



## SABER CONVENCER A LA EMPRESA

“La seguridad es una tarea de todos”. ¡Qué bien suena y qué complicado es conseguirlo! Los códigos de buenas prácticas y normas relacionadas con la seguridad de la información dan indicaciones sobre qué es lo que hay que hacer y cómo con las distintas tecnologías y elementos de gestión, pero en ningún sitio dice cómo hacer ver a los empleados y a los directivos que “todos” también les incluye a ellos. No me preocupan tanto los de fuera, como no ser capaz de convencer a la totalidad de los integrantes de la empresa.

### Las preocupaciones

Existe una parte de la seguridad de la información que se puede abordar de manera más o menos rápida y sencilla; depende fundamentalmente del presupuesto disponible para proyectos relacionados con seguridad. Todo lo relacionado con la seguridad de redes y sistemas (digamos seguridad “informática”) se puede englobar en el marco de proyectos y herramientas más o menos evolucionadas (autenticación, código malicioso,

al enviar información por correo-e, etc.

En la Dirección de Seguridad debemos ser capaces de entender esto y buscar soluciones creativas que permitan mejorar sustancialmente la seguridad, pero sin interferir en los objetivos, aunque haya que ir cambiando los hábitos en el día a día.

En este sentido, nos preocupa más tener recursos disponibles para eliminar las vulnerabilidades de los sistemas de información, que disponer de una herramienta que las analice diariamente. Nos preocupa más que los empleados (incluidos los directores) entiendan la importancia de notificar los incidentes de seguridad que disponer de una herramienta de gestión de incidencias de empleados. Nos importa más llegar a un acuerdo con el Departamento Comercial para encontrar un equilibrio entre aumentar la seguridad de los servicios y las quejas de los clientes que llegan al Departamento de Atención al Cliente porque “antes era más fácil usar sus servicios”, porque eso hace que el Departamento Comercial tenga más difícil llegar a su cifra de ventas.

Lo primero que debe plasmar el comité es la política de seguridad de la compañía, que debe entenderse como las reglas básicas. La política tiene que ser útil y dar indicaciones válidas en un lenguaje cercano que sirvan de pauta ante las situaciones en las que se encuentra el personal de la empresa en el desarrollo de su trabajo en el día a día. Si la política es “políticamente correcta” y cumple perfectamente con los requerimientos de todas las normas y leyes posibles, pero los empleados no la entienden, ni saben qué quiere decir, ni identifican lo que dice la política con su trabajo diario, ni entienden qué es lo que tienen que hacer y cuándo, no funcionará bien.

Pero aquí no acaba el trabajo, no basta con dejarla en la intranet, hay que lograr, como sea, que se entienda y se aplique, y para eso no hay recetas mágicas. Aquí la exoneración de responsabilidades no sirve de mucho, lo que se pretende no es cubrir el expediente o darle cumplimiento a una determinada normativa, lo que buscamos es que los empleados entiendan la importancia de su papel en la seguridad de la compañía y qué es exactamente lo que esperamos de ellos, cómo pueden ayudar.

Lograr que el personal asuma que la seguridad no es un asunto que le corresponde resolver a Informática o Sistemas es pura obsesión. Sólo con esta actitud, los propios empleados llegan a darse cuenta de la conveniencia de cambiar algunos hábitos por otros nuevos, y son ellos los que proponen alternativas para mejorar la situación.

Sólo con esta actitud, los propios empleados llegan a darse cuenta de la conveniencia de cambiar algunos hábitos por otros nuevos, más seguros, y son ellos los que proponen alternativas para mejorar la situación.

Seguridad tiene que estar tan presente en la vida de la compañía como Sistemas, Financiero o Recursos Humanos. Todas las semanas tienen que recibir algo, aunque sea poca cosa, que les recuerde que existe un Departamento de Seguridad y que ellos también tienen un papel protagonista. ■

Lograr que el personal asuma que la seguridad no es un asunto que le corresponde resolver a Informática o Sistemas es pura obsesión. Sólo con esta actitud, los propios empleados llegan a darse cuenta de la conveniencia de cambiar algunos hábitos por otros nuevos, y son ellos los que proponen alternativas para mejorar la situación.

IDS / IPS, análisis de vulnerabilidades, gestión de identidades, SIM/SEM, etc.). Cuando cambiamos el enfoque de “informática” a “información”, la situación empieza a complicarse.

Conseguir que el resto de direcciones de la empresa vea la seguridad como un requisito de negocio más, como una ayuda y no como un freno, sólo se consigue siendo tremendamente empático. Es decir, entendiendo las necesidades de los distintos departamentos para cumplir con sus objetivos y desarrollar unos controles de seguridad compatibles con esas necesidades del negocio.

Ya es bastante complicado llegar a los objetivos de ventas, tener listas las versiones de software en los plazos a los que la empresa se ha comprometido, atender las solicitudes de los clientes en el plazo previsto, como para decir que todo el personal tiene que pasar por charlas formativas, rellenar nuevos formularios de notificación de incidencias, dejar de compartir su contraseña con otros compañeros, tener cuidado

### Los consejos

En Arsys Internet, se ha intentado dar la vuelta a esta situación de arriba hacia abajo y no pelear por lo que no merece la pena. Con esta premisa, se tiene que ir filtrando la seguridad desde arriba hacia abajo, empezando por los directores. Para eso, se ha constituido un Comité de Seguridad formado por los directores de los departamentos que pueden tener algo que decir en materia de seguridad de la información; no sólo integrado por las áreas técnicas, sino también por las de negocio. Los Directores Generales de las tres áreas apoyaron en su momento la creación del Comité, dándole el respaldo corporativo.

En ocasiones, es necesario negociar para lograr que una iniciativa de seguridad salga adelante con el consenso del comité. Es mejor tener una política de control de accesos regular que ninguna política de control de accesos o una rigurosa, pero que la mitad de la empresa no aplica.



Olof Sandstrom  
Director de Seguridad

ARSYS INTERNET