 3.1 se presenta un esquema (similar al de la figura 2.1) con la relación entre algunos de los conceptos. Por lo general, las **amenazas** están asociadas a un factor externo (o agente de amenaza) que aprovecha una vulnerabilidad inherente a los activos, controles o información que se está protegiendo. Conviene expresar a las amenazas en el tiempo **presente del modo subjuntivo**, para resaltar que se trata de un hecho que puede ocurrir con determinada probabilidad. Por ejemplo: "que la información *sea alterada* por el ingreso de un virus informático en el sistema". De la misma forma, conviene expresar las **vulnerabilidades** en el tiempo **presente** o **pasado del modo indicativo**. Por ejemplo: “No *se instaló* un sistema antivirus”. Normalmente las vulnerabilidades se asocian a una falla en los controles, pero también pueden deberse a una característica intrínseca del activo. Por ejemplo: “El sistema *abarca* una gran variedad de tecnologías, dificultando la detección y tratamiento de *bugs* en las aplicaciones”, o también “Por requerimientos regulatorios la información *debe* almacenarse en papel, por lo que puede ser afectada por agua, fuego o humedad”.

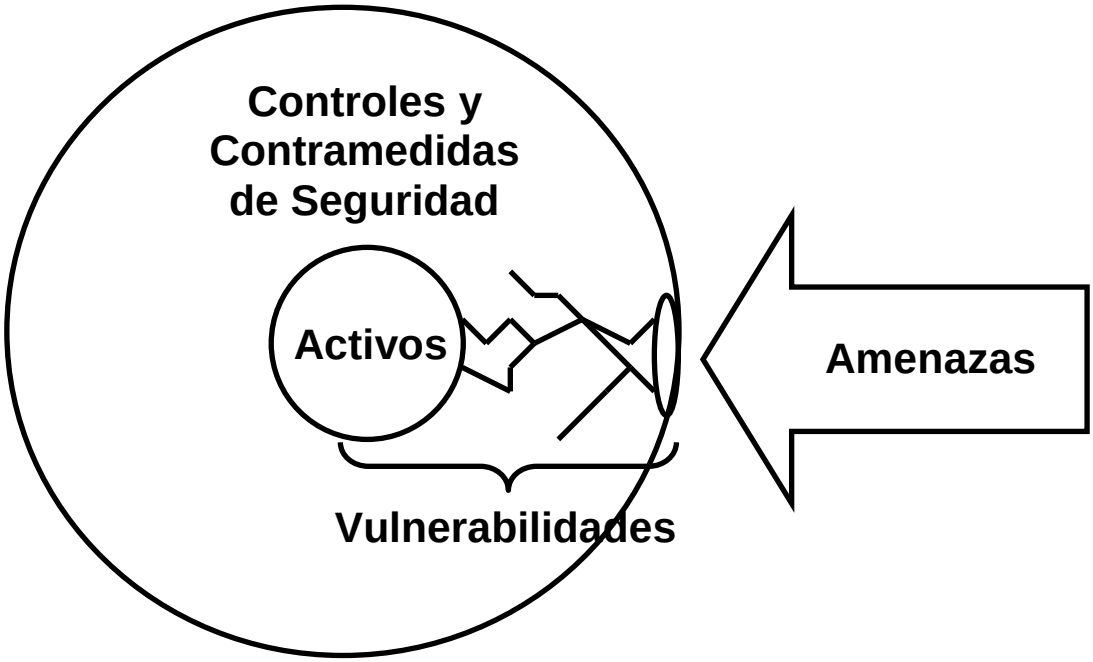

Figura 3.1

La gestión de riesgos es una de las principales actividades de **planificación** en la gestión de la Seguridad de la Información. Reconocemos de manera explícita que nuestro esfuerzo de protección de la información depende de factores en general ajenos a nosotros (amenazas), factores internos (nuestras vulnerabilidades), y que nuestra respuesta puede reducir (pero no eliminar) los riesgos asociados.

El proceso de Gestión de Riesgos normalmente incluye 3 etapas que trataremos en las secciones que siguen:

- **Análisis de Riesgos** (*Risk Analysis*)

- **Valoración de Riesgos** (*Risk Evaluation*)
- **Tratamiento de Riesgos** (*Risk Treatment*)

En todo momento, debe tenerse en cuenta que si bien la gestión de riesgos involucra a especialistas en la materia, es un proceso que requiere de la participación activa de **todas las áreas de la organización**, ya que en *última instancia*, son éstas quienes poseen el conocimiento sobre el negocio, y sobre las amenazas y vulnerabilidades que lo aquejan. Que las áreas sean quienes están más relacionadas con el negocio y por lo tanto conozcan mejor que nadie las amenazas, *no implica* que la gestión de riesgos deba quedar librada a su decisión solamente. Todo lo contrario, volviendo sobre la negociación entre dueños y custodios, debe existir una **tercera parte** que guíe este proceso (normalmente los analistas, administradores de seguridad o, por qué no, consultores).

Por último, la **Alta Dirección** debe apoyar la gestión de riesgos, permitiendo a las áreas invertir recursos y tiempo en las actividades requeridas, y aceptando formalmente los riesgos residuales.

3.1 Análisis de Riesgos

El Análisis de Riesgos es el uso sistemático de la información para identificar fuentes de riesgo y calcular sus **valores** en función a la probabilidad de ocurrencia y el impacto.

El factor de impacto del riesgo se basa en la **tasación** o **valoración** que tiene el **activo** para la organización, ya que identifica el grado de daño y las consecuencias producidas cuando una amenaza se concreta. A mayor valoración del activo, mayor el impacto, y viceversa.

El factor de probabilidad del riesgo (o de que una amenaza se concrete) se basa en la **tasa de ocurrencia** de los **incidentes** relacionados con la amenaza. Normalmente, para la concreción se dan dos condiciones: existe algún factor externo (también llamado agente de amenaza) que aprovecha un factor interno (relacionado con alguna vulnerabilidad en el activo o los controles). La probabilidad de ocurrencia de la amenaza depende entonces de la probabilidad de la aparición del factor externo, junto con la probabilidad de que ese factor externo aproveche alguna vulnerabilidad.

El proceso de Análisis de Riesgos normalmente incluye:

- Identificación de **activos** de la organización.
- **Tasación** o **valorización** de los activos.
- Identificación de **controles** ya implementados.
- Identificación de las **amenazas** y su **probabilidad de ocurrencia**.
- Identificación de las **vulnerabilidades** y probabilidad de ser aprovechadas por las amenazas (**nivel de vulnerabilidad**).
- Estimación del **impacto** de las amenazas sobre los activos.

- Estimación de la **magnitud del riesgo** en función de las probabilidades de ocurrencia e impactos calculados.

Las formas posibles para combinar la probabilidad de ocurrencia con el impacto son muchas, pero siempre con la premisa de que el nivel de riesgo calculado debe aumentar si cualquiera de esos dos factores de contribución aumenta. Existen dos enfoques generales en el Análisis de Riesgos: el **cuantitativo** y el **cualitativo**.

3.2 Análisis de Riesgos Cuantitativo

En el análisis de riesgos cuantitativo, se utiliza **información estadística** para calcular al riesgo como un valor promedio, o valor esperado[16]. En general se trata de un **valor monetario** que expresa cuánto dinero, *en promedio*, podemos esperar perder a lo largo de un período determinado. La matemática detrás del análisis cuantitativo puede ser tan sofisticada como queramos, pero en algunas situaciones puede simplificarse bastante. Por ejemplo, cuando la amenaza considerada ocurre con una frecuencia conocida, y cada vez que ocurre el impacto monetario es el mismo (y conocido), se utiliza, por un lado, la **tasa de ocurrencia anual** (**ARO** por *annualized rate of occurrence*) de la amenaza para estimar la probabilidad de ocurrencia; y por el otro, el valor monetario de la pérdida para estimar el impacto (**esperanza de pérdida única**, o **SLE** por *Single Loss Expectancy*). El riesgo se expresa directamente como la multiplicación de ambos factores, obteniéndose el costo anual esperado causado por esa amenaza (**esperanza de pérdida anualizada**, o **ALE** por *annualized loss expectancy*). Consideremos un ejemplo de análisis cuantitativo:

1. El *activo* que protegemos son los datos de la tarjeta de los clientes de la organización.
2. La *amenaza* que estamos considerando es la divulgación por robo de la *laptop* de un consultor que almacenaba una parte de dicha información[17].
3. El *valor* del activo lo estimamos en unos $400.000.
4. El porcentaje de registros generalmente contenidos en un *laptop* es de un 25% (esto se llama **factor de exposición**, o **EF** por *exposure factor*)
5. El *impacto* de la amenaza se calcula multiplicando el valor del activo por el factor de exposición:
   SLE = EF x Valor del Activo = $100.000 (perdemos el 25% de un activo valuado en $400.000).
6. La *probabilidad de ocurrencia* se estima con datos estadísticos:

[16] Según la norma BS 25999-1:2006: "El riesgo es generalmente cuantificado como un efecto promedio, sumando el efecto combinado de cada posible consecuencia, pesada de acuerdo con la probabilidad asociada de cada consecuencia, para obtener un 'valor esperado'". Eso no es ni más ni menos que la esperanza matemática o media de la distribución de probabilidad de las pérdidas ocasionadas por una amenaza (en general expresadas en términos monetarios).

[17] Muchos se preguntarán en qué circunstancia puede ser razonable que un consultor almacene en su *laptop* la información de tarjetas de créditos de los clientes. Yo me pregunto lo mismo, pero lamentablemente, es un ejemplo que he tomado de las noticias de las publicaciones especializadas en seguridad. Ocurre muy a menudo.

ARO = 0,25 (según la estadística de la industria, o propia de la organización, se roba una *laptop* cada cuatro años)[18].

7. El *riesgo* calculado (expresado monetariamente) es:
   ALE = ARO x SLE = $25.000 (en promedio, es lo que esperamos perder en un año por el robo de *laptops* a consultores).

Como veremos en la etapa de Valoración de Riesgos, expresar los riesgos de manera monetaria tiene la ventaja de que podemos comparar ese valor con el **costo de las contramedidas** que lo mitigan. Hasta podemos calcular un retorno de inversión de la seguridad. Sin embargo, el enfoque cuantitativo tiene varios puntos flacos. Para empezar, el cálculo anterior sólo tiene sentido en amenazas con estadísticas conocidas (aparición de virus, *worms*, desastres naturales, riesgo comercial, etc.). Existen algunos tipos de incidentes que sencillamente a las organizaciones no les gusta reconocer (fraude interno, divulgación de información de clientes) a menos que sea absolutamente imprescindible. Otros tipos de incidente no ocurren lo suficientemente seguido como para estimar la probabilidad en forma confiable, sobre todo aquellos incidentes de baja probabilidad de ocurrencia, pero alto impacto[19].

