AUTORES

FERNANDO SEVILLANO JAÉN

Licenciado en Ciencias Económicas y Empresariales (Universidad Complutense de Madrid, 1995), Máster en Gestión e Investigación de la Comunicación Empresarial (Universidad Rey Juan Carlos, 2009) y Doctor en Informática (Universidad Rey Juan Carlos, 2010). Con 25 años de experiencia, su carrera profesional se ha desarrollado siempre en el sector privado y en compañías del sector de las Tecnologías de la Información y las Comunicaciones, colaborando además estrechamente en tareas de docencia e investigación con diferentes universidades y escuelas de negocio. Esto le ha permitido apostar por un doble perfil de tecnología y negocio. En los últimos diez años se ha centrado en el área de la ciberseguridad, en particular, en entornos industriales y de infraestructuras críticas. Actualmente es Head of Cyber Risk Consulting en Willis Towers Watson, donde lidera el diseño y desarrollo de servicios en el área de la gestión del ciberriesgo.

MARTA BELTRÁN PARDO

Ingeniera Electrónica (Universidad Complutense de Madrid, 2001), Licenciada en Ciencias Físicas, rama de Física Industrial y Automática (UNED, 2003) y Doctora en Informática (Universidad Rey Juan Carlos, 2005). Actualmente es Profesora Titular de Universidad en la Universidad Rey Juan Carlos de Madrid, donde desde hace casi veinte años trabaja en sistemas distribuidos y en ciberseguridad y privacidad, tanto en docencia como en I+D+i. En estas disciplinas ha publicado más de 30 trabajos de investigación en revistas y congresos de reconocido prestigio. Es una de las pocas investigadoras españolas que ha publicado trabajos en conferencias

técnicas hacker internacionales como las BlackHat o las Defcon, o en conferencias técnicas militares como las ICC (actuales CYCON). Además es cofundadora del Cybersecurity Cluster de la Universidad Rey Juan Carlos, directora del MOOC de Ciberseguridad en las plataformas URJCx y MiriadaX, coordinadora del Grado en Ingeniería de la Ciberseguridad y directora del Máster en Ciberseguridad y Privacidad.

PRÓLOGO

La Ciberseguridad se puede definir como la protección de activos frente a amenazas, siempre que estos activos sean digitales y/o que las amenazas provengan del espacio digital. El reto que esta disciplina supone en la actualidad es que los activos pueden ser los tradicionales ordenadores, servidores o incluso teléfonos; pero también coches, contadores de la luz o lavadoras. Y que las amenazas, de muy diversos tipos, pueden afectar a una agencia de inteligencia, a una gran corporación o a un gobierno, pero también a un ciudadano anónimo o a un menor en edad escolar.

Para nosotros un profesional que se dedique a la Ciberseguridad debe dominar un conjunto de conocimientos orientados a diseñar, construir, adaptar y utilizar infraestructuras tecnológicas de confianza (seguras, respetuosas con la privacidad, fiables) incluso aunque se produzcan errores, omisiones o ataques maliciosos. Esta disciplina tiene que ver con las técnicas, pero también con los procesos, los métodos y las herramientas. Y al contrario que el resto de las disciplinas de la rama de la ingeniería o la tecnología presenta una particularidad que explica la necesidad de una colección como ésta que comienza con este libro: en muchas ocasiones, realiza su labor contra un adversario.

Los profesionales especializados en Ciberseguridad tienen un perfil muy completo que, además, evoluciona rápidamente. Es decir, son profesionales en constante formación ya que los adversarios ya mencionados evolucionan, así como la infraestructura tecnológica foco de su trabajo o los usos que le damos. ¿Quién nos iba a decir hace unos años que un coche iba a ser, eminentemente un sistema software? ¿O que se podría afectar a la salud de una persona mediante un ciberataque a su marcapasos? ¿O a una población entera amenazando, por ejemplo, a una potabilizadora de agua?

Esta colección es un proyecto personal de esta, su coordinadora; pero también de un grupo de profesores, investigadores y profesionales que colaboran hace años en formar a profesionales de la ciberseguridad, en investigar en temas punteros de la disciplina, en ayudar a distintos tipos de organizaciones a mejorar sus niveles de seguridad y en concienciar a distintos grupos de población (sobre todo, menores y personas en riesgo de exclusión social o tecnológica) sobre la importancia de conocer y de tomar las decisiones correctas para su protección personal.

