RESUMEN DE LA TESIS DOCTORAL

Hoy en día, las empresas e instituciones son cada vez más complejas, tanto desde el punto de vista orgánico como desde el punto de vista funcional. Estas se mueven en un contexto global y altamente dinámico donde parece necesario un estudio en profundidad de una seguridad integral que dé respuesta a las demandas, cada vez más frecuentes, de protección de los activos de las organizaciones, independientemente de la naturaleza física o lógica de los mismos.

Así, un profesional especializado en la protección lógica de tales activos (e.g., un ingeniero de telecomunicación responsable de la ciberseguridad dentro de una organización) debería, al menos, no solo dominar con soltura metodologías y técnicas de seguridad propias de su ámbito de formación académica y correspondiente experiencia laboral, sino también conocer y considerar otras muchas áreas o disciplinas que resultarán fundamentales a la hora de tomar decisiones y ejercer sus responsabilidades.

El principal objetivo de esta Tesis Doctoral es proponer un marco de referencia y modelo de gestión de seguridad integral que se ajuste a las necesidades de las organizaciones actuales y al contexto que las rodea, aunando una actuación complementaria y conjunta entre los principales actores, como son las áreas de seguridad física (e.g., seguridad patrimonial, seguridad corporativa, etc.) y las áreas de seguridad lógica (e.g., seguridad informática, seguridad de la información, ciberseguridad, etc.), entre otros, en pos de la protección de los activos (tangibles e intangibles) de tales organizaciones.

Adicionalmente al objetivo anterior, también se pretende concretar una propuesta de marco de referencia de seguridad integral. Para ello, se han presentado sendas ejemplificaciones del modelo propuesto sobre dos escenarios teóricos: un primer caso contextualizado sobre una hipotética empresa de consultoría de tamaño pequeño, donde el foco se sitúa en cómo abordar la implantación en una organización donde no existe ninguna función formal de seguridad; y un segundo caso sobre una empresa ficticia de alquiler de vehículos de tamaño mediano, donde el interés ya no reside tanto en la puesta en marcha del marco de seguridad integral, sino en cómo una perspectiva integral de la seguridad contribuye a la resolución eficiente de ciertos problemas en la operativa de la empresa y, por ende, a la consecución de sus objetivos empresariales. Mediante estos ejemplos se ponen de manifiesto las bondades aportadas por el marco de referencia de seguridad integral propuesto, así como los posibles problemas e inconvenientes a los que se habría de hacer frente durante la implementación, despliegue, operación y mantenimiento del modelo.

Cualquier activo de una organización es susceptible de convertirse en víctima de un ataque deliberado o un incidente fortuito, independientemente de si el origen es físico, lógico o mixto, por lo que la adopción de un marco para una seguridad integral como el propuesto en esta Tesis Doctoral contribuiría al correcto desarrollo de las operaciones de una organización y a la mejora en la conciencia de las organizaciones sobre los asuntos de seguridad. Todo ello, sin dejar de lado una clara mejora en el desarrollo sostenible de la organización gracias a la optimización del uso de recursos destinados a la protección de sus activos, ampliando el rango de acción de la protección con los mismos recursos y evitando grandes brechas de seguridad derivadas de enfoques inconexos.

De esta manera, el trabajo desarrollado revela la idoneidad del marco de referencia propuesto, así como de la aproximación que, tradicionalmente, se viene adoptando en el ejercicio de las funciones de seguridad, ya sean de carácter físico o lógico, además de proponer alternativas en los aspectos formativos y de aprendizaje que, tanto los profesionales de la seguridad como los aspirantes a serlo, deberían considerar.

Esta Tesis Doctoral se estructura alrededor de los siguientes capítulos:

- El Capítulo 1, donde se expresa la necesidad de una visión integral de la seguridad, incluye los motivos que justifican su razón de ser, así como los objetivos que se establecen en esta memoria, la metodología empleada y el plan de trabajo diseñado para alcanzar dichos objetivos.

- El Capítulo 2, dedicado al estudio y planteamiento de la seguridad de los activos de una organización, contempla la evolución temporal del concepto de seguridad hasta nuestros días, profundizando en las principales vertientes física y lógica de protección y destacando la misión de elementos clave para garantizar la efectividad de la seguridad, tales como el análisis de riesgos, la inteligencia o el marco regulatorio de la actividad.