Por otro lado, está el problema de la estimación del impacto en términos económicos. En el ejemplo dijimos que lo estimábamos en $400.000, pero no cuál era la interpretación de esa cifra. ¿Se trata de la suma de todos los límites de crédito de los clientes? ¿Se trata del impacto financiero sobre la organización en indemnizaciones? ¿Se trata de la variación del valor de la acción de la organización en la bolsa cuando el público se entera del incidente? El típico error cuando usamos un enfoque cuantitativo es utilizar un modelo incompleto que no incorpore todas las variables que debería, y que en consecuencia estiman un impacto menor al real. A veces, directamente, no se puede calcular en términos monetarios, porque el modelo que usamos es incompleto, o inaplicable. Muchos autores sostienen que el método ALE es solamente una forma elegante de acomodar los números para que digan lo que queremos que digan[20].

3.3 Análisis de Riesgos Cualitativo

En el análisis de riesgos cualitativo cambia la forma de estimar las componentes, utilizándose el **juicio**, **experiencia** e **intuición** de expertos y personas involucradas en los procesos del negocio. Se utilizan técnicas como Delphi, *brainstorming*, *focus groups*, cuestionarios, *checklists* y entrevistas para obtener los resultados, y los valores se expresan como números enteros (escalas de 1 al 5, como promedios de tales valores, con las palabras “Alto, Medio, Bajo”, etc.). Existen muchas maneras de combinar la probabilidad de ocurrencia y el impacto para calcular el riesgo en un análisis cualitativo,

[18] Aclaro, por si hace falta, que este dato es absolutamente inventado para el ejemplo.
[19] Para una muy buena explicación de por qué ALE “sencillamente no es bueno”, ver Jaquith, Andrew: *Security Metrics: Replacing fear, uncertainty, and doubt*, Upper Saddle River (NJ), Addison-Wesley, 2007, págs. 31 a 36.
[20] Op. cit.

probablemente tantas como organizaciones haya. Una de ellas es usando **matrices predefinidas** con entradas para el nivel de amenaza (factor externo), el nivel de vulnerabilidad (factor interno) y valor del activo, y como salida, el valor estimado de riesgo. En la tabla 3.1 se muestra un ejemplo[21]. En ese contexto, una amenaza que tenga una probabilidad media de ocurrir (nivel de amenaza, por ejemplo, un virus informático), y que aproveche una vulnerabilidad para la que la organización no está bien preparada (nivel de vulnerabilidad, por ejemplo, un equipo conectado en forma directa a internet y que carece de protecciones antivirus) va a resultar en un valor de riesgo de 3, 4 o 5 (en una escala del 1 al 7) dependiendo del valor del activo considerado (mientras mayor sea el valor, mayor el valor del riesgo).

Otra forma es calculando el riesgo como una multiplicación de dos factores, utilizando una escala numérica. En la figura 3.2 se muestra un ejemplo, donde la probabilidad de ocurrencia y el impacto de una amenaza adoptan valores entre 1 y 10, y el riesgo asociado lo hace entre 1 y 100. En este caso, la interpretación del riesgo es un área rectangular en un gráfico de dos dimensiones.

Valor del Activo	Nivel de Amenaza (factor externo)								
	Bajo			Medio			Alto		
	Nivel de Vulnerabilidad (factor interno)								
	Bajo	Medio	Alto	Bajo	Medio	Alto	Bajo	Medio	Alto
Bajo	1	2	3	2	3	4	3	4	5
Medio	2	3	3	3	4	5	4	5	6
Alto	3	4	5	4	5	6	5	6	7

Tabla 3.1

Un punto importante a tener en cuenta es que, ya sea que se use una matriz como la de la tabla 3.1 o se represente al riesgo como un área como en la figura 3.2, los valores numéricos empleados **no tienen un significado** en sí mismos, como en el caso del análisis cuantitativo. El valor calculado del riesgo sólo tiene sentido en la medida en que se lo compare contra otros riesgos, o contra una escala preestablecida.

El análisis cualitativo de la figura 3.2 puede parecer sencillo a simple vista. El desafío viene con la **cantidad** de activos y amenazas que deben manejarse, y por el hecho de que los riesgos son estimados por diferentes personas en la organización. El proceso requiere de mucha **coordinación** por parte de un especialista en riesgos que reúna toda la información producida por las partes, logre una **visión consensuada** entre los distintos dueños y custodios, y presente un análisis integral para que la Alta Dirección entienda el significado y pueda tomar las acciones adecuadas.

[21] La tabla está adaptada de *BS 7799-3:2006 – Information security management systems – Part 3: guidelines for information security risk management*, Londres, BSI, 2006, pág. 45.

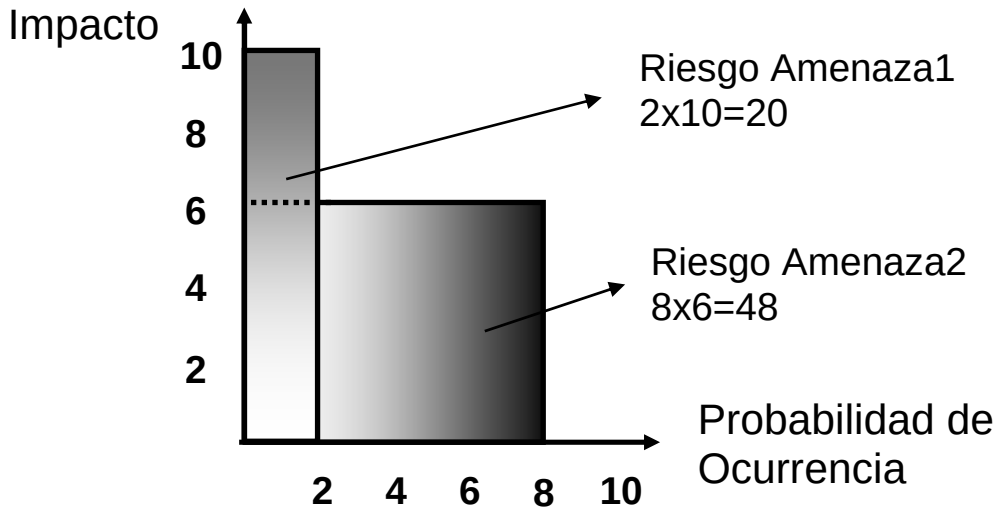

Figura 3.2

Considérense los resultados de un ejercicio real de Gestión de Riesgos[22]. Los resultados se presentan con la forma de un gráfico de burbujas en la figura 3.3. Las escalas numéricas utilizadas son iguales que las de la figura 3.2. El tamaño de cada burbuja es proporcional a la cantidad de amenazas con los mismos niveles de riesgo. Para entender el esfuerzo que le requirió a la organización, pensemos que el proceso involucró el trabajo de 8 áreas funcionales y duró alrededor de 3 meses, incluyendo, además del Análisis de Riesgos, la valoración y el Tratamiento. Las áreas tuvieron que identificar (y describir) 69 activos, 101 amenazas, y otras tantas vulnerabilidades. Además, se pidió que para cada activo se identificaran (y se evaluaran la eficacia de) los controles ya implementados. Los valores de Impacto y Probabilidad de Ocurrencia se calcularon estimando los niveles de 5 variables para cada amenaza (la probabilidad de aparición de las amenazas, el nivel de vulnerabilidad, y los impactos sobre confidencialidad, integridad y disponibilidad). Para las 5 variables solamente se pidió que se identificaran tres niveles: “alto”, “medio”, o “bajo”[23]. Aún así, la cantidad de variables que debieron consensuarse entre dueños, custodios y administradores de seguridad fue de 505, solamente para el Análisis de Riesgos.

[22] En una empresa mediana de servicios del rubro bancario en la que participé como consultor.

[23] Creo que no puedo remarcar con el suficiente énfasis que estamos hablando de un *ejemplo* tomado de la vida real, pero que cada organización puede seleccionar otras escalas, otras variables, e incluso, otra manera de combinarlas.

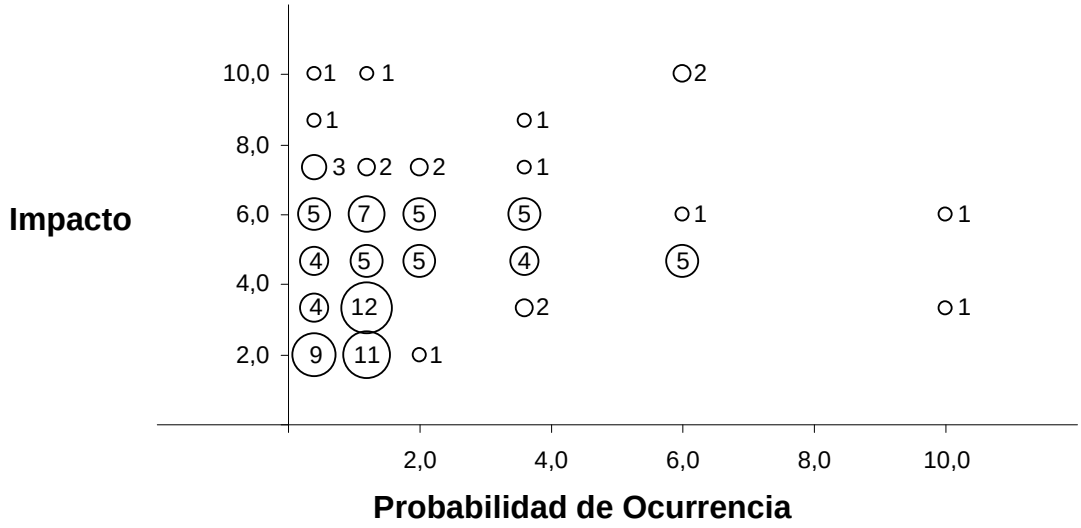

Figura 3.3

3.4 Valoración de Riesgos

El propósito de la valoración de riesgos es identificar el **significado** que los riesgos calculados tienen para la organización y jerarquizarlos por importancia. El grupo que realiza la valoración debe ser multidisciplinario, con participantes de distintas áreas de la organización. Ésta debe cerciorarse de que los propietarios de los activos involucrados estén presentes en el proceso. Se deben comparar los niveles calculados de riesgo con una escala de riesgo establecida especialmente para dicho efecto, con la finalidad de que la **Alta Dirección decida** qué medidas se van a implementar en la etapa de tratamiento de riesgo. Los criterios que usualmente se utilizan para efectuar la valoración son:

- **Impacto económico** del riesgo.
- **Tiempo de recuperación** de la empresa.
- **Probabilidad de ocurrencia** del riesgo.
- **Probabilidad de interrumpir las actividades** de la empresa.

