GOBIERNO DE ESPAÑA
MINISTERIO DE INDUSTRIA, ENERGÍA Y TURISMO

INTECO
Instituto Nacional de Tecnologías de la Comunicación

Guía para empresas:

identidad digital y reputación online

INSTITUTO NACIONAL DE TECNOLOGÍAS DE LA COMUNICACIÓN

Edición: Noviembre 2012

La *"Guía para empresas: identidad digital y reputación online"* ha sido elaborada por el Instituto Nacional de Tecnologías de la Comunicación (INTECO):

Pablo Pérez San-José (dirección)

Susana de la Fuente Rodríguez (coordinación)

Cristina Gutiérrez Borge (coordinación)

Eduardo Álvarez Alonso

Laura García Pérez

El **Instituto Nacional de Tecnologías de la Comunicación (INTECO)** es una sociedad estatal adscrita al Ministerio de Industria, Energía y Turismo a través de la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información. La misión de INTECO es reforzar la ciberseguridad, la privacidad y la confianza en los servicios de la Sociedad de la Información, aportando valor a los ciudadanos, empresas, AA.PP. y al sector TIC, y coordinando esfuerzos con los organismos nacionales e internacionales que trabajan en esta materia. Su Observatorio de la Seguridad de la Información (http://observatorio.inteco.es) tiene como objetivo describir, analizar, asesorar y difundir la cultura de la seguridad, la privacidad y la e-confianza.

En la elaboración de esta guía, INTECO ha contado con el apoyo técnico de:

Índice

1. Introducción

El uso de los servicios de Internet no se circunscribe únicamente a los individuos, ya que empresas, organizaciones y entidades participan activamente en la Red para apoyar o potenciar sus actividades. Por tanto, es cada vez más importante la creación de una **identidad digital corporativa**, basada en una estrategia de comunicación sólida que les permita alcanzar una posición en entornos colaborativos en Internet, y comunicarse mejor con sus clientes, proveedores y público en general.

Una parte importante de esa identidad digital está formada por la presencia de las organizaciones en redes sociales. Las empresas, conscientes de esa importancia, utilizan las redes sociales de manera profesional planificando previamente su estrategia de comunicación en ellas. Además, están satisfechas con el uso de redes sociales ya que valoran su experiencia de manera muy positiva.

Un 26,8% de las pequeñas y medianas empresas españolas usa alguna red social[1], y el grado de satisfacción que las entidades otorgan a su experiencia de uso profesional roza el notable con una nota de 6,9 sobre diez puntos[2].

> *El debate sobre si h0y las empresas deben tener o no una presencia activa en los medios sociales carece ya de sentido.*
>
> *La revolución ya se ha producido y, con independencia de cuál sea su resultado final, las organizaciones y sus marcas deberían "salir a la calle virtual" a experimentar, a equivocarse, a fracasar, a triunfar.*

Las motivaciones que mueven a las empresas a tener presencia en redes sociales son diversas. En primer lugar, las empresas reconocen que las redes sociales representan una de las vías más importantes de promoción de sus productos o servicios, ya que implican una mayor llegada al público, a un menor coste. Y, en segundo lugar, afirman que su presencia en redes sociales mejora la difusión y comunicación con el cliente y con otros profesionales.

Aprovechar las posibilidades que ofrece la presencia en redes sociales brinda a las empresas numerosas ventajas. En comparación con los medios tradicionales, las redes sociales permiten acercarse a los clientes objetivo y dialogar con ellos.

Pero también las empresas deben ser conscientes y valorar los posibles riesgos derivados de la incursión de las empresas en los medios sociales. Surge un nuevo

[1] Fuente: INTECO: *Estudio sobre seguridad de la información y continuidad de negocio en las empresas españolas.* Disponible en: http://www.inteco.es/Seguridad/Observatorio/Estudios/Estudio_pymes_seguridad_2012

[2] Fuente: *Observatorio sobre el uso de las redes sociales en las PYMEs españolas*. Fundación Banesto en colaboración con el Ministerio de Industria Turismo y Comercio y la Empresa Nacional de Innovación (ENISA) (2011). Disponible en: http://www.inteco.es/studyCategory/Seguridad/Observatorio/Biblioteca/observatorio_redes_sociales_FB

escenario en el que las amenazas para las organizaciones se intensifican por el número de incidentes y la gravedad de sus consecuencias, provocando no solo paradas y retrasos en la normal actividad del negocio, sino también pérdidas económicas, de imagen y reputación online. Una empresa se puede formular preguntas como: ¿qué hacer cuando suplantan la identidad de mi organización en la Red? o ¿cómo proceder cuando alguien ajeno a mi empresa publica una información negativa sobre la misma? Esta guía busca dar respuesta a estas y otras preguntas.