Fruto de estas colaboraciones surgió hace ya unos años un curso abierto, masivo y online (un MOOC) del que se celebraron cuatro ediciones en dos plataformas diferentes y por el que pasaron cerca de 20.000 alumnos y alumnas. También el actual Máster en Ciberseguridad y Privacidad o el Grado en Ingeniería de la Ciberseguridad de la Universidad Rey Juan Carlos, pionero en España. También nuestras participaciones en otros programas de formación, en proyectos de investigación nacionales e internacionales, en iniciativas de transferencia, en medios de comunicación y foros de divulgación, en eventos, conferencias, etc. Todas estas actividades nos han permitido detectar aquellos temas, que por su importancia como materias básicas para la disciplina o por su novedad, requieren de un tratamiento profundo y riguroso, pero también ameno y aplicable, en una colección de libros.

Y aquí estamos, con el primero de los que esperamos sean recursos útiles para todos los lectores que quieran acercarse a este tema con diferentes intereses. En primer lugar, nuestros estudiantes, que siempre agradecen referencias actualizadas y didácticas en las asignaturas y materias que tienen que cursar. En segundo, nuestros socios y colaboradores, profesionales que necesitan comprender mejor el contexto en el que se mueven y profundizar en algo que les condiciona en gran medida en la actualidad, sea cual sea su perfil o sector de actividad. Y en tercero, para cualquier ingeniero, tecnólogo o ciudadano curioso que quiera asomarse a un campo que, por todas sus dimensiones y aristas, afecta a nuestras vidas en muchos más aspectos de los que solemos imaginar.

Esperamos que, para todos ellos, y para alguno más que nos sorprenda, esta colección resulte útil e interesante. Y por qué no, divertida, aprender siempre lo es. Y esperamos que lo hagáis leyendo nuestros libros, aunque sea un poco.

Marta Beltrán
Madrid, Junio 2020.

PREFACIO

Este libro es el que abre la colección de Ciberseguridad. Para nosotros tiene sentido, ya que se centra en la gestión del ciberriesgo, que es una de las principales misiones de un profesional de la ciberseguridad en la actualidad.

En este libro se persiguen los siguientes objetivos:

- Discutir la figura del director de seguridad, su evolución, su contexto y su misión actual en relación con la gestión del ciberriesgo.
- Proporcionar a cualquier persona interesada en esta gestión una visión general acerca de las características del ciberriesgo y de sus componentes, así como de las fases que se deben seguir para gestionarlo y de los estándares, marcos de trabajo o metodologías que puede seguir para llevarlas a cabo.
- Proponer, desde la experiencia, una serie de recomendaciones para las fases más importantes de esta gestión que ayuden a cualquier persona que tenga que llevarlas a cabo a hacerlo con ciertas garantías de éxito.
- Analizar en profundidad las estrategias de mitigación y de transferencia del ciberriesgo.
- Incorporar aspectos de Privacidad, de manera específica, a todo el proceso de gestión.

Para cumplir con estos objetivos este libro se estructura en diez capítulos. El Capítulo 1 analiza el papel de director de seguridad, mientras que el Capítulo 2 realiza una introducción al concepto de ciberriesgo y propone unas fases o etapas

para llevar a cabo su gestión. Una vez comprendida la función del director en la gestión de este tipo de riesgos, el Capítulo 3 realiza un recorrido por los estándares, marcos de trabajo y metodologías que se han utilizado tradicionalmente en la gestión del ciberriesgo en diferentes contextos y a diferentes niveles, y que podrían servir como guía para realizar las fases propuestas en el capítulo 2.

A partir del Capítulo 4, el libro desarrolla las fases más importantes de los procesos de gestión, dedicando este capítulo a la identificación de ciberriesgos. Los capítulos 5 y 6 se centran en el análisis, en concreto el Capítulo 5 discute el análisis del impacto del ciberriesgo mientras que el Capítulo 6 expone todo lo relacionado con el análisis de la probabilidad. El Capítulo 7 discute la cuantificación del ciberriesgo mediante el uso de diferentes herramientas estadísticas.

El Capítulo 8 presenta las estrategias de mitigación del ciberriesgo, fundamentales cuando, una vez cuantificado, se pasa a tratarlo. Por eso el Capítulo 9 complementa a éste proponiendo el uso de estrategias de transferencia y presentando la ciberpóliza de seguros como una tendencia muy importante en la actualidad. Por último, el Capítulo 10 analiza la importancia de tener en cuenta los riesgos para la Privacidad de manera específica, proponiendo herramientas concretas para hacerlo y discutiendo la idoneidad de las mismas.