En el caso de análisis de riesgos *cuantitativo*, la valoración es más sencilla, en principio, porque el significado de los niveles de riesgo ya tienen una interpretación: se trata del dinero que la organización espera perder a causa de una amenaza determinada. El criterio consiste simplemente en comparar el **costo** de implementación de las posibles contramedidas, y el **ahorro** monetario producido. Para ilustrar estos conceptos, consideremos el ejemplo de análisis cuantitativo ya utilizado:

1. Como ya se estableció, el *riesgo sin contramedidas* es:
   ALE_0 = $25.000
2. Se considera una *contramedida* que involucre la encripción de la información, que consigue disminuir el riesgo a un valor inferior:

ALE_1 = $5.000

3. El *costo de la contramedida*, en la forma de licencias de *software*, se puede expresar anualmente como:
   Costo1 = $10.000
4. Con estos datos, se puede calcular el *ahorro* que produce la aplicación de la contramedida (la instalación de la herramienta de encripción):
   $Ahorro_1 = ALE_0 – ALE_1 – Costo_1$ = $10.000
5. El **retorno de inversión en seguridad** (o **ROSI**, por *return on security investment*) se calcula de la misma manera que se calcula un ROI:
   ROSI = Ahorro / Costo = $10.000 / $10.000 = 1
   Lo que significa que por cada peso invertido, se obtiene otro peso como ahorro.
6. El **criterio de valoración** consiste en elegir aquella contramedida (¡puede haber más de una opción!) que tenga un mejor ROSI
7. Si el ROSI < 0 entonces se *acepta el riesgo*, porque la contramedida es más cara que el ahorro

Nuevamente, debemos destacar que el análisis cuantitativo sólo tiene sentido para amenazas bien estudiadas, con abundante estadística, y cuando las consecuencias de la concreción de la amenaza son realmente conocidas[24].

En el caso del análisis *cualitativo*, la organización debe empezar por definir cuál es el **significado** de los distintos niveles que el riesgo puede adoptar en términos que tengan **sentido para el negocio**. Por ejemplo, en el gráfico de la figura 3.3, ¿qué significado tiene la burbuja que se ubica en las coordenadas (6,6), con un riesgo calculado de 36 sobre 100? ¿Y la burbuja en (10,6)? ¿Es equivalente ese nivel de riesgo de 60 con el de la burbuja en (6,10)? ¿Requieren del mismo tipo de tratamiento, ya que cuentan con el mismo nivel de riesgo?

La interpretación se hace en función de los valores asignados por las áreas a las 5 variables mencionadas en la sección anterior[25]. Son las propias áreas funcionales de la organización que identificaron dichos valores las que asignan un significado concreto a las coordenadas del riesgo. Por ejemplo, en el ejercicio bajo análisis, una amenaza cuya probabilidad de ocurrencia sea *media*, pero que la probabilidad de que se aproveche de las vulnerabilidades de la organización para su concreción sea *alta* da como resultado que la coordenada “probabilidad de ocurrencia” de la figura 3.3 adopte el valor 6. Para asignarle significado al impacto, se usan las otras tres variables: por ejemplo, una amenaza que si se concreta tiene un impacto *alto* en confidencialidad, *medio* en integridad, y *bajo* en disponibilidad, da como resultado que la coordenada “impacto” también adopte el valor 6.

[24] En todas las conferencias en las que expuse el tema de la valoración de riesgos, siempre surgió, palabras más, palabras menos, la siguiente pregunta en el auditorio: “¿qué pasa cuando el ahorro no justifica el control, pero en realidad un incidente de ese tipo está poniendo en riesgo la credibilidad de la organización frente a los clientes?”. Mi respuesta: “ah, pero entonces hicimos mal el análisis de riesgos en primer lugar, porque el impacto económico es evidentemente mayor al calculado.”

[25] Vale aquí la misma aclaración que en la sección anterior, se trata del ejemplo de una posible metodología entre varias que puede elegir una organización.

La interpretación del nivel de riesgos es importante para que la organización determine qué amenazas son aceptables, y cuáles no. Normalmente se lo hace fijando un **umbral de riesgo máximo tolerable**, por encima del cuál las amenazas deben recibir un tratamiento. Ese nivel particular de riesgo es el que más importa interpretar. Dicho umbral depende de **apetito de riesgo** de la organización. Existen negocios que deben aceptar un nivel general de riesgos mayor que otras. Por ejemplo, en términos generales, un sitio de Internet dedicado a las recetas de cocina probablemente acepte un umbral de riesgos aceptables mayor que un sitio que maneje información personal de los usuarios.

Consideremos el umbral de riesgos aceptables de la figura 3.4, que sigue en línea con lo mostrado en la figura 3.2 de la sección anterior. En ese caso, hemos considerado que un nivel de riesgos de 16 es aceptable, todas las amenazas cuyos niveles de riesgo calculados se encuentren dentro del área demarcada son aceptables para la organización.

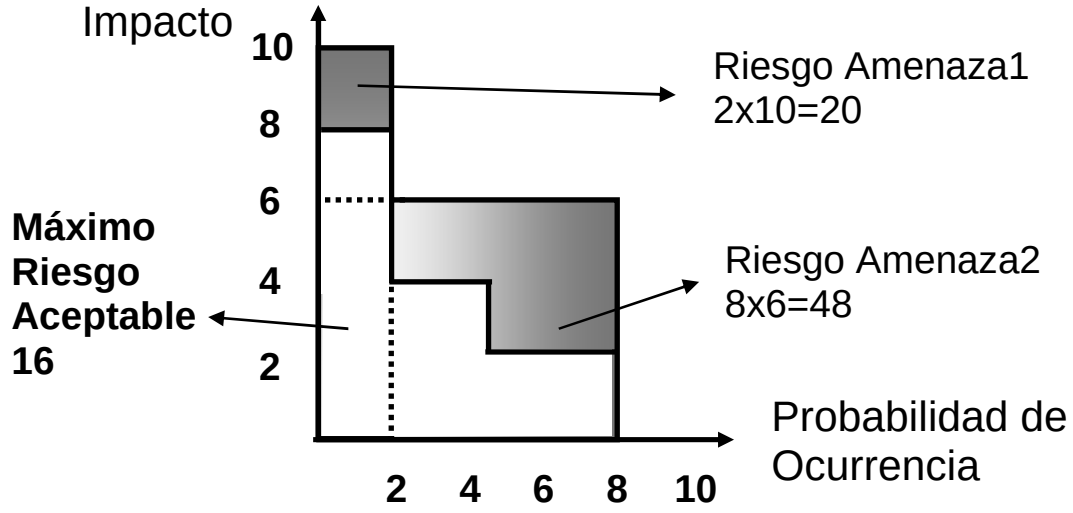

Figura 3.4

Tal vez un mejor método que el anterior para evaluar si el riesgo es aceptable o no, sea utilizar un **área de riesgo aceptable**, como se muestra en la figura 3.5. En este caso el máximo riesgo aceptable también es 16, pero se evalúan ambas componentes (probabilidad de ocurrencia e impacto) por separado y ninguna puede superar el valor de 4. Tratar a las componentes por separado a veces es preferible a simplemente tratar de disminuir los riesgos, porque pone de manifiesto qué aspecto de la amenaza conviene tratar. No es lo mismo reducir el impacto de una eventual amenaza, que su probabilidad de ocurrencia, como veremos en las secciones posteriores.

Siguiendo con el ejercicio real, la organización se decidió por un área de riesgo aceptable de 1,8 (sobre 10) para la probabilidad de ocurrencia, y 2,2 (sobre 10) para el impacto. El riesgo equivalente aceptable era de 3,96 (sobre 100). El significado de aceptar 1,8 para la componente de probabilidad de ocurrencia era que una amenaza podía tener una probabilidad *media* de aparición, siempre que la probabilidad de que encontrase una vulnerabilidad

fuese *baja*; o bien, que si la probabilidad de aparición era *baja*, entonces la probabilidad de aprovecharse de una vulnerabilidad podía ser *media*. Con respecto al componente del impacto de la amenaza, el valor aceptable por debajo de 2,2 implica que tanto en confidencialidad, integridad o disponibilidad el impacto es *bajo.* En el gráfico de la figura 3.3 se observa que de las 101 amenazas identificadas solamente 20 eran aceptables a priori.

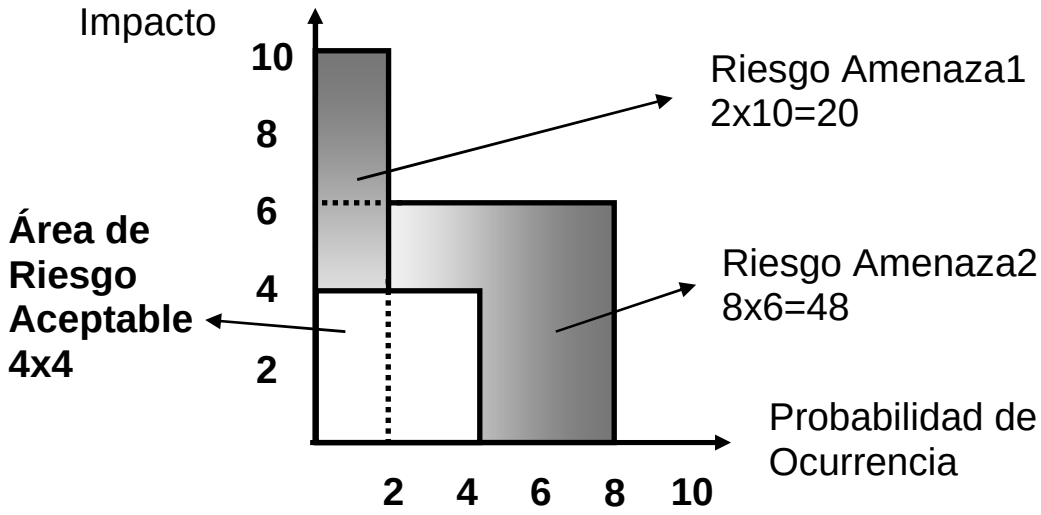

Figura 3.5

Existen algunas consideraciones importantes sobre la valoración de riesgos *cualitativa*. Por un lado, a diferencia del caso cuantitativo, es una actividad que se desarrolla **al mismo tiempo** que el análisis del riesgo. Por el otro, deben definirse **precisamente** los niveles de probabilidad e impacto. Esto es necesario para homogeneizar el resultado del análisis y valoración de los riesgos y disminuir la componente de juicio individual de los involucrados. Por ejemplo, puede entenderse que “impacto alto significa imposibilidad de brindar nuestro servicio”, “impacto medio significa que brindamos el servicio, pero no estamos en condiciones de facturarlo”, e “impacto bajo significa que no podemos adquirir nuevos clientes”; otra alternativa es definir conjuntos de sistemas o información de impacto Alto, Medio, Bajo *a priori*, en función a la “cercanía” con las actividades principales del negocio. Del mismo modo puede definirse “probabilidad alta significa que el evento ocurre sistemáticamente”, “probabilidad media significa que el evento no es sistemático, pero ha ocurrido en el último año más de una vez”, etc.

