¿QUÉ PREOCUPA?

LA SEGURIDAD GLOBAL Y LOS MUNDOS DE LA SEGURIDAD: SEGURIDAD FÍSICA, SEGURIDAD DE LA INFORMACIÓN, SEGURIDAD TI, AUDITORÍA Y CONTROL DE SEGURIDAD

Mis queridos colegas, algunos llevamos prácticamente 20 años en el mundo IT y unos 15 al menos encargados de esa "bicha" denominada **seguridad**, entre otros quehaceres cotidianos, sin tiempo alguno de aburrirnos. Para hablar del animal en cuestión ("seguridad"), lo propio es mencionar algunas de sus principales características y explicar qué solemos entender por ella.

En mi humilde opinión la seguridad es algo intrínseco a tres factores: el primero y más importante son las **personas**, el segundo, el **medio**, y el tercero las **relaciones** de todo tipo que estas personas establecen con dicho medio, entendiendo por medio todo aquello que sirve para el desarrollo de nuestra vida y día a día, en todas y cada una de sus facetas.

Hasta la época reciente, la seguridad se ha visto de manera aislada y sesgada en la mayoría de las organizaciones y, por supuesto, sólo de refilón y a nivel personal, dado que no era una materia que se enseñara, sino que las personas aprendimos en función de nuestra evolución, entorno, principios y circunstancias.

Dado que nuestro mundo, denominado "Tierra", ha evolucionado y cambiado sus fronteras geográficas, políticas, étnicas, culturales, económicas, en un proceso sin fin denominado globalización, se hace necesario pensar que el resto de materias debe evolucionar de manera inminente para poder adecuarse a los nuevos escenarios que nuestras sociedades plantean, y, sobre todo, a los problemas que la evolución de la tecnología y de la gestión de la información implican.

Es por ello que materias como las leyes, regulaciones, marcos económicos, culturas y, en general, formas de hacer –y en especial nuestra entrañable y no poco compleja seguridad–, deben sufrir un profundo cambio y alinearse en su planteamiento y su gestión no sólo con estas demandas actuales, sino también con las que ya debemos estar previendo a corto, medio y largo plazo.

Con tan arduo objetivo y con un nivel muy alto de diversidad de materias de seguridad en nuestra misión, y diversidad de opiniones y formas de gestionarlas, la única solución posible que se puede aplicar es conseguir aunar la gestión de todas y cada una de estas materias bajo un mismo prisma y con una misma filosofía, de tal manera que podamos avanzar con premisas alineadas, coherentes y, sobre todo, coordinadas en la multitud de temas que nos ocupan; en resumen, que "globalicemos nuestra gestión para atender los problemas y las necesidades de la globalización de nuestra vida."

Con tan arduo objetivo y con un nivel muy alto de diversidad de materias de seguridad en nuestra misión –y diversidad de opiniones y formas de gestionarlas–, la única solución posible que se puede aplicar es conseguir aunar la gestión de todas y cada una de estas materias bajo un mismo prisma y con una misma filosofía.

Visión de integración de los mundos de la Seguridad

Aunque son de sobra conocidos y parecen distintos, los problemas de cada uno de los mundos, en sí no lo son en esencia y cada día menos. Por ejemplo, la seguridad física tradicional cada vez utiliza más sistemas basados en tecnología y comunicaciones para llevar a cabo su labor, sistemas cada vez más automatizados y muy similares en su diseño y explotación a cualquier aplicación de monitorización de sistemas de IT. ¿Qué diferencia hay entre una aplicación de gestión de alarmas físicas y video vigilancia con un sistema de gestión de alarmas y monitorización de sistemas hardware o software?

En ambos casos un operador, una vez está definido el sistema y en fase de explotación del mismo, actuará de igual manera y responderá conforme al protocolo acordado en cada caso en que salte una alarma. Quizás el problema que veo, y que debemos empezar a resolver -además de la rotación del sector- es la formación y especialización de los vigilantes y auxiliares para convertirlos en técnicos de vigilancia y control.

Por qué no, entonces, pensar en poder gestionar de manera conjunta y por qué no llegar a poder integrar y correlar este tipo de sistemas, con el fin de disponer de una trazabilidad total (objetivo deseado por cualquier auditor) desde que alguien o algo entra por la puerta física (sistema de control de accesos a edificios) o lógica de una corporación (sistemas de control de accesos de aplicación), qué hace dentro (*log's*), a qué accede (recursos), qué se lleva y cómo (información) y cuándo sale y en especial, qué evidencia suficientemente probatoria deja de todo ello para poder reconstruir lo que ha hecho y poder presentar pruebas con cobertura legal en caso de necesidad (cubriendo el no repudio); incluso poder almacenar información que nos proporcione patrones de comportamiento, tanto de las personas como de los sistemas y equipos que intervienen en todo el proceso.