El objetivo perseguido es desarrollar un análisis riguroso de los conceptos de identidad digital y reputación online en el ámbito empresarial desde el punto de vista de la seguridad, generando conocimiento en cuanto a los riesgos existentes y aportando una serie de pautas de actuación y recomendaciones para la gestión de la identidad y reputación online.

Bajo esta premisa se desarrollan los siguientes epígrafes:

- Identidad digital.
- Reputación online.
- Riesgos en la gestión de la identidad y reputación.
- Marco legal.
- Recomendaciones para la gestión de la identidad digital y reputación online.
- Bibliografía.

2. Identidad digital

Hoy en día, las organizaciones difunden su imagen en Internet mediante herramientas como páginas web corporativas, blogs empresariales, perfiles y páginas en redes sociales y, en general, en la llamada, Web 2.0.

Más allá de lo que la propia empresa publique y dé a conocer de sí misma, la identidad digital corporativa se ve complementada con lo que los propios usuarios y clientes opinan sobre la empresa en Internet. Incluso, no es necesario que una empresa se encuentre presente en Internet, para que puedan surgir este tipo de opiniones sobre ella. Así pues, el contenido generado por terceros forma parte de su identidad digital de la misma manera que el creado por la propia empresa.

> *La **identidad digital corporativa**, por tanto, puede ser definida como el conjunto de la información sobre una empresa expuesta en Internet (datos, imágenes, registros, noticias, comentarios, etc.) que conforma una descripción de dicha organización en el plano digital.*

En este sentido, aparece un nuevo concepto, los "prosumidores": sujetos activos que participan del mismo proceso de la construcción de la marca a través del diálogo abierto con otros consumidores y con las propias compañías[3].

> *En la Web 2.0 cualquier empresa o profesional puede tener presencia digital gracias a clientes y usuarios sin necesidad siquiera de tener una página web, tanto para hablar maravillas como para maldecir un servicio o producto.*

La Web 2.0 constituye un nuevo canal masivo de comunicación para las empresas y las redes sociales representan una herramienta mediante la cual las organizaciones disponen de un *feedback* en tiempo real de clientes y usuarios.

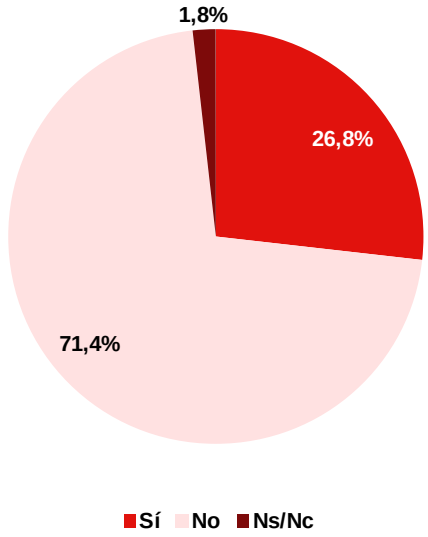
Las organizaciones son conscientes de la importancia de estar presentes en los medios sociales. Así, una cuarta parte (26,8%) de las pequeñas y medianas empresas en España utiliza alguna red social de manera profesional[4]. En aquellas organizaciones en las que el contacto directo con el cliente es parte importante de la actividad de la entidad se utilizan más las redes sociales. Este es el caso, por ejemplo, de hostelería y turismo, finanzas y seguros y educación y servicios sociales[5].

[3] Fuente: DAVID MARTÍNEZ PRADALES: *Las marcas y las redes sociales. Identidad digital y reputación online.* Evoca. *Cuadernos de comunicación*. Disponible en: http://www.evocaimagen.com/cuadernos/cuadernos5.pdf

[4] Fuente: INTECO: *Estudio sobre seguridad de la información y continuidad de negocio en las empresas españolas.* Disponible en: http://www.inteco.es/Seguridad/Observatorio/Estudios/Estudio_pymes_seguridad_2012

[5] Véase nota al pie 2.