Por último, el resultado de valoración de riesgos debe recibir una **aprobación formal** por parte de la Alta Dirección, ya que es esta última la que define los niveles de riesgos aceptables para el negocio. Normalmente, si bien no es cierto en un sentido *operativo*, se acepta que es la Alta Dirección la encargada de “realizar” la valoración de los riesgos.

3.5 Tratamiento de Riesgos

Una vez que el riesgo ha sido valorado y la organización ha determinado cuáles son los activos de la información sujetos a riesgos, y cuál es su significado, la Alta Dirección debe elegir una **estrategia** para su tratamiento.

Al margen de considerar el impacto financiero del riesgo en la organización, ésta debe considerar el costo de actuar sobre alguna de las opciones del tratamiento del riesgo. La organización debe asegurarse de que existe un **buen balance** entre el costo de la protección y el valor de los activos protegidos, para no perjudicar la rentabilidad ni la competitividad de la empresa. Para el tratamiento del riesgo las buenas prácticas consideran cuatro estrategias genéricas:

- **Reducción del riesgo:** aplicación de **controles** sobre los activos que disminuyen el riesgo. La reducción del riesgo normalmente se elige cuando los controles a implantar para disminuir los riesgos a los niveles de aceptación previamente identificados por la empresa son económicamente factibles.
- **Aceptación del riesgo:** la Alta Dirección entiende el riesgo y explicita su aceptación en un **documento formal**. La aceptación del riesgo normalmente se elige cuando el diseño del control para mitigar el riesgo es más costoso que las consecuencias del riesgo. Sin embargo, debe resaltarse el hecho de que esta opción implica entender y aceptar las consecuencias de la concreción de una amenaza en forma objetiva y con conocimiento.
- **Transferencia del riesgo:** traslado del riesgo a **terceras partes**, por ejemplo, mediante una tercerización de los controles, o la contratación de un seguro. La transferencia del riesgo normalmente se elige cuando el diseño del control para mitigar el riesgo es costoso, pero las consecuencias del riesgo son devastadoras para la empresa y la transferencia del riesgo es económicamente viable.
- **Evasión del riesgo: cese de las actividades** que producen los riesgos. La evasión del riesgo normalmente se elige cuando el diseño del control para mitigar el riesgo es costoso, las consecuencias del riesgo son devastadoras para la empresa, pero la transferencia del riesgo no es económicamente viable.

Algunos autores aceptan una quinta “estrategia” que es la negación del riesgo (*denial*), pero es más bien una forma de describir lo que no debe hacerse (pero que algunas organizaciones hacen), la no-estrategia, o la estrategia de las “malas prácticas” [26].

El riesgo residual es el riesgo remanente luego de haber implementado las decisiones tomadas en el tratamiento del riesgo. La Alta Dirección debe asegurarse de que entiende estos riesgos residuales y de que el nivel de riesgos residuales se encuentra dentro de los **parámetros aceptables**.

[26] Ver por ejemplo, Harris, Shon: *CISSP Certification, All-In-One Exam Guide, Second Edition*, Emeriville, McGraw-Hill, 2003.

Volviendo al ejemplo de una gestión de riesgos real en una organización, en la figura 3.6 se muestra el gráfico de riesgos residuales *propuestos* a la Alta Dirección. Nótese que de las 101 amenazas identificadas, 19 han quedado por fuera del área de riesgo aceptable, y el gráfico es más parecido al de la figura 3.4 que al de la figura 3.5. Los valores de los riesgos han disminuido sensiblemente, pero en algunos casos, sencillamente era imposible disminuir los valores del impacto o de la probabilidad de ocurrencia, y la organización no tuvo más remedio que aceptarlos de manera consciente y objetiva.

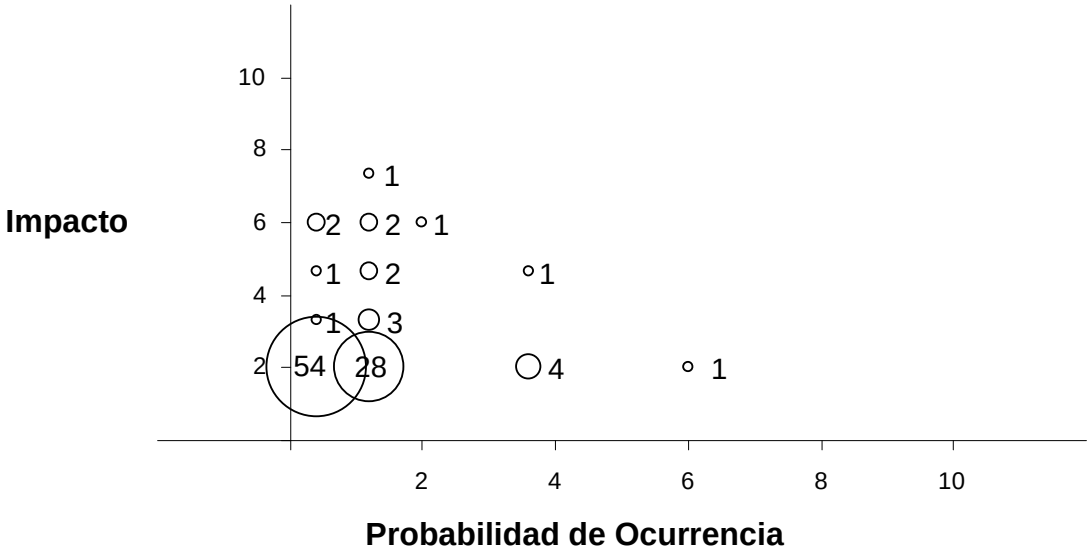

Figura 3.6

La etapa del tratamiento de riesgos es la más difícil de llevar a la práctica, porque es en la que debemos **"hacer cosas"**. En las dos etapas anteriores, relevábamos información, realizábamos una serie de reuniones de trabajo en grupo y llegábamos a conclusiones.

Como las condiciones en las que está inmersa la organización (y su negocio) no se mantienen estáticas en el tiempo, los riesgos se modifican constantemente, y también debe hacerlo su análisis, valoración y tratamiento. En consecuencia, el proceso de gestión de riesgos debe ser implementado **periódicamente**. En todo momento, los datos que utilizamos en los gráficos se están modificando, y la organización debe mantener la claridad con respecto a las sucesivas etapas de análisis, valoración e implementación de controles. Por ejemplo, en el caso de los controles que actúan sobre los riesgos, tenemos los controles implementados, los que queremos implementar, y los que se están implementando. De igual manera, tenemos los riesgos residuales **propuestos** (antes de que implementemos los controles) y los riesgos residuales **reales** (si es que podemos medirlos de manera independiente, una vez implementados los controles). Estos riesgos residuales reales, se convierten luego en los riesgos *"a secas"* en un posterior análisis de riesgos. Gestionar estas variables y su **evolución** a lo largo del tiempo constituye un desafío importante.

Deberíamos esperar que el gráfico *real* de los riesgos de la organización vaya evolucionando de la situación inicial de la figura 3.3 hacia la de la figura 3.6 (si todo sale de acuerdo a lo planeado). Sin embargo, es posible que cuando la organización comience nuevamente el ciclo de gestión de los riesgos, habrán aparecido nuevos activos que cuidar y nuevas amenazas, y tal vez la eficacia de algunos controles establecidos no habrán sido los que se esperaban, por lo que el riesgo analizado sigue estando en un valor por encima del umbral de aceptación.

4 Controles Administrativos

A partir de este momento utilizaremos en forma intercambiable las palabras *controles* y *contramedidas:* son las actividades, tecnología, técnicas y conocimiento que aplicamos para modificar los valores del riesgo con el objetivo de controlar las amenazas a los activos de información.

En términos generales, existen tres **tipos de controles**:

- **Controles físicos:** por ejemplo, una cerradura, un guardia de seguridad, un perro, iluminación, una cerca, etc.
- **Controles técnicos o lógicos:** relacionados con la tecnología y sistemas de la información, como por ejemplo, un *firewall*, IPS, el uso de encripción, etc.
- **Controles administrativos:** relacionados con las actividades y pautas cumplidas por las personas, como por ejemplo, un procedimiento de aprobación, una medida disciplinaria, una política de seguridad, un *checklist* de seguridad, etc.

Ningún control cae exclusivamente en una de las categorías, sino que normalmente tienen los tres aspectos en distintas proporciones. Por ejemplo, un guardia de seguridad que controla con un libro de entradas el ingreso o egreso de *notebooks* de un edificio es a la vez un control físico y administrativo. Un molinete con tarjeta de proximidad es a la vez un control físico y tecnico.

Los controles también se pueden clasificar de acuerdo con el **tipo de funcionalidad** (o tipo de protección) que proveen:

- **Controles preventivos:** detienen o evitan eventos no deseados.
- **Controles detectivos:** identifican eventos no deseados que han ocurrido.
- **Controles correctivos:** corrigen las causas y/o consecuencias de eventos no deseados.
- **Controles disuasivos:** desalientan violaciones de seguridad.
- **Controles de recupero:** recuperan recursos y capacidades de la organización luego de un incidente.
- **Controles compensatorios:** proveen alternativas a otros controles débiles o muy costosos para implementar.

La funcionalidad está muy relacionada con el tratamiento de los riesgos, ya que define qué aspectos del riesgo (probabilidad o impacto) se van a mitigar. Por ejemplo, para tratar el riesgo de una amenaza con baja probabilidad de ocurrencia, pero alto impacto, lo más conveniente será algún control correctivo o de recupero antes que uno preventivo, ya que antes de disminuir aún más la probabilidad de ocurrencia, sería mejor primero intentar prepararse para cuando ocurra el incidente. Debemos cuidarnos de mitigar los “aspectos equivocados” de una amenaza.