- El Capítulo 3, en el que se propone un marco de referencia para una seguridad integral, contempla aspectos estructurales y funcionales de seguridad integral capaces de atender a los requisitos de protección de los activos tangibles e intangibles de la organización y a situaciones extraordinarias de crisis, sin olvidar la necesidad de cumplir con las normas, leyes y regulaciones vigentes. Adicionalmente, este capítulo incluye una propuesta de formación concreta en seguridad integral para profesionales.

- El Capítulo 4, encargado de exponer dos casos de uso para el marco de referencia de seguridad integral, pretende mostrar dos vías de aplicación del modelo útiles para las organizaciones: un primer caso básico de implantación del modelo sobre una empresa pequeña (i.e., entre 10 y 49 trabajadores) y un segundo caso de explotación (y posterior implantación) del modelo sobre una empresa mediana (i.e., entre 50 y 249 asalariados).

- El Capítulo 5, presenta las principales conclusiones de la Tesis Doctoral, así como las aportaciones realizadas con la misma y los desarrollos futuros.

- Por último, en los Apéndices A, B, C, D y E se recogen elementos que, sin ser específicos de la propuesta de marco de referencia de seguridad integral del Capítulo 3, resultan fundamentales para la correcta interpretación y aplicación del mismo, tanto desde el punto de vista teórico como práctico, así como de la propia Tesis Doctoral en su conjunto.

Capítulo 5

Conclusiones, aportaciones y desarrollos futuros

5.1. Conclusiones

La seguridad es una herramienta necesaria para mitigar y, en su caso, evitar la materialización de ciertas amenazas que impactan negativamente sobre el desarrollo de las operaciones de una organización. Sean de la naturaleza que sean, se trata de un problema grave que crece y avanza exponencial e inexorablemente. Desafortunadamente, nadie puede decir que está fuera de peligro.

Cualquier activo de una organización es susceptible de convertirse en víctima de un ataque deliberado o un incidente fortuito, independientemente de si el origen es físico, lógico o mixto, por lo que la adopción de un marco para una seguridad integral como el propuesto en esta Tesis Doctoral contribuye al correcto desarrollo de las operaciones de una organización y a la mejora en la conciencia de las organizaciones sobre los asuntos de seguridad. Todo ello, sin dejar de lado una clara mejora en el desarrollo sostenible de la organización gracias a la optimización del uso de recursos destinados a la protección de sus activos, ampliando el rango de acción de la protección con los mismos recursos y evitando grandes brechas de seguridad derivadas de enfoques inconexos.

5.1.1. Condicionantes analizados

En el contexto de la protección de los activos de una organización, dentro de la mayoría de estas suelen cohabitar dos facciones a alto nivel que provienen

de dos orígenes bien diferenciados y cuya composición también es muy diferente. La primera de estas corrientes es la que tradicionalmente se ha venido a denominar seguridad corporativa, seguridad física, seguridad patrimonial, etc. Independientemente de cómo se la conozca, su función es la protección tradicional de los bienes, las instalaciones y las personas de la organización, cuyos responsables suelen corresponderse con miembros de las escalas superiores de los ejércitos, de los cuerpos de seguridad pública e, incluso, de centros de inteligencia. La segunda de las áreas en cuestión es la llamada seguridad informática, seguridad lógica, seguridad de la información o, más recientemente, ciberseguridad, cuyo origen es muy diferente al caso anterior, con una componente técnica muy profunda, vinculada a la gestión de riesgos de tecnología, la recuperación ante desastres, la configuración de redes, etc. Se trata de un ámbito muy próximo al negocio de la organización y con una historia muy reducida en comparación con la seguridad física. En la actualidad, la gran mayoría de las organizaciones todavía mantienen sendas estructuras paralelas, con operaciones separadas y estancas, para abordar la seguridad de sus activos. Independientemente de que, en algún caso, la seguridad física y la seguridad lógica puedan compartir elementos tales como personas, inteligencia o infraestructura, los objetivos de ambas áreas siguen siendo dispares, las plataformas de trabajo siguen siendo inconexas, los presupuestos siguen siendo independientes, los estándares de trabajo no están coordinados, etc., con el consiguiente impacto negativo sobre el fin último, es decir, la protección de los activos de la organización haciendo un uso razonable, óptimo y eficiente de los siempre limitados recursos internos.

