



## ... LA FORMACIÓN, CONCIENCIACIÓN Y SENSIBILIZACIÓN EN SEGURIDAD

Cuando esta revista se puso en contacto conmigo proponiéndome una colaboración en esta sección, me sentí muy halagado, y me planteé realizarla tratando de no entrar en ningún tipo de tecnicismo, para eso ya están otras secciones, me dije a mí mismo.

Tras unos días pensando en el encabezamiento de la misma "¿Qué preocupa?", y en sus correlaciones ¿a quién preocupa? y ¿en qué materia?, la respuesta a la última me pareció evidente: en el seno de SIC debía ser: ...¿seguridad en informática y comunicaciones?, ¿seguridad de la información?, ¿seguridad de los sistemas de información?... Bueno, mal empezamos, no se puede empezar divagando acerca del ámbito en el que nos movemos, no obstante, precisar el mismo ayudaría a que la respuesta a las otras dos preguntas se ajustase más a lo que se espera que sea el contenido de esta colaboración; demos entonces por buena la pregunta ¿en qué materia? La primera de las respuestas: "Seguridad en informática y comunicaciones", esperando el momento oportuno en que se pueda promover el debate que todos tenemos en mente respecto del "ámbito de actuación", sin herir susceptibilidades ni levantar ampollas.

### La sensibilización debe propiciar en los usuarios reacciones reflejas de protección y de convencimiento en la necesidad de adoptar medidas de seguridad.

Decidí entonces tratar de buscar la respuesta a la segunda de las preguntas iniciales, ¿a quién preocupa?, para luego poder contestar a la primera.

¿Qué me preocupa a mí? Soy demasiado nuevo en la plaza como para que pueda ser relevante mi opinión acerca de cualquiera de los temas que giran entorno de la "seguridad en informática y comunicaciones". Empezamos de nuevo:

¿Qué preocupa al: ¿Responsable de seguridad?, ¿Responsable de seguridad de la información?, ¿Director de seguridad de la información?, ¿Director de seguridad informática? Vaya por Dios, seguimos sin tener las cosas muy claras, esos son los cargos de mis predecesores en esta sección, no vayamos a abrir un segundo debate acerca de la "organización", y busquemos una respuesta rápida y de compromiso; a fin de cuentas, a la mayoría de nosotros nos preocupan unos u otros temas en función del puesto de trabajo que ocupamos en la organización de nuestras respectivas empresas y de nuestra propia responsabilidad (ámbito de actuación), aceptemos pues como respuesta a la pregunta ¿a quién preocupa?: "a las empresas".

Llegados a este punto solo queda dar respuesta a la pregunta inicial ¿Qué preocupa? o precisando

do el alcance pactado de la misma, ¿qué preocupa a las empresas en materia de Seguridad en informática y comunicaciones?

#### Las personas, el eslabón más débil

En el poco tiempo que llevo inmerso en estos temas, he podido comprobar a través de las reuniones con compañeros de mi entidad, a través de sesiones de trabajo con responsables de otras entidades, "desayunos de seguridad", seminarios, congresos y revistas especializadas, que hay un tema que está en boca de todo el mundo y que es uno de los objetos de reconocida preocupación por parte de la mayoría de las empresas, el 66% de las mismas según las últimas encuestas: me refiero al de "las personas", su formación, concienciación y sensibilización en materia de seguridad de la información.

No por manido pierde su vigencia el aforismo "La cadena es tan fuerte como el más débil de sus eslabones", y cuando preguntamos en materia de seguridad de la información a los directivos de las empresas, todos en mayor o menor grado consideran que su eslabón más débil son las personas. No se trata de entrar en una discusión

acerca de lo cierta o no que pueda ser dicha afirmación, la realidad es que esa es la preocupación que manifiestan.

No hemos de perder de vista las otras dos patas del trípode en el que se sustenta cualquier modelo de seguridad de la información: la tecnología y los procedimientos, pero tanto la una como los otros están íntimamente relacionados y ligados en su eficacia, y eficiencia a ese tercer y fundamental soporte para el modelo que son las personas.

El primer paso, "formación", abarca todos y cada uno de los aspectos de la seguridad de los sistemas de información, desde el pilar fundamental: definición y comunicación de la política de seguridad, pasando por el establecimiento de programas de formación generales y específicos en esta materia; no debemos caer en el error de pensar que solo los responsables de los sistemas de información necesitan formación continua en materia de seguridad, es evidente que su especialización si requerirá que esta sea continua y específica, pero todos los usuarios necesitan la formación necesaria para poder evitar, prevenir, detectar y comunicar en su caso cualquier incidencia de seguridad. Esta formación debería ser proporcionada en el momento de su incorporación a la empresa, manteniéndose unos ciclos

formativos permanentes que permitan el reciclaje continuado de los mismos. Los métodos: cursos, reuniones de trabajo, charlas, *e-learning*, etc. son múltiples y la eficacia de los mismos depende en gran parte del segundo eslabón: la "concienciación".

Según el Diccionario de la Lengua Española de la R.A.E. concienciar es hacer que alguien sea consciente de algo, y consciente: que siente, piensa, quiere y obra con conocimiento de lo que hace. Estoy seguro de que todos los que nos dedicamos a la seguridad nos conformaríamos con que las personas que trabajan sobre nuestros sistemas de información, conociesen las implicaciones que conlleva esa concienciación en materia de seguridad, y conseguir que sea efectiva no tiene por qué ser una utopía, sino un trabajo nuestro de cada día.

Partiendo de que el concepto de seguridad ya esté asumido en las empresas, el siguiente nivel sería conseguir esa toma de conciencia por parte de todo el personal de la misma. No es una labor a la que nos debemos dedicar a tiempo parcial, sino que como algún compañero me comentó en cierta ocasión, se trata de "evangelizar" día a día, a través de nuestro hacer y el de nuestros colaboradores, resolviendo las dudas que puedan plantearnos los usuarios con ánimo de colaboración, utilizando "expresiones amigas" en nuestras relaciones (¿cuántas veces hemos agradecido esa información transmitida tras la famosa "esto solo es culturilla pero escucha ..."? y conseguir que todo usuario valore la información que tiene la empresa, las implicaciones de la pérdida de confidencialidad, integridad o disponibilidad de la misma y promover su autoformación.

Por último, bien merece citar a la "sensibilización"; ésta debe tener entre otros objetivos propiciar en los usuarios reacciones reflejas de protección, el convencimiento de la necesidad de adoptar medidas de seguridad, incluso cuando éstas pueden significar un pequeño obstáculo en el quehacer diario.

Hay que reforzar el valor de las personas en la dinámica de la empresa, y que cuando se fijen los deberes y obligaciones de las mismas, se haga tratando de conseguir que renueven la confianza en sí mismas, en sus propios recursos, y trabajen en su propio progreso y en el de la entidad. Querer mejorar, aprender, permanecer atentos, abiertos a otras maneras de hacer, ser y entender, mostrarse receptivos a la innovación; en resumen, no se trata solamente de aplicar seguridad, sino de implicarse en esta tarea día a día. ■



>Fernando Víctor Ferrá Homar  
Responsable de Seguridad Informática  
BANCA MARCH