Aunque un conocimiento en profundidad de aspectos básicos en seguridad corporativa puede ayudar mucho a aprovechar por completo los contenidos incluidos en este libro, nuestro propósito al escribirlo ha sido dirigirnos a una audiencia amplia que comprende a estudiantes, ingenieros, profesionales del sector o directivos. Hemos intentado no dar nada por hecho para que el libro resulte útil como una primera aproximación a la materia a aquellos que no son directores de seguridad o que no esperan serlo en el corto plazo.

Querríamos expresar nuestro agradecimiento a todos los alumnos, compañeros, socios o clientes que nos han acompañado en estos años y de los que hemos aprendido mucho de lo que ha quedado plasmado en estas páginas.

Fernando Sevillano y Marta Beltrán
Madrid, Junio 2020.

1

LA DIRECCIÓN DE SEGURIDAD

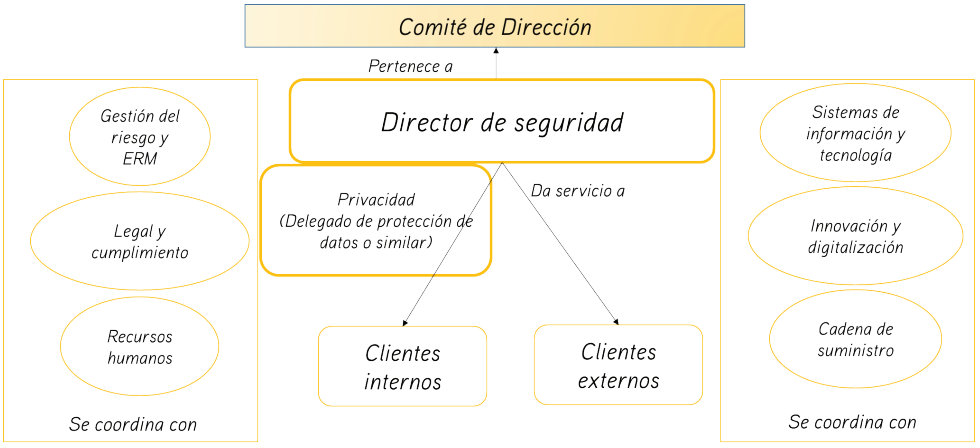
1.1 EL DIRECTOR DE SEGURIDAD Y SU EQUIPO

Hace unos 25 ó 30 años que se comenzó a discutir la figura del director de seguridad con una función similar a la que tiene hoy en día. El denominado efecto 2000 y los atentados de septiembre del 2001 terminaron de convencer a muchos de su importancia. En aquel entonces, se trataba de una figura puramente técnica, que se centraba mucho en la protección de los activos fundamentales, los datos y los sistemas de información que los procesaban, mediante cifrado, protección del perímetro de la red y fortificación o bastionado de servidores. De hecho la figura solía denominarse *Chief Information Officer* (CIO) y en muchos casos dependía orgánicamente, o se relacionaba estrechamente, con la dirección que se encargaba de la gestión de los edificios, oficinas e infraestructuras (y por lo tanto de la seguridad física).

El rol del director de seguridad ha evolucionado mucho en estos años, hasta denominarse casi siempre en la actualidad *Chief Information Security Officer* (CISO) *o Chief Security Officer* (CSO). Su perfil sigue siendo muy técnico, pero se debe complementar con habilidades de comunicación y con una comprensión en profundidad del negocio y de sus objetivos. Además, suele reportar directamente al *Chief Executive Officer* (CEO) o a un consejero delegado y ocupa un puesto muy importante y de liderazgo en la mayor parte de los consejos de dirección (o por lo menos, así debería ser; en algunas organizaciones con gran nivel de madurez es incluso un vicepresidente o VP). En las organizaciones en las que el director de seguridad se encuentra en un escalón inferior del organigrama, su dependencia suele ser del CIO o del CTO (el *Chief Technology Officer*, es decir, el Director Tecnológico) o de una figura equivalente. De todas formas, en esto de las dependencias y los organigramas, cada caso es único.

Procesos, personas y luego, ya sí, tecnología.

El problema con la evolución que ha seguido el rol del CISO hasta la actualidad es que se han ido incrementando sus funciones y su transversalidad, hasta considerarle una (súper)persona capaz de saber de casi cualquier cosa y de tomar decisiones en casi cualquier área, desde los detalles más técnicos de bajo nivel sobre una tecnología concreta, pasando por aspectos de contratación, formación y recursos humanos, legales y de cumplimiento, de innovación o transformación digital o de compras y cadena de suministro, por mencionar sólo algunos ejemplos. Pasando en muchos casos también a su esfera las responsabilidades relativas a la privacidad y a la protección de datos. Vamos a intentar resumir, con el siguiente esquema y en la tabla que tienes a continuación, las funciones de un director de seguridad en la actualidad y su relación con otras funciones, aunque es sólo lo más importante y depende mucho de cada organización.