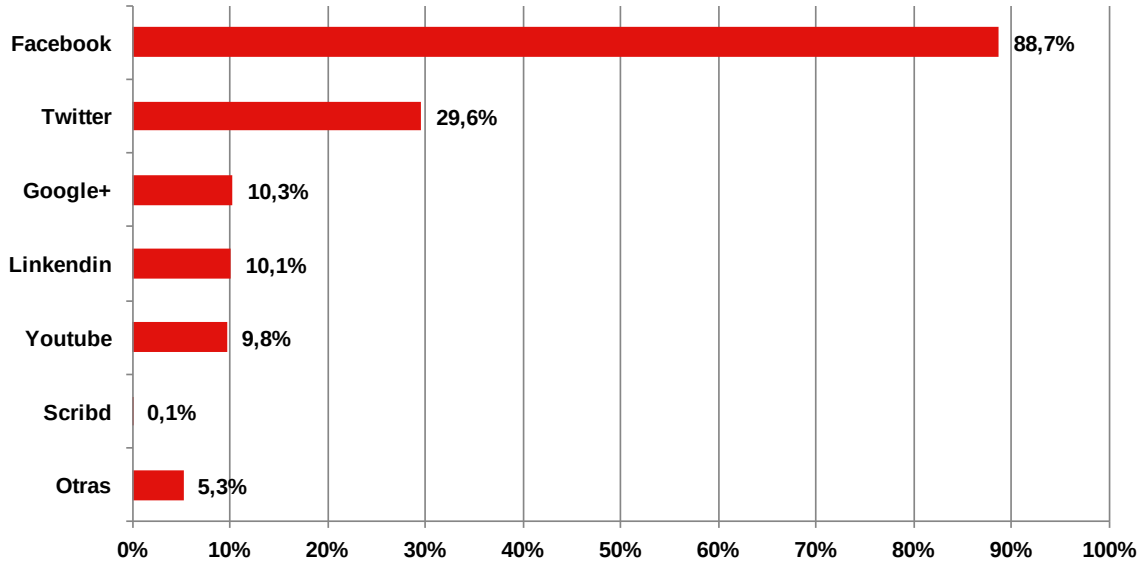
Gráfico 1: Pequeñas y medianas empresas españolas que tienen un perfil en alguna red social (%)



Fuente: INTECO (2012)

De las empresas que manifiestan disponer de perfiles o páginas en redes sociales, un 88,7% se encuentra en Facebook. A gran distancia se colocan redes sociales como Twitter (29,6%), Google+ (10,3%), LinkedIn (10,1%) o Youtube (9,8%).

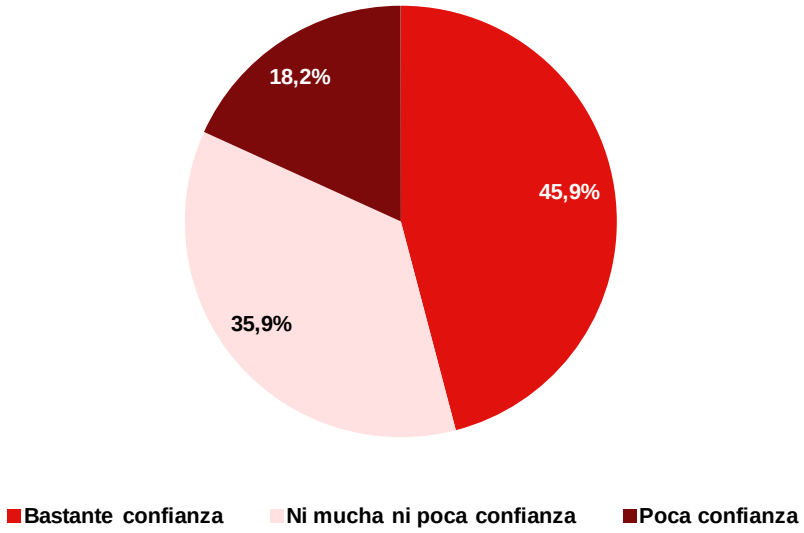
Gráfico 2: Pequeñas y medianas empresas españolas que usan cada una de las redes sociales (%)



Fuente: INTECO (2012)

Las empresas españolas, como no podía ser de otro modo, están abrazando la Web 2.0 en todas sus dimensiones. De hecho, un 45,9% de las empresas otorga *bastante* confianza a las redes sociales, frente a un 35,9% que se muestran indiferentes y un 18,2% que afirma que las redes sociales les generan *poca* confianza.