En fin, ¿no aplicamos o buscamos de alguna manera esto en nuestro negocio con aplicaciones como un CRM o un Datawarehouse para nuestros clientes? ¿No hablamos en todos y cada uno de los foros a los que asistimos de alinear la seguridad con el negocio y gestionar los riesgos y, por ende, la propia seguridad, e incluso certificarnos en esta materia?

¿Qué diferencia hay entre una aplicación de gestión de alarmas físicas y video vigilancia con un sistema de gestión de alarmas y monitorización de sistemas hardware o software?

Al igual que pensé en su momento que no hay diferencia de fondo en la gestión de los sistemas *mainframe*, intermedios o micro, y que se pueden gestionar de igual manera, y que cada vez distinguimos menos quién es quién porque unos crecen y otros se abren a soporte al resto, tampoco pienso que exista gran diferencia en la gestión de la seguridad física, de IT o de la información.

¿Cómo lo pretendemos hacer sin tener una visión global de todos y cada uno de los aspectos o materias de seguridad (física, lógica, información, control, fraude, etc.)?

Los "malos", –nuestro enemigo– están ahí, disponen de más medios y más tiempo y tienen acceso a todo; cosa que no siempre sucede en nuestro caso.

Disculpad mi entusiasmo con este tema pero es un objetivo personal que hace tiempo me marqué y por el que aposté en mi compañía, y que otros ya hicieron incluso antes aunque quizás aún era pronto; ahora, el cambio de siglo ha dado un giro que lo hace más realizable.

Los problemas son varios, pero al igual que pensé en su momento que no hay diferencia de fondo en la gestión de los sistemas *mainframe*, intermedios o micro, y que se pueden gestionar de igual manera, y que cada vez distinguimos menos quién es quién porque unos crecen y otros se abren a soportar al resto, tampoco pienso que exista gran diferencia en la gestión de la seguridad física, de IT o de la información y, mucho menos, desde el punto de vista de auditor o de las regulaciones, metodologías o normativas que abarcan todas las áreas.

Perfil del Gestor de la Seguridad Global y posicionamiento

Ahora bien, para lograr este objetivo la persona o personas a las que en cada una de vuestras organizaciones se les encomiende esta labor deben estar respaldadas, sin duda, por la Dirección, deben tener una formación multidisciplinar y continua en todas y cada una de las materias para poder entender las problemáticas, y deben de tener una piel especial en cuanto a su identificación con los principios de seguridad. Es necesario que mantengan contactos con otros actores y asistan a foros.

En cuanto a su posicionamiento en la compañía deben ser independientes del resto de áreas pero con una capacidad de coordinación y comunicación con todas ellas, además de disponer de un Comité donde se presenten los planteamientos y se tomen las decisiones, siempre en base a información elaborada y no en base a supuestos.

Además deben ser capaces de marcar un Plan Estratégico referente a la Gestión de Seguridad y convencer del mismo, sin perder de vista los ratios de eficacia y eficiencia en la aplicación y consecución del mismo.

El problema que veo, y que debemos empezar a resolver –además del de la rotación del sector– es la formación y especialización de los vigilantes y auxiliares para convertirlos en técnicos de vigilancia y control.

Preocupaciones del Gestor

Para finalizar, creo oportuno reseñar –en este caso como profesional del mundo de la Seguridad y Auditoría– las principales preocupaciones que un buen responsable de seguridad debiera tener en su plan de acción. Son las siguientes:

- Plan de concienciación y creación de cultura de seguridad en empleados, proveedores y clientes, en definitiva, en todas y cada una de las personas; plan de detección y gestión de vulnerabilidades de los equipos, sistemas, procedimientos operativos, sistemas de monitorización, etc.
- Plan de seguimiento y medidas para evitar el fraude organizado y suplantación de identidad física y digital
- Plan de clasificación de la información, y, en general, de todos los activos de la compañía.
- Plan de selección, funciones y competencias de los perfiles de las personas alineado con RRHH; definición de funciones, objetivos, proyectos y tareas de cada una de las áreas de seguridad.
- Plan de trazabilidad de registros y registros de calidad, con garantía de evidencia probatoria de todos los accesos.
- Plan de continuidad de negocio con sus planes de emergencia y recuperación; plan de gestión de riesgos y alineamiento con el ciclo de vida de los procesos de negocio, cuadros de mando y herramientas de gestión.
- Plan de integración de funciones de seguridad.
- Plan de formación y comunicación con todos los actores, y certificación de sus procesos de gestión de la seguridad, concibiendo ésta de una manera integrada e integral.

Muchas gracias a todos mis colegas de profesión porque sin vosotros y vuestro trabajo de día a día nuestro reto no sería posible. ■

Pedro Pablo López Bernal
Gerente de Infraestructura de Seguridad y Auditoría
RURAL SERVICIOS INFORMÁTICOS, S.C.