Esto ha implicado que cueste mucho cubrir estos perfiles, ya que es casi imposible encontrar personas con la formación y con la experiencia necesarias. Y que se hable muy a menudo de la alta rotación que se produce en estos puestos y de profesionales "quemados" que no soportan durante mucho tiempo la presión a la que se ven sometidos o que no se sienten suficientemente reconocidos. Muchos informes recientes estiman que el tiempo de vida de un director de seguridad no suele superar los 2 ó 3 años en la actualidad.

Gestión del riesgo	***Recursos humanos***	***Cumplimiento***
Coordinar los procesos de evaluación y análisis de riesgos.	*Preparar planes de formación y concienciación.*	*Mantener el listado de obligaciones de cumplimiento.*
Proponer estrategias de mitigación y transferencia.	*Gestionar nuevas contrataciones.*	*Coordinar a los departamentos y funciones afectados por estas obligaciones y darles soporte.*
Planificar el despliegue de las mitigaciones y controles. Coordinar Programas y Planes.	*Fomentar la cultura de seguridad mediante políticas y procedimientos de seguridad.*	*Mantener el contacto con autoridades y grupos de interés.*
Tecnología	***Comunicación***	***Respuesta a incidentes y continuidad del negocio***
Diseñar, desplegar, mantener, actualizar, etc. mitigaciones y contramedidas para prevención.	*Redactar y actualizar documentos de seguridad.*	*Coordinar la respuesta a incidentes desde la notificación hasta el posincidente, obteniendo lecciones aprendidas que sirvan para la mejora continua.*
Diseñar, desplegar, mantener, actualizar, etc. mecanismos de detección.	*Realizar comunicación interna, vertical y horizontal.*	*Gestionar acciones legales y recoger evidencias digitales.*
Gestionar presupuesto, adquisiciones, subcontrataciones, cadena de suministro.	*Realizar comunicación externa con terceras partes, socios, proveedores, clientes, etc.*	*Garantizar los niveles comprometidos de continuidad y coordinar la recuperación.*

A todo esto hay que sumarle que en muchas organizaciones se comienza a construir la casa por el tejado, nombrando un director de seguridad pero sin asignarle un equipo ni unos recursos. Es recomendable, en organizaciones pequeñas o medianas o incluso en *startups*, no tener un director de seguridad sino un ingeniero o arquitecto de seguridad. Según vaya creciendo un equipo de seguridad alrededor de este primer profesional que dedique el 100% de su tiempo a la seguridad, se puede plantear tener un director de seguridad virtual, externo, de tipo asesor, a tiempo parcial, etc. Hasta que se pueda consolidar la figura de un director de seguridad a tiempo completo, que debe ser el objetivo. Pero no tiene sentido tenerlo sin asignarle recursos para que pueda hacer su trabajo. Puede ser una maniobra de imagen, pero se descubrirá más tarde o más temprano porque suele crear una falsa sensación de seguridad en la organización (“ya hay alguien que se encarga de esto”) que generará problemas en algún momento.

Y, ¿con qué equipo debería contar un director de seguridad? Es prácticamente imposible proponer una estructura estándar para este equipo, ya que su estructura ideal y los perfiles que lo componen dependen del tamaño de la organización, su sector de actividad, su nivel de madurez, su nivel de tolerancia al riesgo, etc. Pero de nuevo, haciendo un ejercicio de generalización, este equipo (que sea a tiempo parcial o completo, externo o interno, virtual o no; debe existir) debe incluir los siguientes perfiles de manera orientativa:

- Arquitectos de seguridad, con capacidad para comprender las amenazas que corre la organización y para diseñar y construir arquitecturas tecnológicas seguras, decidir cuáles son los controles y contramedidas más adecuados en cada escenario.
- Ingenieros de seguridad, con capacidad para identificar y analizar las vulnerabilidades presentes en la organización y proteger y defender sus activos frente a posibles amenazas desplegando, configurando, etc. los controles y contramedidas más adecuados en cada caso. Es muy importante que alguno de estos miembros del equipo sea capaz de planificar y gestionar proyectos.
- Administradores de seguridad, con capacidad para mantener y operar de manera cotidiana estos controles y contramedidas.
- Analistas de seguridad, con capacidad para producir, revisar y evaluar la información que proviene de distintas fuentes y procesos y convertirla en inteligencia que permita identificar riesgos.
- Desarrolladores e ingenieros del software con capacidad para producir herramientas y software seguro. Este perfil es especialmente importante en el caso de organizaciones que proporcionen o comercialicen sus propios productos o servicios.
- Investigadores, forenses y en general, profesionales con capacidad para detectar incidentes de seguridad y responder adecuadamente cuando se producen.
- Responsables de cumplimiento, auditores y asesores en aspectos legales.
- Responsables de formación y concienciación.
- Responsables de adquisiciones, gestión de proveedores y de la cadena de suministro.