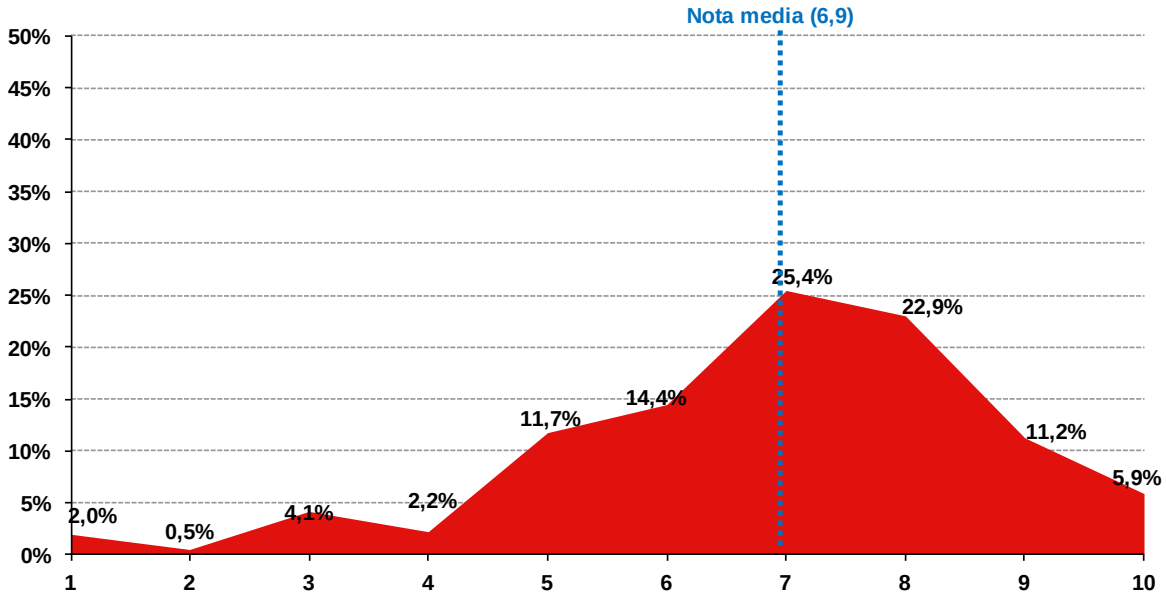
Gráfico 3: Grado de confianza de las pequeñas y medianas empresas españolas en la utilización de redes sociales (%)



Fuente: INTECO (2012)

Y por último, ¿cómo valoran las empresas el uso de redes sociales? En una pregunta de valoración de 1 a 10, la nota media que las organizaciones le otorgan a su experiencia en los medios sociales es un 6,9. El 7 y el 8 reúnen casi la mitad (48,3%) de las puntuaciones y solo un 8,8% valora esta presencia por debajo del 5.

Gráfico 4: Valoración global del uso de las redes sociales por parte de las pequeñas y medianas empresas (%)



Fuente: Fundación Banesto (2011)

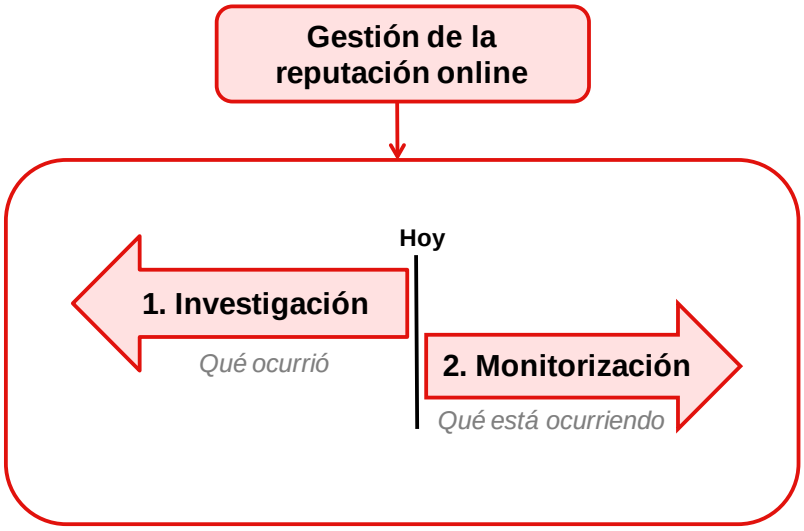
3. Reputación online

La reputación corporativa es el concepto que mide cuál es la valoración que hace el público de una compañía. Esta definición es trasladable al mundo de Internet y a la Web Social o Web 2.0 donde aparece la idea de reputación online corporativa.