Por último, existen los **controles de acceso**, que son un tipo especial de control para gestionar y permitir el acceso a la información y a los activos relacionados. Por ejemplo, la tecnología de autenticación y autorización de usuarios, permisos sobre archivos, redes, y sistemas de información, etc. Históricamente, la disciplina de Seguridad de la Información comenzó con la necesidad de implementar los controles de acceso, y actualmente concentran buena parte de las actividades operativas de ese departamento en las organización (la gestión de usuarios y contraseñas, la asignación de permisos sobre archivos y aplicaciones, etc.).

4.1 Aspectos Organizacionales

Cualquier control técnico puede ser vulnerado sin una correcta gestión de los aspectos administrativos, relacionados con las personas y los procesos de una organización. Existe una serie de lineamientos organizacionales que complementan a los controles técnicos y son fundamentales para aumentar la probabilidad de éxito. Los más importantes son:

- **Seguridad por Capas:** la probabilidad de que una amenaza logre aprovechar una vulnerabilidad disminuye si debe atravesar más de un control en forma secuencial.
- **Concientización en Seguridad *(Security Awareness)*:** capacitación y entrenamiento en el uso correcto y protección de la información y los activos de la empresa. Tanto para usuarios, como custodios y dueños.
- **Separación de Tareas *(Separation of Duties)*:** división de las tareas críticas de la organización en sub-tareas asignadas a más de una persona, para que la concreción de determinadas amenazas (por ejemplo, fraude) requieran de la connivencia de varios actores.
- **Rotación de Funciones *(Job Rotation)*** y **Vacaciones Obligatorias *(Mandatory Vacations)*:** generan rotación de la gente que realiza determinadas funciones críticas con la finalidad de aumentar la probabilidad de que se descubran conductas inapropiadas.
- **Registro de Responsabilidad *(Accountability)*:** mantener un historial (protegido) de quién hizo qué cosa, con qué activos, y cuándo. El registro de responsabilidad puede usarse tanto como control disuasivo como detectivo.

Más específicamente para los **controles de acceso**, existen dos lineamientos organizacionales fundamentales para su correcta aplicación:

- **Necesidad de saber *(Need to know)*:** la información debe ser accedida por personas o entidades que tengan un motivo válido para hacerlo, en función de las clasificaciones y niveles de acceso.
- **Mínimo Privilegio *(Least Privilege)*:** el acceso o manipulación de la información debe darse en forma restrictiva, no como la norma, sino como una excepción. Por defecto, ninguna persona o entidad debe tener asignado más permisos que los estrictamente necesarios.

La problemática puntual relacionada con las personas será abordada con mayor detalle en el episodio 2.

4.2 Roles y Responsabilidades

Las buenas prácticas establecen una serie de roles y responsabilidades referentes a la gestión de la Seguridad de la Información. Los más importantes son:

- **Alta Dirección:** define directrices, establece responsabilidades y provee los recursos necesarios. Sobre la importancia del involucramiento y apoyo de la Alta Dirección ya se habló en la sección 2.4.
- **Dueño de la información:** responsable último y (generalmente) productor de la información o activos. El dueño debe tener adecuada autorización sobre sus activos (normalmente, cada Gerente de línea es el dueño de los activos de su sector en la organización).
- **Custodio:** responsable por la implementación correcta de los controles. Se trata de una función delegada por el dueño (normalmente, es el Gerente de Tecnología). Un dueño puede ser el propio custodio de determinada información.
- **Oficial de Seguridad:** quien gestiona los aspectos del día a día de la Seguridad (puede incluir más o menos capacidad operativa, según el caso)
- **Auditor:** quien evalúa en forma *independiente* la gestión de la seguridad y los controles implementados
- **Usuario:** quien accede a la información para realizar sus funciones dentro de la organización. Debe cumplir con las políticas y procedimientos establecidos. Algunas veces los usuarios son los propios dueños de la información.

La gobernabilidad del esfuerzo de seguridad depende en gran medida de que las partes logren una buena comunicación y comprensión mutua. La seguridad en una organización implica la necesidad de compatibilizar necesidades distintas (y a veces contrapuestas), y homogeneizar conocimiento distribuido. Se trata de una importante **negociación interna**, que además está inserta dentro del día a día operativo de cada una de las áreas. Quien realmente conoce el valor para el negocio que tiene la información en cuestión (el dueño), no necesariamente está capacitado para entender los costos o los detalles de la implementación de las medidas de seguridad (los custodios), o el conocimiento metodológico necesario para evaluar amenazas y vulnerabilidades (el oficial de seguridad). Por ejemplo, los dueños muchas veces caen en la tentación de asignar el máximo valor a todos los activos e información de los que son responsables, pero los custodios están más interesados en poder asignar de manera eficiente los recursos invertidos en la operación de las medidas de protección (básicamente ahorrar tiempo y dinero).

Por otro lado, quien tiene una **preparación metodológica** en seguridad (el oficial de seguridad) en general no puede conocer los procesos de negocio al nivel en que lo hace el dueño, ni entender la carga operativa total que tienen

que manejar los custodios. Su tarea debe limitarse a la facilitación del proceso de negociación interna, descubrimiento de situaciones que requieren atención y determinación de si se están cumpliendo o no los objetivos y pautas de seguridad.

Un caso particular representan los auditores (internos, externos, de sistemas, etc.). Muchas veces se confunde sus funciones con las de un oficial de seguridad, pero la función de la auditoría es asegurar una **mirada independiente** de la implementación de las técnicas y herramientas de seguridad, incluyendo los procesos de gestión. Las capacidades técnicas pueden (y muchas veces, deben) ser similares, pero para evitar conflictos de intereses, los auditores no deben estar involucrados en la implementación. Por ejemplo, la auditoría contable es un requisito legal anual para asegurar que el balance presentado a los accionistas y demás partes interesadas es preciso (la información es íntegra) y que sus decisiones están bien fundamentadas.

Por último, están las necesidades de los usuarios de la información. Ellos necesitan la información para (ni más ni menos) **desarrollar el negocio** de la organización. Por lo tanto, debe existir un proceso de toma de conciencia para que éstos entiendan por qué existen controles de seguridad sobre la información, y el **entrenamiento** suficiente para saber utilizarlos. Las medidas de seguridad no deben entorpecer las actividades operativas de los usuarios más allá de lo razonable (nuevamente, la toma de conciencia), o éstos terminarán por desactivarlas, ya sea de manera formal (justificando su caso ante la Alta Dirección), o informal (encontrando la manera de saltear los controles).

4.3 Documentación

Según la norma ISO 9000[27], la documentación en una organización permite la comunicación del **propósito** y la **coherencia** de la acción. Entre los aportes mencionados por dicho estándar sobresalen el de proveer la formación apropiada (a las personas); el de la repetibilidad y la trazabilidad; y el de proporcionar evidencia objetiva. Todas estas características, de una u otra forma, ya han sido mencionadas en la sección 4.1, especialmente en lo concerniente a los aspectos relacionados con las personas (que requieren entrenamiento y toma de conciencia) y los controles administrativos (que requieren repetibilidad y trazabilidad, o registro de responsabilidad).

Respecto de la comunicación de propósito, la principal forma es a través del establecimiento de la **Política Corporativa de Seguridad**. No debería extrañarnos, entonces, que uno de los pilares de las normas ISO sea el establecimiento de una *política* (de *Calidad* si se trata de ISO 9001, de *Seguridad de la Información*, si se trata de ISO/IEC 27001, o *Ambiental*, si se trata de ISO 14001).

[27] *ISO 9000:2005 - Sistemas de Gestión de la Calidad - Fundamentos y Vocabulario*, Ginebra, ISO, 2005 (traducción certificada), sección 2.7.1.

Los tipos de documentación utilizados para la gestión de la Seguridad de la Información pueden ser de lo más variados. En general, la clasificación de la documentación de acuerdo con el tipo de documento se muestra gráficamente en una **pirámide documental** como la de la figura 4.1. El nombre, funcionalidad y contenido de los escalones de la pirámide puede variar de organización en organización, y la que se muestra en la figura es solamente un ejemplo tomado de un caso real. Un esquema documental debería identificar qué documentos son más o menos específicos en cuanto a lo operativo, cuáles contienen el **"qué"** se quiere o se debe (o se va a) hacer en la organización, y cuáles contienen el **"cómo"** se va a conseguir lo anterior. A medida que se escala cada nivel de la pirámide debería requerirse un nivel creciente de **aprobación** dentro de la organización (por ejemplo, una Política debería ser aprobada por la Alta Dirección, mientras que un Instructivo de Trabajo podría ser aprobado por quien va a llevar a cabo la función, o su supervisor). El nivel en la pirámide también da una idea de la frecuencia con la que se realizarán modificaciones al documento.

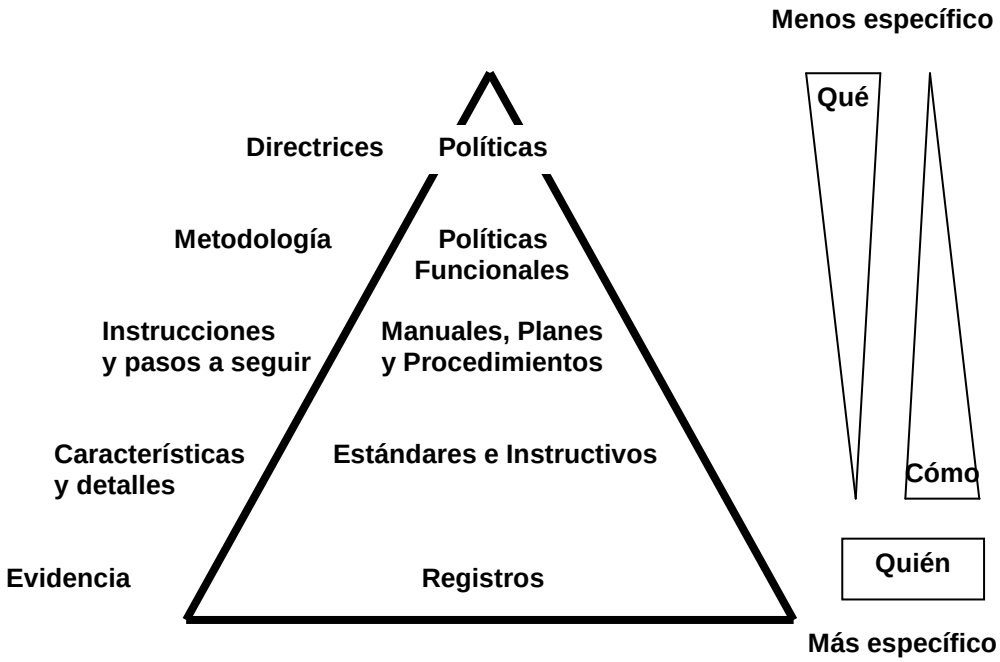

Figura 4.1. Un ejemplo de pirámide documental

Existe una serie de documentos o tipos de documentos que las buenas prácticas recomiendan considerar para gestionar la Seguridad de la Información en la organización[28]:

- **Política Corporativa:** es un documento firmado por la **Alta Dirección**, sin demasiadas precisiones operativas y en el que debe quedar en claro una

[28] Los nombres de la lista son ligeramente distintos a los de la figura 2.10, para acentuar el hecho de que son meros ejemplos y que las organizaciones deben definir su documentación según sus necesidades. En particular, la terminología utilizada aquí es bastante compatible con las normas ISO.

intención o **dirección** de hacia dónde quiere ir la organización en materia de seguridad. Debería revisarse con una periodicidad cercana a la anual, pero puede modificarse con una periodicidad menor. Además de una Política Corporativa de Seguridad de la Información, pueden existir políticas de Continuidad del Negocio, de Privacidad, de Seguridad Personal, entre otras, de acuerdo con la industria en la que se desenvuelve la organización.