Como comentábamos antes, existen organizaciones sin equipo de seguridad y otras que tienen un equipo de cientos de personas. Si te interesa saber algo más sobre la estructura ideal de este tipo de equipos, los roles y competencias que suelen ser necesarios, etc. existen diferentes documentos, recomendaciones y guías que ayudan a un director de seguridad a configurar su equipo, realizando las contrataciones de los perfiles más adecuados y formando a los que ya están en él para que adquieran las competencias que les faltan.

El NICE (National Initiative for Cybersecurity Education) Cybersecurity Workforce Framework probablemente sea una de las iniciativas más completas y actualizadas en lo que se refiere a las competencias y roles necesarios en un equipo de seguridad.

1.2 SEGURIDAD CORPORATIVA Y SEGURIDAD DE PRODUCTO

Otro de los retos a los que se enfrenta un director de seguridad en la actualidad, siempre desde el punto de vista organizativo y de función, es la confusión que existe en ocasiones entre la seguridad corporativa y la seguridad del producto. Se hace al director de seguridad "propietario" de la seguridad, de toda, sin hacer distinciones. Y se le proporciona un equipo para que se haga cargo de ella.

Idealmente, los clientes del director de seguridad deben ser siempre internos, es decir, sus funciones, si recordamos la lista que acabamos de hacer, se relacionan con la seguridad de la organización, la seguridad interna. Pero en organizaciones en las que se proporciona un producto o servicio a terceros (*Business to Business* o *Business to Client*) a veces se involucra al director de seguridad en incorporar seguridad y privacidad desde el diseño para estos productos y servicios, en la respuesta a incidentes cuando éstos se producen en los clientes, etc. Es decir, se hace que el director de seguridad también tenga que dar servicio a clientes externos.

El director de seguridad no debería tener ninguna responsabilidad en la seguridad de los productos y servicios que se desarrollan o proveen para terceros. Y si la tiene, debe quedar muy clara esta doble función y se le debe dar soporte para que la asuma con garantías.

Por norma general este es un error importante ya que el enfoque y las herramientas que se utilizan para garantizar la seguridad corporativa y la del producto suelen ser muy diferentes. Incluso puede ocurrir que ambas direcciones de seguridad, la corporativa y la de producto, tengan intereses encontrados. Siempre que sea posible, en organizaciones suficientemente grandes y maduras, ambas funciones deben ser independientes.

1.3 MITOS Y LEYENDAS

En los últimos años se repiten ciertos mantras en relación con la dirección de seguridad que probablemente has escuchado o leído en multitud de ocasiones. Como la mayor parte de los estereotipos o lugares comunes, probablemente tengan algo de cierto o de razón, o la tenían cuando surgieron.

Algunas afirmaciones parecen ciertas porque las escuchamos muy a menudo y a personas a las que respetamos. Pero si somos un poco críticos o las evaluamos con cuidado, pueden ser trampas que nos lleven a tomar malas decisiones.

O, como mínimo, a dudar de las nuestras ya que parece que vamos a contracorriente. Analicemos a continuación algunos de estos mitos y leyendas (sólo algunos, porque daría para un libro completo).

1. El CISO debe ser el embajador de la seguridad en el comité de dirección

Esto era cierto en los comienzos de la figura del director de seguridad, en aquella época su principal función era recordar al resto de los miembros del comité de dirección la importancia de la seguridad, y su mera existencia servía como medida de concienciación. El director de seguridad tenía que aprovechar su presencia en el comité, casi siempre, para representar a su equipo frente al resto de directores, evangelizar acerca de su función y conseguir recursos. De ahí la analogía con las figuras diplomáticas. Pero hoy en día todo esto ya no es tan necesario (la mayor parte de las organizaciones están convencidas de la importancia de la seguridad, que suele ser una de las máximas preocupaciones de los CEOs actuales) y la función del CISO es mucho más importante y decisiva.

