



## ESTRATEGIAS PARA SEGUIR PROGRESANDO EN LA SEGURIDAD T.I.C.

La evolución que en los últimos diez años se ha producido en el ámbito de la seguridad de la información, nos conduce a la conclusión de que ha habido profundos cambios cualitativos y cuantitativos en el mismo. La situación actual nos permite constatar la importancia que la misma ha adquirido para todas las entidades, públicas o privadas.

En este periodo la progresión ha sido muy importante y podemos identificar múltiples y variadas causas que han incidido significativamente en el desarrollo que ha acaecido. La seguridad está de moda, con toda la carga de sentimientos positivos y peyorativos que el propio término pueda suscitarlos.

En el bloque de los elementos que crean problemas o nos complican la seguridad podemos considerar la nueva forma de hacer negocios por las facilidades que la tecnología nos proporciona, especialmente en lo relativo a las posibilidades de conectividad 'Martini' (dónde, cuándo y cómo quieras).

Sin hacer demasiados equilibrios taxonómicos, estableceremos dos grandes bloques de 'cosas' que afectan al contexto que estamos considerando.

En el bloque de lo que llamaríamos elementos dinamizadores podemos considerar la aparición de requerimientos legales o reguladores como la LOPD y SOX entre otros, los propios avances tecnológicos, el impulso en los negocios a basar su gestión por procesos, no siendo ajenas las organizaciones de T.I. a las buenas prácticas preconizadas por ITIL, ISO 20000 y de forma específica en seguridad ISO27001 o el modelo CobiT.

En el bloque de los elementos que crean problemas o nos complican la seguridad podemos considerar la nueva forma de hacer negocios por las facilidades que la tecnología nos proporciona, especialmente en lo relativo a las posibilidades de conectividad 'Martini' (dónde, cuándo y cómo quieras) potenciando la movilidad, las tendencias a externalizar ciertas actividades y a incorporar a terceros en los flujos de los negocios de nuestras empresas u organizaciones y, por supuesto, el hecho de que los 'malos' han permutado el objetivo de la satisfacción personal por el objetivo de ganar dinero.

En dicho contexto, selecciono dos áreas que preocupan de forma especial a quienes estamos vinculados a la seguridad de la información al objeto de establecer algunas reflexiones y consideraciones sobre las mismas -más bien son

pensamientos en voz alta-, que nos sirvan de contraste sobre la situación en nuestras corporaciones y que si procediese, nos permitan pasar de preocuparnos a ocuparnos y reconducir nuestras estrategias.

### Las expectativas de Seguridad y sus relaciones con la Dirección y con los Negocios

Los 'Competidores internos', por su novedad, son uno de los últimos motivos de preocupación. Organizaciones de solera como los Servicios Jurídicos, algo más recientes los auditores internos, y los más noveles,

como Riesgos Corporativos, entre otros, están reclamando funciones que podríamos pensar son exclusivas de Seguridad. Los debates son y serán interesantes pues la tarta es apetitosa y 'estar de moda' la hace más atractiva.

La incorporación de los aspectos legales y reguladores complementando los puramente técnicos, y la nueva dimensión de los análisis de riesgos más amplios que los tradicionales tecnológicos, hacen que nos preguntemos si es más fácil que un abogado o un conocedor profundo de las funciones del Negocio

Los 'Competidores internos', por su novedad, son uno de los últimos motivos de preocupación. Organizaciones de solera como los Servicios Jurídicos, algo más recientes los auditores internos, y los más noveles, como Riesgos Corporativos, entre otros, están reclamando funciones que podríamos pensar son exclusivas de Seguridad. Los debates son y serán interesantes pues la tarta es apetitosa y 'estar de moda' la hace más atractiva.

aprendan el método de análisis de riesgos y conceptos de seguridad, o que un técnico de seguridad aprenda a interpretar leyes o conozca profundamente los negocios.

Evidentemente, las empresas de una cierta dimensión, deberán tratar el tema si todavía no lo han hecho.

Con matices distintos, pero la situación se parece a la iniciada en la década de los 80

cuando la irrupción de los PC's propició el nacimiento de la informática departamental pero que en la perversión de sus bondades derivó en algunos casos a reinos de taifas, convirtiéndola en desparramada en vez de distribuida. Nos puede servir de base el análisis de su evolución para evitar que se genere confusión y se repitan errores.

### El apoyo de la Dirección

Otro asunto, en este caso antiguo, es el apoyo de la Dirección. El primer estadio es conseguir que se dediquen recursos, personas y dinero, a la seguridad de forma recurrente. El segundo estadio consiste en que se determinen las funciones a desempeñar, se reconozca la autoridad y que se transmita al resto de la organización con la instrucción de que se colabore en las actividades y proyectos que se desarrollen. El primero es frecuente que se dé, pero en el segundo no es tan habitual que se produzca la investidura de autoridad y se comunique.

Es esencial tener muy clara la *visión* -y la *misión*- que la Dirección tiene de nosotros, no la que pensamos que tenemos, pues desajustes en las percepciones generan distorsiones importantes. Que se nos dote de cierto presupuesto no debe hacernos inferir que se nos considera una actividad que forma parte del 'core' del negocio. No todos estamos en negocios de banca por Internet por poner un ejemplo de tipo de negocio en el que la seguridad es consustancial con el mismo. Tener bien calibradas las expectativas de nuestra función facilitará la estrategia que

deberemos desarrollar.

