



Mar Monsoriu  
Consultora (Latencia SL)

## Uso y abuso de las redes sociales en las empresas

Hace unos meses en estas mismas páginas (Número 168) se explicó que, en la actualidad, las Redes Sociales profesionales y de negocios son imprescindibles, debido a las muchas las ventajas que ofrecen. Por ejemplo: búsqueda y oferta de empleo cualificado localización de clientes, proveedores, inversores, socios, colaboradores y todo tipo de contactos; actualización permanente de la agenda de correos electrónicos y teléfonos; intercambio de experiencias y conocimientos; evaluación de productos y servicios antes de lanzarlos al mercado y, por supuesto, planificación de campañas de marketing con un altísimo nivel de segmentación. Por todo lo anterior, este tipo de Redes están creciendo y consolidando sus posiciones en el ambiente ejecutivo y empresarial español, especialmente en el relacionado con el sector tecnológico.

Sin embargo, hay que reconocer que son cada vez más los empleados que, de modo casi clandestino, acceden desde su puesto de trabajo a Redes que nada tienen que ver con su quehacer laboral. Redes generalistas como: Facebook, Hi5, Orkut o Myspace; redes especializadas de búsqueda de pareja tipo Match.com o Meetic o las centradas en alguna afición o deporte como Moterus o Footbo, captan cada vez más su atención.

**E**l fenómeno de las Redes Sociales se ha puesto de moda tan repentinamente que son bastantes los trabajadores que se comportan como crios. Es decir, se distraen en exceso explorando las posibilidades que ofrecen estas plataformas. Es más, en opinión de la autora de éstas líneas, ahora ocurre con las Redes Sociales algo parecido a lo que sucedió hace unos años con el correo electrónico. En aquellos tiempos, aunque se usaba para asuntos laborales (pocos al principio) algunas personas se pasaban las horas enviando desde las cuentas corporativas todo tipo de mensajes en cadena, diapositivas de buena amistad y mejores senti-

mientos, bromas, chistes, dibujos y fotografías, a veces algo subditas de tono.

El principal problema de semejante intercambio de mensajes de correo poco relacionados con el trabajo no era necesariamente la

organizaciones. En una etapa de la historia de Internet donde no eran tantos los usuarios que tenían acceso a la Red desde sus hogares, no era infrecuente que de vez en cuando entre las noticias de prensa y televisión se alertara a los usuarios de la llegada de nuevos

.....  
**“Empleados y empleadores deberían encontrar un equilibrio que destense a los primeros y no afecte al rendimiento que esperan obtener de sus trabajadores los segundos”**  
.....

pérdida de tiempo, sino los virus y todo tipo de software malicioso que se colaba en los equipos y en las redes de las empresas y de las

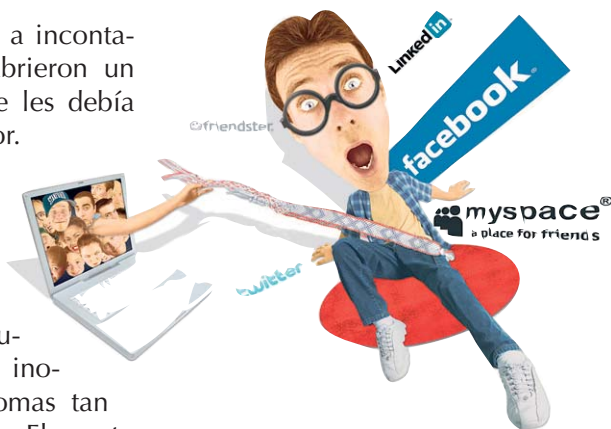
virus. Aun está fresco en la memoria colectiva el recuerdo del famoso virus “I love you” que causó considerables estagros en el

mundo laboral, debido a incontables empleados que abrieron un mensaje de correo que les debía resultar muy prometedor.

De manera parecida los virus se fueron colando en forma de salvapantallas y todo tipo de ejecutables camuflados en inocentes archivos de bromas tan celebradas en esa época. El asunto comenzó a tomarse más en serio cuando en algunas empresas (recuerdo una de fabricación de muebles, por ejemplo) estuvieron varios días sin poder trabajar por culpa de que un archivo les había machacado toda su información incluidos los pedidos, las facturas y cualquier tipo de comunicación con proveedores y clientes.

El daño causado en el conjunto de las empresas españolas jamás podremos cuantificarlo, pero todos los profesionales del sector TIC sabemos que lo hubo, y que en algunos casos fue considerable. Tanto como que empresas (grandes y pequeñas), organizaciones y organismos públicos comenzaron a elaborar normas de uso del acceso a Internet. En algunos casos además se implementaron medidas más o menos restrictivas en función de los potenciales peligros y de la utilización que se hacía de los recursos. De la falta de control se pasó a una supervisión a veces exagerada como medida de reeducación de los usuarios que, con el tiempo, han aprendido en su mayoría a ser conscientes de los problemas que puede conllevar hacer un mal empleo de Internet en la empresa.

Todo el anterior extenso preámbulo, -que espero que los lectores sepan disculparme-, viene a cola-



ción porque en estos días, con la eclosión de las Redes Sociales estamos volviendo a revivir lo que acabo de contar. Bien es cierto que con algunas novedades pero, en esencia, es lo mismo. Los trabajadores están usando unas herramientas sin haber recibido instrucciones acerca de las mismas. Especialmente acerca de los potenciales riesgos que conllevan y que, por si sirve de ayuda, a continuación pasamos a exponer.