2. La seguridad es un trabajo de todos

De acuerdo, de nada sirven los controles y contramedidas si no existe una cultura que haga que todos los miembros de la organización se involucren en la gestión del riesgo. Los objetivos del director de seguridad tienen que estar alineados con los del resto de la organización, si no, no podrá hacer su trabajo y el fracaso está garantizado. Pero, cuidado, la responsabilidad última es del director de seguridad y de su equipo, no repartamos culpas cuando las cosas no van bien.

3. Céntrate en lo básico, en lo sencillo, siempre desde el diseño

Los conceptos de *low hanging fruit* y de *shift-left* (y todos los equivalentes) se han extendido mucho en los últimos años y son muy comunes en charlas, conferencias, formaciones y eventos. Es verdad que hay muchas cosas que con poco riesgo, presupuesto y recursos podemos hacer para mejorar la seguridad de la organización, que no tenemos que obsesionarnos con soluciones complejas y sofisticadas y debemos prestar atención a aquellas iniciativas que tienen un retorno mayor y más rápido. Igual que es verdad que incorporar la seguridad y la privacidad desde el diseño, desde las primeras etapas de un proyecto o producto, nos ahorrará muchos costes y disgustos. Pero se han repetido tanto estos mantras que se han llevado a un extremo, y al final, hay tantas cosas básicas, que de nuevo hay que priorizar entre ellas. Y si no priorizamos e intentamos llevar absolutamente todo hacia la izquierda, hacia las fases de diseño, no avanzaremos nunca. La seguridad sigue siendo un tema de equilibrio, de compromiso, y aunque nos centremos en lo sencillo y en incorporarlo cuanto antes, esto no nos ahorra las difíciles decisiones que tienen que ver con priorizar.

4. No hace falta que tengas un equipo de seguridad, externaliza, organiza un bug-bounty

Es verdad que muchas organizaciones no tienen un equipo de seguridad o no lo tienen desde el principio. Y que algunas funciones típicas de este equipo se pueden externalizar (incluso la propia dirección de seguridad). Pero también es verdad que ésta no suele ser una solución ideal o escalable ni con vocación de permanencia. No es lo mismo externalizar la dirección de seguridad, que la detección y respuesta ante incidentes (en un SOC externo, un *Security Operation Center*, por ejemplo). Ciertas funciones y en ciertas organizaciones se pueden dejar en manos de terceros, pero es una decisión que hay que tomar con mucha precaución y con criterio. Y hay que revisarla de vez en cuando porque algo que resultaba eficiente en un determinado escenario puede dejar de serlo si este escenario cambia.

Un claro ejemplo es el de las *bug bounties*, que tan de moda se han puesto en los últimos años. Muchas organizaciones delegan en terceros, a través de este tipo de programas, la búsqueda de vulnerabilidades en sus productos o servicios. Y hacerlo de esta forma, en exclusiva o sin medir bien el alcance del programa de recompensas (qué se busca, cómo se gestionan los informes recibidos, qué capacidad hay para remediar las vulnerabilidades descubiertas, cómo se recompensa a los investigadores que participan, etc.), suele ser un error importante.

5. Confía en tus instintos, es sentido común

El director de seguridad debe ser una persona segura de sí misma y con capacidad para la toma de decisiones. Pero debe saber que todos tendemos a simplificar, sobre todo cuando tenemos que tomar decisiones en situaciones con incertidumbre o ambigüedad, que son típicas cuando se trabaja en seguridad. Y esto hace que nos afecten distintos tipos de sesgos que nos pueden llevar a tomar decisiones equivocadas, en las que la diferencia entre riesgo real y riesgo percibido sea sustancial (o bien porque infravaloramos el real o bien porque lo sobrevaloramos). Es necesario disponer de herramientas que nos permitan tomar decisiones con criterios objetivos y dudar de nuestros instintos para obtener los mejores resultados posibles.

6. Eres un técnico, el aspecto de la documentación o la forma en la que presentas la información no es importante, no trabajas en marketing

Este es un error muy común, puesto que es habitual que en su relación con el resto de la organización el director de seguridad y su equipo tengan que convencer, concienciar, alertar, etc. en temas relativos a la seguridad o involucrarles en la toma de decisiones. Y el resultado de todas estas interacciones dependerá mucho de cómo se transmita y presente la información, hay que ser consciente de ello y utilizarlo en nuestro favor.