El modelo de gobierno de la función y la cooperación de los Negocios en nuestras actividades es el tercer factor clave. Cómo les involucramos en nuestros temas y cómo conseguimos que nos dediquen tiempo, es el objetivo que se persigue, pero la presión de la eficiencia afecta a todas las organizaciones y nadie anda sobrado del recurso personas/

tiempo. Se deben diseñar estrategias realistas evitando planteamientos voluntaristas que nos hagan inoperativos los comités y grupos de trabajo que se crean y a la tercera reunión languidezcan. Es fundamental hablar en el lenguaje de los Negocios, huir del técnico; es un aprendizaje que debemos realizar para que nos entiendan, comprendan y apoyen.

### La gestión operativa y técnica de la seguridad

Plantearse la gestión de la seguridad mediante un proceso es estratégico. El modelo de procesos a aplicar es tal vez lo menos importante, lo fundamental es tener uno y ser coherente con el mismo, con sus puntos fuertes y débiles. Uno de los criterios para seleccionarlo debería ser que estuviese alineado con el posicionamiento corporativo respecto de dicho modelo si lo hubiera o si estuviese previsto establecerlo.

Diseñar, implantar o incrementar el nivel de madurez del mismo debe ser nuestro foco de atención dependiendo de la situación en que nos encontremos. El proceso de Gestionar Seguridad tiene múltiples interfaces con los procesos de T.I. y de los negocios, y su despliegue total requiere tiempo.

### La gestión operativa del proceso

La gestión operativa del proceso es otra de las preocupaciones. A fecha de hoy no existen herramientas que permitan gestionar todas las actividades del proceso

Cuando la magnitud de la inversión y gasto en una parcela empieza a ser relevante, es la primera derivada y nos preocupamos de los costes. Debemos medir y, aunque no es simple, no tenemos otra alternativa, y eso nos inquieta, pues nos exigen rentabilidades. No obstante, superado el esfuerzo inicial de empezar a realizarlo, los beneficios y argumentos que nos proporcionará son indudables.

y subprocesos de forma integrada. Hay soluciones parciales que cubren más o menos ciertos subprocesos.

Una preocupación adicional es el hecho de que no todos los eventos e informaciones a tratar en el proceso son automatizables pero, sin embargo, no se pueden obviar. Hay que ser consecuentes con la realidad: muchos de los 'controles' o 'mecanismos' que implantamos no son activos 'per se', exigen la actitud de una persona para que operen y en esos casos no hay sonda que

monitoree; como mucho, se detectarán a posteriori los posibles incidentes.

Los cuadros de mando y sistemas de indicadores están en la cresta de la ola.

### Los costes de la seguridad y de la inseguridad

Mención especial merece lo alusivo a los costes de la seguridad y de la inseguridad. Cuando la magnitud de la inversión y gasto en una parcela empieza a ser relevante, es la primera derivada y nos preocupamos de

La incorporación de los aspectos legales y reguladores complementando los puramente técnicos, y la nueva dimensión de los análisis de riesgos más amplios que los tradicionales tecnológicos, hacen que nos preguntemos si es más fácil que un abogado o un conocedor profundo de las funciones del Negocio aprendan el método de análisis de riesgos y conceptos de seguridad, o que un técnico de seguridad aprenda a interpretar leyes o conozca profundamente los negocios.

los costes. Debemos medir y, aunque no es simple, no tenemos otra alternativa, y eso nos inquieta, pues nos exigen rentabilidades. No obstante, superado el esfuerzo inicial de empezar a realizarlo, los beneficios y argumentos que nos proporcionará son indudables.

El enfoque que debemos dar al tema SGSI en cuanto al alcance, certificarse o no, proyectos parciales o totales, etc., son as-

### Herramientas de gestión técnica

Por último y en el ámbito de las herramientas de gestión técnica, la experiencia de los proyectos de implantación de determinados tipos de productos, abordados en los últimos años, nos hacen ser cautos. Cuando el proyecto entra en el campo de la gestión de la seguridad, hemos aprendido que para que sean útiles no es suficiente tenerlos instalados, además requieren personas que actúen en función de las informaciones que proporcionan y, a veces, no se dispone de

esas personas.

Otra dificultad es la interoperabilidad entre las distintas soluciones que a lo largo del tiempo podemos haber decidido implantar. Las últimas tendencias relativas a productos del tipo S.I.M. o U.T.M. están en esa línea. El concepto de madurez debemos aplicarlo no sólo a los productos, también nuestras organizaciones deben estarlo para que sean rentables a las empresas.

### Conclusión

Aprovechemos el buen momento de la seguridad de la información, la tecnología es condición necesaria pero no suficiente, dediquemos tiempo a los aspectos organizativos y de relación con los otros agentes que interactúan con nosotros, profesionalicemos nuestra gestión basándonos en las 'buenas prácticas' y evitemos los experimentos tecnológicos si no son imprescindibles.

La magnitud de nuestro gasto e inversión nos hace ser observados y evaluados por nuestros 'mayores'. ■



Manuel Palau Rolduá  
Jefe de la Unidad de  
Políticas y Normativa  
Dirección de Sistemas  
IBERDROLA