En estos momentos no existen problemas aislados de seguridad, sino que cualquier incidente tiene diversas dimensiones cuyos impactos deben ser analizados por profesionales coordinados capaces de contener el incidente y sus implicaciones negativas. No existen problemas exclusivos o independientes de cualquier área de la organización. ¿Acaso cuando desde los departamentos de seguridad física investigan algún caso de fraude no solicitan correos electrónicos, ordenadores personales o teléfonos móviles de la organización con los que llegar a conclusiones certeras y, llegado el caso, respaldar una determinada acción coercitiva? ¿Acaso cuando se ponen en marcha planes directores de seguridad lógica no se demanda la presencia de elementos físicos de seguridad para el control de accesos, la videovigilancia o la continuidad de negocio? Por no hablar de aquellas circunstancias en las que, ante requisitos vitales de autonomía y confidencialidad (e.g., una investigación interna de fraude de algún empleado, un requerimiento judicial por alguna causa abierta contra la organización, etc.), la información y la inteligencia compartidas, junto con unos principios básicos de actuación, se convierten en una auténtica necesidad para la organización, donde la visión integral de la seguridad se antoja imprescindible.

La función seguridad ha de abordar situaciones complejas en su gran mayoría y, por momentos, difíciles de trasladar adecuadamente a la alta dirección de la organización para que esta las interprete debidamente. Por lo general, dado que no se trata de una ciencia exacta, la terminología empleada puede contribuir a aumentar la confusión de la organización a la hora de vislumbrar la relación de las operaciones de negocio con la seguridad. Se trata de una situación más común de lo imaginado que puede verse mucho más agravada cuando, en lugar de existir un único interlocutor y responsable de seguridad integral dentro de la organización, existen varios (e.g., responsable de seguridad física, responsable de seguridad lógica, etc.), debido a que la complejidad se ve multiplicada por cada uno de los responsables y la atención de la organización se ve dividida por el mismo factor: cada responsable de seguridad (e.g., física, lógica, etc.) presenta un problema independiente que debe prevalecer sobre los demás responsables frente a la organización, mientras que esta, la organización, comienza a dudar acerca de si ha entendido bien la situación, si el problema ya se lo ha escuchado antes a otro responsable y si debe prestar más atención a uno u otro interlocutor. Pero, sobre todo, la organización comienza a tener la sensación de que los aspectos de seguridad se han vuelto demasiado complejos y numerosos, a los que está dedicando más dedicación y esfuerzo de los que son necesarios para un área de apoyo a los procesos clave de la organización.

5.1.2. Sencillez y eficiencia

Así, frente a todo lo anterior y en línea con los objetivos planteados en §1.2, este trabajo plantea en el Capítulo 3 un modelo de seguridad integral que simplifica el desarrollo de la función de seguridad dentro de la organización bajo una perspectiva conjunta y singular, alejando las desconfianzas propias de la presencia de múltiples disciplinas complejas y aportando una normalización y desmitificación de la seguridad que permite a las organizaciones centrarse en sus prioridades y hacer un uso eficiente de su dedicación y esfuerzos ante problemas serios. El día a día de la seguridad está rodeado de problemas. Problemas de muy diversa índole e importancia, cuyo impacto puede abarcar desde aspectos estratégicos hasta otros operativos dentro de la organización, que pueden afectar a activos tangibles o intangibles, cuya resolución puede ser inmediata o necesitar de varias iteraciones para darlos por resueltos, que precisan de mucho tiempo y recursos para afrontarlos o que, por el contrario, prácticamente no requieren dedicación. El esfuerzo para la resolución de cualquier problema de seguridad siempre será menor desde un plano integral que desde un planteamiento divergente ya que en el último caso el esfuerzo se gestiona desde equipos de distintas disciplinas, mientras que en el primer caso los recursos están organizados y coordinados por lo que el esfuerzo se gestiona a través de disciplinas conjuntas.

5.1.3. Transparencia y agilidad

El planteamiento que hemos propuesto de la seguridad integral evoluciona el concepto tradicional de protección sobre los activos de la organización e incorpora actividades (e.g., estrategia, inteligencia, normativa, riesgos, etc.) sobre las que se reduce la complejidad e incluso la duplicidad operativa, con la consiguiente mejora de conflictos y confusiones, y se logra la optimización de recursos y cargas laborales. El modelo de seguridad integral propuesto aporta agilidad y capacidad de reacción a la hora de atender consultas urgentes o tomar decisiones en materia de seguridad dentro de la organización, ya sean de índole estratégica, táctica u operativa. Esta aproximación puede marcar la diferencia entre un resultado exitoso o no, ante una situación que se ha de gestionar desde el área de seguridad (e.g., un fraude financiero) gracias a la reducción de elementos de decisión o consulta no coordinados y al empleo de productos de inteligencia integrales.