7. La solución está en esta nueva tecnología

Ya lo hemos comentado antes, la tecnología es muy importante para un director de seguridad, pero no debe ser lo más importante. El mercado de la ciberseguridad mueve miles de millones de dólares cada año y el marketing puede llegar a ser muy agresivo. Esto provoca cierta ansiedad en los equipos de seguridad, que sienten siempre que van un paso por detrás y que están tardando en incorporar ese nuevo producto o servicio del que todo el mundo habla en el sector. Y por algo será… Pero hay que tener en cuenta el ruido mediático que generan ciertos incidentes, la repercusión de lo que hacen las grandes empresas (que puede funcionarles bien, pero no tiene por qué funcionarnos bien a nosotros), los efectos de

los mensajes que se repiten en las conferencias y charlas de seguridad. La tecnología no suele resolver nuestros problemas. De hecho en ocasiones, una nueva tecnología puede aumentar nuestra superficie de exposición, relajar el comportamiento de las personas de la organización y hacer que se corran más riesgos, generar conflictos con otras tecnologías dentro de una estrategia de defensa en profundidad, etc. Por lo que la decisión de incorporar un nuevo producto de seguridad no puede tomarse a la ligera, de nuevo se trata de saber priorizar. Hay que mantener la cabeza fría ante las presiones del marketing y las modas.

1.4 EL BUEN DIRECTOR DE SEGURIDAD

Si tuviéramos que escribir una carta a los Reyes Magos y pedirle una persona adecuada para asumir funciones de director de seguridad ¿qué le pediríamos? Como ya hemos comentado, no existen las recetas universales, no en todas las organizaciones funciona lo mismo, hay especificidades que no podemos discutir aquí porque agotarían el libro completo. Pero intentando generalizar y teniendo en cuenta lo que hemos discutido sobre esta función hasta el momento, probablemente no nos equivocaríamos mucho pidiendo lo siguiente. Un buen director de seguridad…

Debe ser relevante:

- Es decir, capaz de resolver problemas reales y de demostrar que las iniciativas que pone en marcha tienen un impacto y gestionan el ciberriesgo de manera adecuada.
- Esto implica capacidad para la cuantificación, para demostrar con indicadores de diferente naturaleza que el trabajo realizado es útil y que hoy se está mejor que ayer, que se ha mitigado, evitado o transferido riesgo invirtiendo los recursos disponibles donde era necesario.
- Capaz de asumir responsabilidades y de tomar decisiones, priorizando y defendiendo las prioridades decididas con argumentos sólidos y soportados por evidencias.
- También debe ser capaz de transmitir que es el experto, que se puede contar con él, que es de fiar, que escucha y que es útil. Tiene que procurar no ser siempre el portador de las malas noticias o el que bloquea cualquier iniciativa por sus potenciales impactos en la seguridad, tiene que aportar y construir.

Debe ser realista:

- Capaz de mantenerse al día y actualizado, lo que implica conocer el contexto externo en el que opera la organización, nuevas amenazas y riesgos, nuevos estándares y mejores prácticas, etc.
- Pero también debe manejar bien el contexto interno, tanto desde el punto de vista del negocio (con el que tiene que estar siempre alineado, debe ser un habilitador) y de las operaciones, como del tecnológico.
- Y también debe conocer bien a esos clientes internos de los que hablábamos antes y sus expectativas, limitaciones, etc. así como el nivel de madurez de la organización y las implicaciones que éste tiene en su función.
- Es deseable que sea capaz de detectar quiénes son sus aliados y quiénes van a ser una barrera. Debe ser capaz de distinguir qué peleas merece la pena luchar en cada momento.
- No debe asumir más responsabilidades de las que le corresponden, comprendiendo bien su situación, su función y qué se espera de él o ella.

Debe ser líder:

- Capaz de gestionar un equipo con funciones, perfiles y responsabilidades muy variados.
- Debe poder motivar y guiar a la organización, en los momentos buenos pero sobre todo en los malos.
- Con la habilidad de traducir de lenguaje técnico a lenguaje de negocio y viceversa, ya que en muchos casos será el puente entre los dos mundos. En general, es deseable que sea un buen comunicador a diferentes niveles, alguien didáctico ayuda mucho en esta función.
- En la medida de lo posible, debe poder anticiparse a los riesgos que vendrán y estar preparado.
- Capaz de planificar a corto, medio y largo plazo (de nuevo, priorizar).
- Capaz de trabajar en un contexto en el que existe un adversario, algo que no es habitual en otros puestos de dirección.

Es decir, el director de seguridad ideal es un líder realista, capaz de influir en la organización y de ser resolutivo, orientado a la ingeniería y a la tecnología pero con capacidad de manejar datos para tomar decisiones en relación con el negocio.

1.5 LA GESTIÓN DEL RIESGO

Una vez discutida la función del director de seguridad en la actualidad, nos queda una pregunta esencial por responder en este capítulo ¿por qué un libro que relaciona la dirección de seguridad y la gestión del riesgo? ¿Qué tienen que ver ambos conceptos?