- **Políticas Funcionales:** son políticas de "menor nivel" que una política corporativa. Tal vez atadas a un **proceso** o una **tecnología** particulares. Por ejemplo, una Política de Control de Accesos, Política de Uso de Internet, etc. Su alcance es más acotado, y si bien hay un listado de "qué" debemos o no debemos hacer, existe un "cómo" implícito en dicho alcance (por ejemplo, una Política de Uso de Internet claramente se refiere a cómo usamos la computadora de la organización).
- **Procedimientos Documentados:** un procedimiento es "la forma especificada para llevar a cabo una actividad o un proceso"[29]. En general se descompone en una serie de **pasos**, a cada uno de los cuales se les asigna un **responsable**, las tareas que debe realizar, y (de ser necesario) dónde queda un rastro o **evidencia** de que las tareas se realizaron (registro). Éste es un documento importante para mantener la repetibilidad de los controles administrativos ya mencionada.
- **Instructivos de Trabajo:** son **instrucciones** detalladas y muy dependientes del contexto sobre cómo realizar una función o tarea específica (con un alto contenido de "cómo"). Se diferencian de los procedimientos en que el instructivo no asigna responsabilidades (sólo se explica *cómo* se debe desarrollar una tarea, *independientemente de quién* lo haga).
- **Guías:** son documentos que establecen **recomendaciones** o **sugerencias**, pero no de cumplimiento obligatorio. Una guía puede servir como referencia metodológica o para interpretar una situación particular. Por ejemplo, la norma ISO/IEC 27002 (la ex ISO/IEC 17799) es una guía para la implementación de controles de seguridad, y se la toma como referencia normativa para la correcta interpretación de la norma ISO/IEC 27001 (que sí es de cumplimiento obligatorio, pero no siempre es sencilla de aplicar a todas las circunstancias).
- **Registros:** son aquellos documentos en donde se guardan **resultados** obtenidos o **evidencia** de actividades desempeñadas. Por ejemplo, un *log* de accesos de un servidor, una base de datos donde se guardan los datos de un sistema CRM, un formulario, una orden de pedido impresa y archivada, etc. Algunos registros se asocian con un documento **plantilla** (o *template*) que se va completando en forma manual o automática. En Seguridad de la Información, los registros son muy importantes (lo mismo que asegurar que no sean manipulados) para mantener el registro de responsabilidad (o *accountability*).

Además de los distintos tipos de documentos que una organización requiere, un esquema documental debe contar con un proceso asociado que controle la **redacción**, la posterior **revisión** (por ejemplo, por el área de Seguridad,

[29] Ob. cit., sección 3.4.5.

Legales o Auditoría para asegurar el cumplimiento de ciertos requisitos indispensables), la **aprobación** (por el nivel jerárquico que corresponda), la **publicación** y la **distribución**, así como el aseguramiento de que los documentos se encuentran **disponibles** y que no se usan versiones obsoletas[30]. Conviene definir las actividades y responsabilidades de control de la documentación en un procedimiento operativo (o equivalentemente, un control administrativo) que asegure el resguardo de la información documental. Se trata de un control doble: por un lado se protege la propia información documentada, pero también (de manera indirecta, si se quiere) se mejora la eficacia de los otros controles de seguridad que descansan en la documentación.

4.4 Gestión de Incidentes

Existe todo un conjunto de controles detectivos que se pueden implementar para descubrir eventos e incidentes de seguridad. Un **evento** de seguridad es "cualquier ocurrencia que indique la posibilidad de que se haya violado la política de seguridad, haya fallado algún control o situación previamente desconocida que pueda ser relevante desde la seguridad"; un **incidente** de seguridad es "uno o varios eventos de seguridad, inesperados o no deseados que tienen una probabilidad cierta y significante de comprometer la operación del negocio o amenazar la seguridad de la información"[31].

La organización debe ser capaz de detectar la mayor cantidad de incidentes para poder responder en tiempo y forma. Debe existir un proceso de **escalamiento** de los incidentes, comprendido por personas clave de la organización (no solamente los administradores de seguridad), **contención** y **recupero** de los mismos.

Otro aspecto importante de la gestión de la Seguridad de la Información tiene que ver con la retroalimentación generada a partir de la información de la que disponemos para saber si las acciones tomadas han sido eficaces o no. Las buenas prácticas establecen que los incidentes también nos deben dejar **lecciones aprendidas**. El control detectivo (y administrativo) más obvio para obtener esta retroalimentación es la revisión de los *logs* de los distintos sistemas y dispositivos de seguridad, servidores y estaciones de trabajo. No es una tarea fácil de gestionar en forma consistente y es muy demandante de tiempo y de habilidades técnicas.

En la práctica, la abundante **cantidad de datos** generados en los sistemas reviste una dificultad fundamental, ya que se supone que una persona lo suficientemente preparada los debe revisar de manera rutinaria, dedicando una buena cantidad de su tiempo con el objetivo de descubrir algún hecho extraño que merezca su atención. El "triste" resultado es que en la mayoría de los casos será una falsa alarma, o no habrá suficiente información como para

[30] Nuevamente, estos requisitos aparecen en cualquier estándar ISO, tales como ISO 9001 e ISO/IEC 27001.
[31] Ambas definiciones son tomadas de la ISO/IEC 27001, ya citada, secciones 3.5 y 3.6.

realizar un diagnóstico preciso de lo que realmente ocurrió. Existe un problema motivacional evidente, por un lado, se necesita un profesional altamente preparado para poder "separar la paja del trigo", pero que realice una tarea muy rutinaria, más típica de una posición más bien inicial o *junior*. Y, dando vuelta el razonamiento, una persona que acaba de iniciarse y que probablemente aprecie tener que "deglutir" en forma rutinaria una buena cantidad de datos como parte de su incipiente formación profesional, no estará lo suficientemente capacitado ni enterado de los detalles operativos y de infraestructura requeridos para el análisis.

La implementación de poderosas **herramientas informáticas** de análisis y correlación de eventos, nos prometen automatizar al máximo lo rutinario y "aburrido para un humano", consolidando la información necesaria para que un experto la analice y realice las averiguaciones pertinentes. Sin embargo, las herramientas requieren de un período de varios meses de ajuste o *tunning*[32], para poder filtrar información redundante o no deseada (típicamente, falsas alarmas). Este ajuste es importante, no sólo para evitar "insensibilizar" a quien realiza el análisis (después de un período de acostumbramiento a falsas alarmas, uno tiende a menospreciar situaciones que realmente podrían ser riesgosas), sino también para optimizar los recursos requeridos para el almacenamiento de los datos.

Existe otro problema relacionado con las **fuentes** de donde se obtienen los eventos que estamos analizando. El grado de compatibilidad de la herramienta de análisis con los equipos desde donde los eventos son detectados no siempre es la óptima, y además, nuevas fuentes pueden aparecer o desaparecer en forma dinámica, en función a las necesidades operativas de la organización. Para volver más difícil esta situación, las fuentes en muchos casos son administradas por diversas áreas de la organización. Por ejemplo, si el Departamento de Tecnología necesita aliviar la carga de la infraestructura de la que es responsable, no va a estar "deseoso" de esperar a que el Departamento de Seguridad tenga lista la aplicación de captura de incidentes *antes* de poner en producción un nuevo servidor. Ni qué hablar de las trabas que surgen por la falta de espacio de almacenamiento de los datos.

El tema central en la gestión del análisis y correlación de eventos es entender que no se trata de un "proyecto" de seguridad, sino de una actividad que involucra a toda la organización. Como tal, previamente a la implementación de una herramienta tecnológica debe existir un procedimiento de escalamiento de cualquier sector operativo al detectar un evento o incidente de seguridad. Nuevamente, se trata de un control administrativo, y para que tenga éxito, se requiere de coordinación y entrenamiento entre los demás sectores operativos involucrados (y en el propio sector de Seguridad), no sólo en cuanto a lo técnico (por ejemplo, definir "qué constituye concretamente un evento o incidente"), sino también frente a la importancia de la detección de eventos para la gestión de la Seguridad (toma de conciencia).

[32] O "*tuneo"*, como se dice en la jerga tecnológica.

4.5 Gestión de la Continuidad del Negocio

Se podría escribir un libro completo sólo sobre Gestión de la Continuidad del Negocio o BCM (por *Business Continuity Management*). De hecho, existe una extensa bibliografía sobre la materia, que además cobró relevancia después de los atentados a las torres gemelas y desastres tales como los producidos por el Huracán Katrina en EE.UU. Se trata de uno de los temas con mayor nivel de madurez dentro de la Seguridad de la Información, y es el que más fácilmente entiende y apoya la Alta Dirección. Desde la perspectiva de la Seguridad de la Información, la propiedad de la información que se protege es la **disponibilidad**, pero sobre todo (y por eso el apoyo antes mencionado) se protege la continuidad de las funciones del negocio, incluso durante una situación de emergencia, o luego de un desastre.