## ► Potenciales peligros de las redes sociales para las empresas

### Pérdida de tiempo.

El primer problema relacionado con las Redes Sociales en Internet con el que se encuentran las empresas es que los trabajadores les dediquen un tiempo excesivo que sustraen de su quehacer laboral. Las Redes pueden ser muy útiles en la investigación de mercados, es cierto, pero cotillear las fotos que ha subido a un perfil tal o cual persona, poco tiene que ver con un trabajo serio. Además dedicar parte de la jornada a actividades relacionadas con el ocio puede suponer una pérdida de productividad para el trabajador y por ende para la empresa. Sin

embargo, la prohibición total de acceso parece estar desaconsejada según algunos estudios que se han realizado al respecto, de modo que empleados y empleadores deberían encontrar un equilibrio que destense a los primeros y no afecte al rendimiento que esperan obtener de sus trabajadores los segundos.

### Inseguridad de los equipos y de las redes.

Otro grave problema estriba en que, por medio de las Redes Sociales, los usuarios reciben mensajes que aparentemente proceden de personas que conocen. Esos mensajes llevan enlaces a programas maliciosos (virus, troyanos, espías, etc.) que contagian a los equipos y a las redes, comprometiendo la seguridad informática de la empresa. Los creadores de este tipo herramientas informáticas para cometer delitos de todo tipo, han migrado sus estrategias de propagación del correo electrónico a las Redes Sociales y a diario ingenian nuevas formas para lograr que los usuarios se infecten. Así que hay que tener cuidado y alertar a los usuarios para que no accedan a estos archivos peligrosos.

### Inseguridad de las instalaciones.

Quienes se dedican al espionaje militar o industrial están de suerte porque soldados y trabajadores publican fotos de sus lugares de trabajo donde se muestran instalaciones y equipamiento. Tal es así que los ejércitos de Estados Unidos e Israel, entre otros, han prohibido a sus efectivos que tengan colgados perfiles en las Redes Sociales para evitar que en los mismos se vean instalaciones militares como, de hecho, ya venía sucediendo. Similar problema ocurre en las empresas. Una simple foto del lugar de trabajo puede

comprometer la seguridad de las instalaciones ante espías industriales, ante ladrones profesionales y ante quien sea.

### **Inseguridad de métodos, procesos y planes estratégicos de la empresa.**

En las Redes Sociales los trabajadores sin darse cuenta pueden hacer comentarios que revelen información sobre los métodos, procesos y planes estratégicos de las empresas. Información que, en manos de rivales, les puede hacer perder ventajas competitivas. Hay que ser muy prudente con lo que se va escribiendo acerca de la actividad laboral diaria.

### **Política de imagen.**

Paralelamente al caso anterior, los trabajadores pueden hacer difundir, sin querer, prácticas y hábitos laborales que den mala imagen de la empresa. Comentarios o bromas acerca de que vende muy caro para lo que ofrece, de lo mal que tratan a los empleados, de la ausencia de ética de los jefes, pueden presentar un cuadro de la empresa poco atractivo y que dañe considerablemente su identidad corporativa.

### **Protección de datos.**

Hay algunos usuarios que, queriendo o sin querer, hacen pública en las Redes Sociales información personal de jefes y empleados de la empresa u organización para la que trabajan. Esta práctica además de ser ilegal puede perjudicar enormemente a los afectados que ven expuesta su intimidad y la privacidad de sus datos.

### **Peligro de head hunting de terceros.**

Muchos empleados ofrecen en sus perfiles información relativa a la empresa donde trabajan, a su puesto de trabajo exacto y al modo



directo de contactar con ellos. Con lo cual quedan expuestos a que desde empresas competidoras se les hagan ofertas y haya fuga de profesionales de unas compañías a otras que los localizan a través de las Redes. Localizar a trabajadores en activo altamente cualificados es una ventaja para algunas empresas y un claro inconveniente para otras que ven cómo se les va el personal al que han estado formando.

### **Fugas de know-how.**

En medio de un ambiente distendido y donde todo se comparte cabe la posibilidad de que empleados de una empresa ayuden o den consejo a colegas o amigos de empresas competidoras ofreciendo soluciones que suponen una verdadera fuga del *know-how*, del conocimiento de la compañía. Por otra parte las soluciones planteadas por terceras personas ajenas a la empresa, si no se analizan suficientemente, pueden llevar a problemas técnicos y de organización debido a la falta de adecuación respecto a los procesos establecidos internamente.

### **Pérdida de valiosos contactos.**

A través de las Redes Sociales se pueden conocer los contactos comerciales y de negocios de otras personas que trabajen para la competencia y se les puede "robar".

Como otros puntos anteriores, lo que supone una enorme ventaja para alguien es un inconveniente para otros. Por medio de las Redes Sociales muchos usuarios pierden clientes y proveedores que pasan a serlo de otros. La forma de evitarlo es mezclar contactos de diverso tipo, no etiquetarlos, y ponérselo difícil a quien pretenda acceder a los mismos.

### **Suplantación del perfil de una empresa.**

Por último, algo que ya comienza a suceder en las Redes Sociales es que hay usuarios que suplantan el perfil público que correspondería tener a una empresa. Es decir, su identidad digital en las Redes. Algo parecido a cuando alguien hacía un sitio web de una empresa porque era consumidor o distribuidor de sus productos. También se está dando el caso de que esas suplantaciones encubren la generación de Comunidades Virtuales Antimarca que pueden perjudicar sobremanera la imagen pública y la credibilidad de una compañía. Sirva de ejemplo las que se muestran en las imágenes que acompañan estas líneas. Sobre este problema sólo resta añadir que el mejor modo, por parte de una empresa, de tratar de evitarlo y/o de contrarrestarlo es crear su propio perfil y difundir las noticias que se consideren oportunas en cada momento. ♦