



¿QUÉ
PREOCUPA?

LA TECNOLOGÍA Y LAS PERSONAS, EN SU SITIO

Han pasado ya 26 años desde el día en que, fruto de la visión de futuro de mi padre, asistí a mi primera clase de informática. De aquel día, todavía recuerdo una frase que debería haber sido grabada en mármol para que con el paso de las décadas la gente confirmase cuanta razón tenía quién la dijo: 'Los ordenadores son máquinas tontas'. Somos nosotros, las personas, quienes les indicamos lo que tienen que hacer. De nosotros depende su funcionamiento y eficacia. Una orden incorrecta, un mal planteamiento o un mal uso llevan a un error o, peor aún, a resultados impredecibles. Lamentablemente, este principio, tan obvio entre los profesionales del sector, parece no haber calado lo suficiente en el resto de los mortales a pesar de que, poco a poco y sin darse cuenta, todos ellos han ido integrando las nuevas tecnologías en sus vidas.

La tecnología es tan eficaz y fiable como las personas que la utilizan. Esta omisión generalizada se está convirtiendo en el motivo más frecuente de incidencias de seguridad de la información y lo que es peor, son las de mayor impacto en la economía y reputación de las empresas.

En los últimos años los empresarios, al igual que todo el mundo, conocedores del incremento de riesgo que supone tener presencia en Internet y guiados por la interminable publicación de incidentes de seguridad sufridos, en el mejor de los casos, por el prójimo, han iniciado una carrera por la adquisición e implementación de todo tipo de soluciones tecnológicas de seguridad, cada vez más sofisticadas. El resultado es que se invierten millones de euros en desplegar SGSIs parciales a golpe de sistemas de gestión de identidades, plataformas de control de acceso, sistemas de correlación de eventos, criptografía digital, etc.

Ciertamente, toda esta carrera por mejorar la seguridad a golpe de tecnología es justificada a la par que loable pero se está ignorando aquel principio básico con el que me bautizaron: **La tecnología es tan eficaz y fiable como las personas que la utilizan.** Esta omisión generalizada se está convirtiendo en el motivo más frecuente de incidencias de seguridad y lo que es peor, son las de mayor impacto en la economía y reputación de las empresas.

¿Quién de nosotros, durante el trayecto del puente aéreo, aburrido tras la lectura de la prensa, no ha girado alguna vez la cabeza para interesarse por el estado de cuentas, los balances o la redacción de un plan estratégico de la pantalla del portátil de nuestro vecino de asiento? O ¿quién no se ha reído alguna vez al oír involuntariamente una conversación entre un transeúnte con un teléfono móvil en la oreja y su interlocutor del que podríamos adivinar la empresa para la que trabaja y hasta el cargo que ocupa? Amén de *post-its* y contraseñas de usuario compartidas.

Estos ejemplos, aplicables en tercera o en primera persona, son sólo algunas escenas cotidianas

en las que los usuarios, actuando sin malicia, comprometen la seguridad de la información, pero la lista de situaciones posibles tiende a infinito si tenemos en cuenta las acciones malintencionadas.

Paradójicamente, mitigar la exposición a amenazas de índole humano no es una tarea inabordable ni costosa. Basta con seguir una breve lista de buenas prácticas modificando ligeramente los procedimientos de trabajo de algunas áreas de soporte al negocio (RRHH, jurídico, formación, etc.). Sin duda, la clave para el éxito es, como siempre, el impulso de la Dirección de la Empresa.

Seleccionar el personal adecuado no debe ser sólo una comparación de experiencias profesionales y una valoración de ciertas cualidades como la habilidad oral y la capacidad

organizativa. Durante el proceso de definición de puestos de trabajo, debería establecerse una relación entre la clasificación de activos, sus niveles de sensibilidad y el nivel de autorización de acceso asignado a cada posición organizativa. Esta información permitiría identificar puestos sensibles para que, desde las áreas de recursos humanos, se analicen con detalle aspectos adicionales como la ética, la moral y el estado psicosomático de los candidatos.

La redacción de los contratos de trabajo debe llevarse a cabo desde una perspectiva más amplia que la estrictamente laboral (horarios, disponibilidad, convenio, salario, etc.). Decir que es necesario incluir cláusulas de confidencialidad, propiedad intelectual y motivos de rescisión puede parecer obvio, pero si revisamos los contratos existentes nos sorprenderíamos por la despreocupación y desprotección legal con la que se han establecido gran parte de las relaciones contractuales con los empleados que manejan información sensible.

También deberían incluirse **cláusulas adicionales** que pusiesen en conocimiento de todos los empleados la propiedad y uso de los activos de la compañía, exigiéndoles su conformidad explícita así como el acatamiento de las políticas de seguridad de la empresa. Omitir esto impedirá legalmente que la empresa pueda, por ejemplo, auditar o analizar el correo electrónico.

El proceso de incorporación de los empleados, además de contemplar el traspaso de conocimientos asociados al puesto de trabajo, así como una visión global de la empresa, debería incluir un capítulo con el que mostrar, sensibilizar y concienciar sobre los aspectos fundamentales de la Política de Seguridad de la Información de

la compañía, así como de las mejores prácticas a seguir. Incluir y enfatizar la Seguridad de la Información en el ciclo formativo inicial hará que los empleados interioricen su importancia y la tengan presente en el desarrollo de sus actividades.

Posteriormente, debería llevarse a cabo una **formación y concienciación continua** basada en la elaboración y publicación de mensajes cortos, pero efectivos que recuerden y refuercen los principios fundamentales y los buenos hábitos para proteger la información. Protectores de pantalla, *pop-ups* de *logon* y *logoff*, rótulos informativos, publicaciones internas, menciones dentro de otros cursos formativos de la compañía, son algunas opciones económicas y efectivas que ayudarán a reforzar la cultura de seguridad de los usuarios.

Motivación, fidelización y seguimiento continuo. Sin duda, ésta es la parte más complicada de llevar a cabo dentro de cualquier organización. En muchas ocasiones los objetivos del negocio tienden a focalizarse en el incremento de beneficios mediante la optimización de los procesos, la reducción de gastos y la externalización de servicios, olvidando que el motor principal de su negocio son las personas y que de su interés y empuje depende gran parte de los resultados. El 'mentoring', el impulso de planes de desarrollo profesionales efectivos, y hacer partícipes a todos los empleados de las directrices, decisiones y planes estratégicos de la compañía son fundamentales para motivar y obtener la implicación y el interés de los empleados por proteger y mejorar el negocio garantizando la confianza mutua entre empresa y empleados.

Puede parecer simple, pero la mejor métrica para conocer el grado de motivación y fidelización de los empleados es incluir **tests psicosomáticos** en la revisión médica anual.

Finalmente, en las situaciones de **finalización de los contratos**, debe seguirse un procedimiento riguroso y estricto de revocación de autorizaciones y accesos, así como de devolución de todos los activos asignados (credenciales, teléfonos móviles, PDAs, ordenadores portátiles, etc.). No hay que olvidar que muchos de estos activos son, al fin y al cabo, repositorios de información sensible.

Es necesario que empecemos a desviar nuestro foco de atención hacia las personas –los usuarios, los empleados– si no queremos encontrarnos en la difícil situación de justificar inversiones millonarias en tecnologías de seguridad de la información delante de Comités de Crisis originados por incidentes de seguridad de índole humano. ■



Andreu Bravo Sánchez
CISSP
Seguridad de la Información
GRUPO GAS NATURAL