La Continuidad del Negocio se puede definir de la siguiente manera: "cómo mantener el negocio de la organización funcionando, todo el tiempo, a pesar de las contingencias externas". Pero vale la pena introducir la definición de la *British Standards Institution* (BSI):

> **2.3 Gestión de la Continuidad del Negocio (BCM)**
>
> **Proceso integral** que identifica amenazas potenciales a la organización y los impactos a las operaciones del negocio que esas amenazas, podrían causar si se concretan; y que provee un marco de trabajo para la construcción de **resiliencia** organizacional mediante la capacidad para una efectiva **respuesta** que proteja los intereses de las partes interesadas, la reputación, la marca y las actividades que agregan valor.
>
> "Nota: la gestión de la continuidad del negocio incluye la gestión del recupero o continuidad de las actividades del negocio en caso de una interrupción, y la gestión del programa general a través de entrenamientos, ejercicios y revisiones, para asegurar que los planes de continuidad del negocio se mantienen actualizados.[33]

Dicho de otra manera, la Gestión de la Continuidad del Negocio es un proceso continuo de **preparación** para cuando ocurra un incidente (más o menos grave) que pueda interrumpir el normal desenvolvimiento de las actividades de la organización. El proceso continuo de gestión y gobernabilidad apoyado por la Alta Dirección y con los recursos apropiados se llama Programa de Gestión de la Continuidad del Negocio, y cuenta con las siguientes etapas, según la norma BS 25999-1:

- Establecer la **Política de BCM.**
- Asignar **responsabilidades.**

[33] *"BS 25999-1:2006 – Business continuity management – Part 1: Code of practice"*, Londres, BSI, 2006, sección 2.3.

- Definir, documentar, implementar y mantener las actividades del **Ciclo de Vida de BCM:**
  - **Entender** la organización.
  - Determinar la **estrategia** de BCM.
  - Desarrollar e implementar la **respuesta** de BCM.
  - **Pruebas**, **mantenimiento** y **revisión.**
- **Concientizar** y **entrenar** a los involucrados.

Una representación bastante simplificada de lo que ocurre normalmente se muestra en la figura 4.2. Podemos considerar que desde el punto de vista del BCM, la organización se encuentra siempre dentro de dos "estados": el estado **normal**, o el estado de **emergencia**. En estado normal, se desarrollan las actividades de gestión, prueba y mejora del esfuerzo de continuidad, que se documenta (principalmente) en los **Planes de Continuidad del Negocio**, o **BCP** por *Business Continuity Plan(s).*

El o los BCP son una colección documentada de procedimientos e información que se desarrolla, compila y mantiene para su **uso inmediato** en un incidente, para que la organización continúe con sus actividades críticas en un nivel aceptable predefinido[34]. Son las instrucciones que debe seguir la organización durante una emergencia.

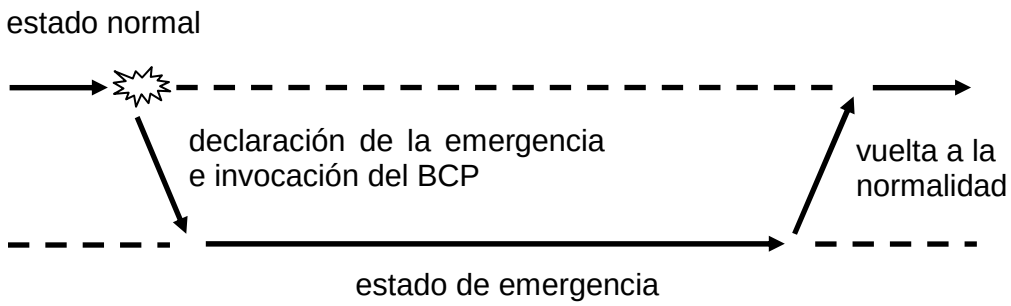

Figura 4.2

A esta altura, resultan evidentes las similitudes de las buenas prácticas de Continuidad del Negocio con las de Seguridad de la Información: debemos establecer una política, asignar responsabilidades, documentar, determinar estrategias, implementar medidas, probar y revisar lo implementado y concientizar a los involucrados. Tampoco queda afuera la Gestión de Riesgos, sólo que BCM se concentra más en la identificación de las consecuencias o impacto de las interrupciones del negocio (dicho proceso se llama **Análisis de Impacto en el Negocio** o **BIA**, por *Business Impact Analysis*) que en la identificación y ponderación de las amenazas que provocan dichas interrupciones. Sin embargo, el proceso de Análisis de Riesgos bien puede superponerse o complementarse con el de Análisis de Impacto en el Negocio.

El proceso de gestión de la Seguridad de la Información es tan similar al BCM que muchas veces, para contar con el apoyo de la Alta Dirección y de

[34] Adicionalmente pueden existir Planes de Gestión de Incidentes (qué hacer inmediatamente ocurrido un incidente), y Planes de Recupero del Negocio (cómo volver a la normalidad una vez manejada la crisis), pero en general se los incorpora *dentro* de los BCP.

sectores claves de la organización, es preferible comenzar por un programa de BCM que incorpore gradualmente aspectos de Seguridad, antes que hacerlo con un Programa de Seguridad de la Información que contenga las actividades de BCM.

4.6 Cumplimiento (*Compliance*)

El término *compliance* muchas veces es utilizado como cumplimiento *legal* o *regulatorio*, pero en realidad, debe entenderse como cumplimiento de los **requisitos**. Dichos requisitos son **externos** a la organización: regulatorios, contractuales y legales, pero también de las buenas prácticas o requisitos implícitos derivados de las expectativas de los clientes y otras partes interesadas.

Las actividades de cumplimiento están empezando ser más visibles en las organizaciones, sobre todo en la medida en que las **leyes** y **gobiernos** están empezando a tomar nota de la importancia de la información para el funcionamiento de las sociedades. Los requisitos pueden analizarse de manera independiente y simplemente cumplirse. O pueden incluirse en el contexto de la gestión de los riesgos del negocio y analizarse como una amenaza más (la de no cumplir con una reglamentación, que supondrá un impacto determinado). El enfoque utilizado dependerá del contexto de la organización (especialmente, el regulatorio).

A medida en que las consecuencias de no cumplir los requisitos externos (de todo tipo: penales, económicas, comerciales, o en imagen) cobran relevancia, aumenta la necesidad no sólo de gestionarlos y cumplirlos, sino de **evidenciar** su cumplimiento. Muchas veces, la carga de la prueba está del lado de la organización, ya sea de forma explícita, o implícitamente debido a las expectativas generadas en las partes interesadas. Para requisitos bien definidos como los legales o regulatorios, evidenciar el cumplimiento puede ser más o menos sencillo, en función de la calidad de la prosa de las leyes y contratos. Pero para el caso de otros requisitos más ambiguos, como los relacionados con expectativas de seguridad (o privacidad) entran en juego dos conceptos muy utilizados en los países más adelantados en materia de cumplimiento (EE.UU y los países de Europa):

- ***Due Dilligence* (debido proceso):** es el proceso de **investigación** previo antes de tomar alguna decisión organizativa importante (adquisiciones, fusiones, venta, incorporación de personal jerárquico, etc.) que da como resultado que la organización entiende los riesgos asociados con lo que se pretende hacer.
- ***Due Care* (debido cuidado):** es el principio del **"hombre razonable"**, muy utilizado en las cortes de EE.UU., que establece que la empresa hace (o hizo, en el caso de una disputa) todo lo que está (o estuvo) a su alcance para controlar los riesgos. El concepto del *due care* es independiente del resultado de un incidente de seguridad, sólo se la considera culpable a la organización en la medida en que haya existido desidia en el debido cuidado.

En Argentina las normas más comunes que motivan a las organizaciones a implementar programas de cumplimiento son:

- ***Sarbanes Oxley Act (SOX):*** ley de EE.UU. que regula a las organizaciones que operan en la bolsa de Nueva York, quienes deben demostrar eficacia en los controles vinculados a procesos que impacten sobre la **integridad** de los estados financieros. Fortalece al gobierno corporativo e intenta reestablecer la confianza del inversor luego de los escándalos de Enron y WorldCom.
- ***Payment Card Industry Data Security Standard (PCI):*** estándar de Seguridad en materia de protección de datos de los consumidores para evitar fraudes con **tarjetas de crédito** que deben cumplir las organizaciones que operan con VISA, American Express, MasterCard, Diner's Club, JCB y Discover.
- **Ley Nacional de Protección de Datos Personales:** ley Argentina de protección de la **privacidad** de los ciudadanos respecto de la información personal contenida en bases de datos de organizaciones. Las organizaciones deben registrar las bases de datos que contienen información personal y aplicar controles adecuados de protección. Se reglamenta con resoluciones de la Dirección Nacional de Protección de Datos Personales.
- **Comunicación A 4609 del BCRA:** para **entidades financieras** (principalemente, bancos). Normativa basada en COBIT, las normas IRAM/ISO/IEC 17799:2002 e ISO/IEC 27001:2005, entre otras. Es el primer paso dentro del roadmap al cumplimiento de Basilea II.

5 Controles Tecnológicos y Físicos

A lo largo del libro hemos ido recorriendo elementos claves de una buena gestión de la Seguridad de la Información. El esfuerzo requerido por todos los integrantes de la organización es considerable.

Primero, se debe alinear el programa de seguridad con el **negocio** de la organización para que éste no carezca de realismo. Luego, deben plantearse directrices, planes y objetivos a cumplir, contando con la voluntad de **invertir** los recursos necesarios, ya sea en tiempo, dinero o en la asignación de prioridades.

Sólo una vez que se cumplen estos requisitos (que las normas ISO llaman "Responsabilidad de la Dirección") la implementación del programa de seguridad puede avanzar sobre los aspectos más bien **administrativos** que hemos cubierto a lo largo del libro: identificación y clasificación de activos de información, asignación de dueños y custodios, gestión de los riesgos a la información, definición de controles (o contramedidas), asignación de responsabilidades, documentación de actividades y controles, gestión de los incidentes (incluyendo la incorporación de lecciones aprendidas), gestión de la continuidad del negocio y cumplimiento.

Paralelamente, el programa de seguridad deberá asegurar que las **personas** (el "eslabón más débil de la seguridad" según numerosa bibliografía) estén adecuadamente entrenadas y enteradas de la importancia de la preservación de las Seguridad de la Información en las actividades del negocio, también denominado "toma de conciencia" o *awareness*. Este aspecto se trata con más detalle en el episodio 2.

A continuación, las buenas prácticas reconocen la importancia de la **Seguridad Física y Ambiental** para la protección de la información y las personas que la generan y toman decisiones basadas en ella. La Seguridad Física, Ambiental y Patrimonial es más antigua como disciplina que la Seguridad de la Información y su bibliografía es tanto o más extensa. Los conceptos y recomendaciones son, en muchos casos, asimilables y análogos en ambas disciplinas, al punto tal que en ambas industrias se está empezando a hablar de una convergencia de las dos disciplinas. Por un lado, la seguridad física de los equipos (incluyendo cableado, servicios de soporte, etc.) y las condiciones del medio ambiente (humedad, contaminación, temperatura, etc.), influyen de manera directa en la preservación de la información; y por el otro, la tecnología de la seguridad patrimonial, ambiental o física, depende cada vez más de otros sistemas con información de soporte que debe ser protegida (pensemos, por ejemplo, en la importancia de los perfiles de acceso en un sistema de control de puertas y molinetes con tarjetas de aproximación).