5.1.4. Flexibilidad y sostenibilidad

En el mundo actual, que es eminentemente global, multidisciplinar, tecnológico, dinámico y no entiende de fronteras, la propuesta de una seguridad integral para los activos de una organización es capaz de ajustarse a la complicada realidad existente alrededor de la información, de las personas, de las regulaciones y, ante todo, de los complejos escenarios de negocio que exigen soluciones completas y sin fisuras. Para este fin, las capacidades de tratamiento, análisis e intercambio de datos ofrecen oportunidades formidables para el desarrollo de las funciones propuestas de seguridad integral, capaces de aportar soluciones claras, eficientes y perdurables, alineadas con las inquietudes y necesidades expresadas por la organización y facilitando el cumplimiento de los objetivos de negocio. Es más, en línea con ciertos valores que prevalecen en estos momentos, tales como la transparencia, la eficiencia o la sostenibilidad entre otros tantos, el marco para una seguridad integral propuesto debe precipitar en las organizaciones y ser un objetivo principal con el que, gracias a una función completa, compacta y suficiente, garantizar la seguridad de sus activos de forma apropiada, optimizando al máximo los recursos que la organización ofrece, así como el rendimiento y reutilización de los mismos a lo largo de las distintas funciones desempeñadas internamente.

5.1.5. Determinación y constancia

No existe una ruta única para lograr la estructura de seguridad integral dentro de una organización, sino que esta dependerá de las características de cada organización, en términos de negocios clave, volumen de empleados, clien-

tes, proveedores, estructura organizativa existente, etc. Sin embargo, el hecho de disponer de una propuesta de seguridad integral como la presentada aquí constituye un punto de partida interesante para iniciar la andadura hacia la materialización de la seguridad integral dentro de una organización. Los retos que se plantean en una organización a la hora de afrontar la seguridad integral no son menores, pero en ningún caso deberían bloquear su puesta en marcha, sobre todo si tenemos en cuenta los beneficios resultantes a través de una visión global y general de la seguridad de los activos de la organización. El concepto de seguridad integral presentado resulta, sin duda alguna, familiar para la mayoría de las organizaciones y profesionales de la seguridad (independientemente de si provienen de la vertiente física o de la vertiente lógica) que, conforme comienza a materializarse, va mostrando un conjunto de beneficios que, en última instancia, redundan en una mayor y mejor protección de sus activos, una racionalización de los medios, una optimización de los procesos, un aumento de la productividad y una mejora en la imagen de la organización. Por supuesto, todo ello constituye un ahorro de costes económicos para la organización. En este sentido, a lo largo del Capítulo 4 se han presentado dos casos particulares que muestran cómo abordar sendas situaciones para transformar dos PYME hacia una perspectiva integral de la seguridad.

5.1.6. Formación ventajosa

La puesta en marcha del modelo de seguridad integral propuesto en este documento precisa, no solo del mandato y respaldo claro e inequívoco de la alta dirección de la organización, sino también de un equipo humano con las capacidades y habilidades necesarias en distintos ámbitos de actuación, desde el perfil más ejecutivo hasta el más operativo. La posibilidad de acceso a estas posiciones (principalmente, de mandos intermedios y dirección) por parte de ingenieros de telecomunicación resulta una opción muy atractiva e interesante en las organizaciones debido a las amplias cualidades desarrolladas durante su formación universitaria en el primer y segundo ciclo (e.g., agilidad mental, capacidad de razonamiento, flexibilidad frente a problemas, propuesta de soluciones adecuadas al contexto particular, etc.), aun a sabiendas de que se pueden presentar carencias razonables (e.g., experiencia profesional, conocimientos específicos de seguridad, etc.) y se presupone que estas pueden ser suplidas en un breve espacio de tiempo. No obstante, cuanto mejor sea la preparación y especialización en seguridad integral, mayor será el valor aportado, percibido y reconocido por la organización. Por lo tanto, la opción de desarrollar iniciativas formativas en materia de seguridad integral, en línea con la propuesta presentada en este documento, ofrece una clara ventaja para los ingenieros de telecomunicación frente a otro tipo de candidatos o titulaciones (e.g., informáticos, militares, etc.).