Es verdad que la cuantificación y la gestión del riesgo han adquirido un papel muy relevante para la gestión de las organizaciones en los últimos años. La disciplina del *Enterprise Risk Management* (ERM) permite gestionar una empresa desde el punto de vista del riesgo, intentando identificar y comprender aquellos riesgos, de diferente naturaleza, que pueden impedir que la organización alcance sus objetivos. Obviamente la finalidad es cuantificarlos (normalmente, en términos de probabilidad de ocurrencia e impacto potencial), monitorizarlos y realizar una planificación estratégica que permita gestionarlos.

Esta gestión se puede realizar mediante la aceptación del riesgo, su evitación, su mitigación o su compartición o transferencia a terceros. Teniendo en cuenta que los riesgos que afectan a una organización pueden ser estratégicos, financieros, operativos, de cumplimiento, etc.

Existen diferentes marcos de trabajo, mejores prácticas e incluso regulaciones (sobre todo en el caso de compañías privadas que cotizan en bolsa) que pueden servir como guía para poner en marcha iniciativas de ERM dentro de las organizaciones. Y es importante que el riesgo se vea, no sólo como un factor que amenaza al cumplimiento de los objetivos de la organización, sino como un posible motor para el cambio y la mejora continua, y por lo tanto, como una oportunidad.

En las organizaciones que trabajan así, que cada vez son más, suele existir la figura del *Chief Risk Officer* o CRO, que suele ser el encargado de coordinar todos los procesos y funciones relacionados con los programas de ERM. Pero dada la naturaleza de este cargo y el perfil del CRO, se suele hacer una excepción con el ciberriesgo, que se intenta tratar de la misma manera que los demás, pero dejando la responsabilidad de su gestión al director de seguridad.

Resumiendo en una frase la función de un director de seguridad en la actualidad podría ser "conocer y cuantificar el ciberriesgo para gestionarlo de acuerdo con la tolerancia decidida por la organización".

Es decir las decisiones tomadas por un director de seguridad tienen que ir orientadas, siempre, a gestionar el ciberriesgo (que es el que le compete) para que no sobrepase los umbrales adecuados para la organización en función de su apetito por el riesgo. Un adecuado conocimiento y análisis de los riesgos que se corren permiten siempre a un director de seguridad priorizar los proyectos e iniciativas que su equipo debe acometer y optimizar el uso de los recursos (humanos, económicos) de los que dispone, que no suelen ser ni mucho menos infinitos.

Un buen director de seguridad debe disponer de una metodología y de herramientas que le permitan tomar estas decisiones de manera objetiva, sin dejarse llevar por sesgos motivados por sus experiencias previas, por las modas, etc. Este tipo de decisiones son las que podrá argumentar y defender delante del resto de directores si es necesario. E integrar en la estrategia de gestión del riesgo que la organización siga de manera global, cuando se gestionen otros riesgos no relacionados con la tecnología, lo ciber o digital. El foco del director deber ser siempre la mejora continua, porque al igual que los riesgos cambian y evolucionan, lo deberá hacer la organización para irse adaptando a las nuevas situaciones. Y también la generación de confianza entre los clientes internos y externos, la gestión de esta confianza como un activo más de la organización. De hecho se habla de que el director de seguridad será en breve un CTO, por *Chief Trust Officer*, dado el tipo de función que está adoptando en estos últimos años.

Por este motivo los capítulos que siguen pretenden ser una guía para que aquellas personas interesadas en este enfoque para la dirección de la seguridad sepan cómo proceder y tengan a su alcance un conjunto de técnicas, herramientas y buenas prácticas que les permitan planificar y realizar su labor cotidiana de manera eficiente y eficaz tomando decisiones de calidad.

Para llevar

LA DIRECCIÓN DE SEGURIDAD

1

Cuidado con

- *Confiar exclusivamente en la tecnología*
- *Dejarse llevar por sesgos, mitos, modas y verdades a medias*
- *Quemarse con la responsabilidad*

Tweet

La misión del director de seguridad es conocer y cuantificar el ciberriesgo para gestionarlo de acuerdo con la tolerancia decidida por la organización.

Ideas principales

- *Las responsabilidades del director de seguridad son muchas y muy variadas, debe contar con un equipo adecuado.*
- *Se debe distinguir entre seguridad corporativa (cliente interno) y seguridad del producto (cliente externo).*
- *El buen director de seguridad debe ser un líder relevante y realista,*

Actividades

Priorizar ***Decidir*** ***Resolver*** ***Planificar***