Es recién en este punto de la implementación del programa de seguridad, después de considerar todos los aspectos organizacionales y de seguridad física, que podemos pensar en aplicar eficazmente la **tecnología** de seguridad en la forma de: productos, *software*, *hardware*, sistemas,

appliances, *tokens*, *passwords*, encripción, controles de acceso, *firewalls*, antivirus, cintas de *backup*, parches de seguridad, etc. Existe todo un universo de técnicas y conocimientos específicos que aplican a este campo que las buenas prácticas normalmente llaman: seguridad operacional; controles de accesos; seguridad en el desarrollo de *software*; seguridad en aplicaciones (incluyendo seguridad web y seguridad de bases de datos); criptografía; diseño y arquitectura de seguridad (en *software* de base, *hardware* y componentes electrónicos); y seguridad en redes, entre otros. Este aspecto tecnológico excede el alcance del libro por su complejidad, longitud y constante cambio.

No estoy ubicando a la tecnología *a continuación* de una serie de requisitos organizacionales porque la considere poco importante, sino todo lo contrario: la tecnología es la causa por la que nos estamos convirtiendo en sociedades de la información (y en definitiva, lo que motiva este libro). Sin embargo, las recomendaciones que surgen de las buenas prácticas de seguridad (que en principio deberían disminuir la complejidad de su gestión) no son fáciles de llevar de la teoría a la acción, y es esta dificultad la que explica la mayoría de los fracasos en la preservación de la confidencialidad, la integridad y la disponibilidad de la información. No es tanto la tecnología la culpable de estos errores, sino no saber usarla, o creer que basta por sí misma.

6 Epílogo

En la sección 1.1 hable de un recorrido personal por la Seguridad de la Información. Me inicié en el campo de la Seguridad de la Información en abril del 2000 (cuando todavía era una "novedad") en una empresa de servicios tecnológicos con una estructura de organización innovadora[35]. En mi sector éramos "Analistas de Seguridad Informática", con una tarea doble: por un lado estaba el análisis sobre las condiciones de seguridad, y por el otro la administración de la tecnología de seguridad de la empresa. Todo lo que hacíamos se centraba en la tecnología: desde la administración de perfiles de usuarios (o "reseteo" de *passwords*, las tareas "tradicionales" de Seguridad Informática), hasta la administración de los firewalls de las redes de la organización (incluyendo la red de servicios corporativos y otras redes que brindaban servicios directamente al cliente). Pensábamos que controlando la tecnología manteníamos la Seguridad de la Información de la empresa.

En orden cronológico, me dediqué a administrar equipamiento de seguridad, adoctrinar y capacitar a administradores de sistemas, realizar revisiones en infraestructura de sistemas, participar de definiciones en proyectos de tecnología (nuevos y existentes), analizar información de seguridad (y desarrollar herramientas ad hoc para poder manejar el volumen), investigar y desarrollar tecnología de seguridad, liderar un grupo de seguridad operativa (junto con los usuarios, los administradores, nuestro jefe, nuestro director, y los otros directores que vienen asociados), vender *software* y *hardware* de seguridad (convenciendo a los clientes de que la solución a sus problemas era la tecnología), implementar los productos y dar soporte a los clientes (pre y pos venta), y por último, asesorar a las organizaciones en la implementación de las buenas prácticas de Seguridad de la Información (incluyendo establecimiento de planes de continuidad del negocio, implementación de sistemas de gestión, gobierno corporativo, e incorporación de tecnología de seguridad).

Es decir, que en mi carrera transité el camino inverso al propuesto a lo largo de este libro (!).

Por suerte, diez años más tarde, tanto las buenas prácticas de la seguridad como yo hemos evolucionado considerablemente, de un enfoque exclusivo en los aspectos tecnológicos, a uno basado en la gestión de la organización y su negocio (con el caballo por delante del carro y no al revés). O tal vez deba decir que las buenas prácticas *ya habían evolucionado* en el año 2000, cuando Bruce Schneier llegaba a la conclusión de que "la seguridad es un proceso, no un producto"[36], solo que recién ahora se empiezan a dar las condiciones como para *ponerlas en práctica.*

[35] Ver Mintzberg, Henry: *Mintzberg y la Dirección*, Madrid, Ediciones Díaz de Santos, 1991. La estructura de este tipo de organizaciones suele modificarse con frecuencia para hacer frente a un contexto por lo general dinámico. En mi caso, se trataba de una industria joven de servicios tecnológicos como lo era la comunicación celular hace unos años.

[36] Schneier, Bruce: *Secrets and Lies: Digital Security in a Networked World*, Nueva York, John Wiley & Sons, 2000.

***

Hasta aquí, solamente hemos repasado los aspectos *salientes* de las buenas prácticas (y debo decir que en una forma bastante *superficial* y *compacta*). En los próximos episodios de esta serie intentaré dar cuenta de los aspectos prácticos y de su complejidad, así como también de una posible solución integradora alineada con los requisitos de la norma ISO 27001.

CONTINUARÁ

A. Anexos

A 1. Bibliografía utilizada

Buenas Prácticas de Seguridad de la Información:

- Harris, Shon: *CISSP Certification, All-In-One Exam Guide, Second Edition*, Emeriville, McGraw-Hill, 2003.
- Information Systems Audit and Control Association (ISACA), htttp://www.isaca.org.
- Jaquith, Andrew: *Security Metrics: Replacing fear, uncertainty, and doubt*, Upper Saddle River (NJ), Addison-Wesley, 2007.
- Mitnick, Kevin y Simon, William: *The Art of Deception: Controlling the Human Element of Security*, Indianapolis, Wiley Publishing, 2002.
- Mitnick, Kevin y Simon, William: *The Art of Intrusion: The Real Stories Behind the Exploits of Hackers, Intruders & Deceivers*, Indianapolis, Wiley Publishing, 2005.
- National Institute of Standards and Technology (NIST), http://www.nist.gov.
- Schneier, Bruce: *Secrets and Lies: Digital Security in a Networked World*, Nueva York, John Wiley & Sons, 2000.
- Tipton, Harold y Henry, Kevin: *Official (ISC)^2 Guide to the CISSP CBK*, Boca Ratón, Auerbach, 2007.

Normas ISO y BS:

- *BS 7799-3:2007 – Information security management systems – Part 3: Guidelines for information security risk management,* Londres, BSI, 2006.
- *BS 25999-1:2006 – Business continuity management – Part 1: Code of practice*, Londres, BSI, 2006.
- *BS 25999-2:2007 – Business continuity management – Part 2: specification*, Londres, BSI, 2007.
- *IRAM ISO 9001:2000 - Sistemas de Gestión de la Calidad - Requisitos*, Buenos Aires, IRAM, 2001.
- *ISO 9000:2005 - Sistemas de Gestión de la Calidad - Fundamentos y Vocabulario*, Ginebra, ISO, 2005 (traducción certificada).
- *ISO/IEC 27001:2005 – Information technology – Security techniques – Information security management systems – Requirements*, Ginebra, ISO, 2005.
- *ISO/IEC 27002:2005 – Information technology – Security Techniques – Code of practice for information security management*, Ginebra, ISO, 2005.

Buenas Prácticas de Gestión *(Management)* y Tecnología de la Información:

- Adams, Scott: *The Dilbert principle*, Nueva York, Harper Collins, 1997.
- Dilbert.com, http://www.dilbert.com.
- Drucker, Peter: *Management, tasks, responsibilities. practices*, Nueva York, Harper Perennial, 1993
- Gros, Carlos Augusto: *Gestión de Riesgos*, Buenos Aires, Intercoop, 2006.

- Mintzberg, Henry: *Mintzberg y la Dirección*, Madrid, Ediciones Díaz de Santos, 1991.
- Saroka, Raúl Horacio: *Sistemas de información en la era digital*, Buenos Aires, Fundación OSDE, 2002.

A 2. Acerca del Autor

Juan Ignacio Trentalance es Ingeniero Electrónico por la Universidad de Buenos Aires (UBA), recibido con Diploma de Honor, y Especialista en Gestión de Servicios de Tecnología y Telecomunicaciones por la Universidad de San Andrés (UdeSA). El presente libro está basado en la tesina requerida para completar la especialización.

Es Director de *Porto, Trentalance, Antúnez y Asociados*, consultora que se dedica a la Seguridad de la Información y a la Calidad, con foco en la implementación de Sistemas de Gestión basados en las normas ISO (9001, 27001, 20000, etc.).

Es CISSP *(Certified Information Systems Security Professional)* por ISC2 *(International Information Systems Security Certification Consortium)*, Auditor Líder en ISO 9001 e ISO/IEC 27001 por Det Norske Veritas (DNV), y Evaluador de Calidad en Auditorías Internas por el Instituto de Auditores Internos de la Argentina (IAIA). También es egresado del Programa de Formación de Emprendedores en el Centro de Emprendedores del Instituto Tecnológico de Buenos Aires (ITBA).

Tiene experiencia como Analista de Seguridad Informática y en *assessments* de Seguridad de plataformas Unix, redes de datos y de telecomunicaciones. Se ha desempeñado como coordinador de Seguridad Operativa en *Movistar* y como consultor independiente para empresas de primer nivel. Participó como implementador en uno de los primeros Sistemas de Gestión de Seguridad de la Información (ISMS) de la Argentina en la empresa *Interbanking*, certificado por TÜV Rheinland bajo la norma ISO/IEC 27001.

Es docente de la Especialización en Servicios y Redes de Telecomunicaciones de la Facultad de Ingeniería de la UBA, en la materia Seguridad en Redes de Telecomunicaciones. Además ha participado como instructor en cursos intensivos de preparación para la certificación CISSP, y ha dictado seminarios y conferencias sobre Biometría, *Business Impact Analysis*, Seguridad Operativa, ISO 27001 y Métricas de Seguridad. Ha realizado investigaciones en tecnología de Biometría por Voz en la UBA con el apoyo del Gobierno de la Ciudad de Buenos Aires.

Es miembro de ISSA *(Information Systems Security Association)*, y socio fundador del capítulo local ISSAArBA (ISSA Argentina Buenos Aires), donde se ha desempeñado como Tesorero y Presidente del mismo.