> *La **reputación online** podría definirse como la valoración alcanzada por una empresa a través del uso o mal uso de las posibilidades que ofrece Internet.*

Para entender la noción de reputación online de una empresa se deben distinguir los conceptos de investigación, monitorización y gestión.

> *La gestión de la reputación online engloba tanto la investigación (qué ocurrió), como la monitorización (qué está ocurriendo), para poder crear la identidad digital de la empresa deseada.*



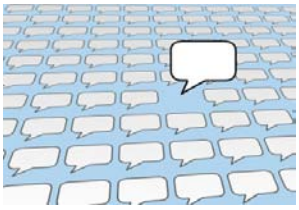
Mapa de gestión de la reputación online[6]

Investigación de la reputación online (*Qué ocurrió*)

La investigación consiste en un análisis retrospectivo de la reputación online de una empresa. Este análisis abarca una primera fase cuantitativa en la que se registran opiniones de usuarios y de medios a través de blogs, foros, redes sociales, etc. sobre la empresa, y una segunda fase cualitativa en la que se identifican las fortalezas y áreas de mejora de la entidad, a través de las opiniones positivas y negativas, respectivamente.

[6] MIGUEL DEL FRESNO. *Cómo investigar la reputación online en los medios sociales de la Web 2.0. Identidad Digital y Reputación Online. Evoca. Cuadernos de comunicación*. Disponible en: http://www.evocaimagen.com/cuadernos/cuadernos5.pdf

Monitorización de la reputación online (*Qué está ocurriendo*)



La monitorización de la reputación online es el seguimiento regular a través de la Red de la identidad digital de la organización. Esta monitorización incluye el registro de las informaciones, los comentarios y opiniones que se generan en Internet sobre la organización, marcas comerciales y otros activos sujetos a propiedad industrial e intelectual, productos o personas.

Esta tarea se apoya cada vez más en aplicaciones informáticas que encuentran, clasifican y analizan la información que circula en Internet y en las redes sociales de forma automatizada, con el objetivo de medir la reputación en Internet.

Gestión de la reputación online

Como hemos visto, la gestión puede definirse como la fase transversal de la reputación online que comprende tanto la fase de investigación como la de monitorización. Esta gestión contempla un conjunto de prácticas:

- La adopción de estrategias de optimización de resultados en motores de búsqueda (*Search Engine Optimization*, SEO) y posicionamiento en los buscadores de Internet (*Search Engine Marketing*, SEM), la creación y publicación de contenidos en perfiles corporativos de redes sociales y páginas web especializadas, el desarrollo de notoriedad y presencia en Internet y la lucha contra contenidos perjudiciales.

  Dentro de este aspecto también se incluye el concepto de *branding online*, o construcción de una marca en línea. El *branding online* es el conjunto de estrategias empleadas para posicionar un sitio web y conducir tráfico relevante hasta el mismo, a menor coste que sólo el empleo de publicidad. Este proceso está estrechamente relacionado con el marketing, que consiste en la creación de campañas publicitarias y de comunicación en medios tanto online como offline, orientados a generar una imagen de la empresa positiva y activa en medios sociales, que repercuta positivamente en el negocio.

- Otro aspecto relevante en la gestión reputacional de las organizaciones depende de la fijación de reglas claras que deben seguir aquellas personas que, o bien representan a la organización, o bien mantienen una relación laboral con la misma. Un comentario inadecuado del Consejero Delegado o un desliz de un trabajador revelando información empresarial sensible, son ejemplos de situaciones que pueden poner en serio peligro el prestigio de la empresa.

- Por último, la gestión de la reputación en Internet requiere de una estrategia que abarque a la totalidad de áreas de negocio, comenzando por la dirección y los recursos humanos, así como la operativa, la gestión con los proveedores, la comunicación y el marketing, las ventas y la atención al cliente.

Cada vez son más las organizaciones (tanto públicas como privadas) que gestionan de forma profesional su identidad digital corporativa y su reputación en Internet y en la Web 2.0, desde la perspectiva de la prevención frente a posibles problemas, como en la reacción y mitigación en caso de incidentes.

Esta gestión ha dado lugar al nacimiento de un nuevo perfil profesional: Social Media Manager o Community Manager. Este profesional desempeña un rol activo y especializado en la generación de "conversación" desde la organización manteniendo una interlocución directa y constante con los usuarios.

4. Riesgos en la gestión de la identidad digital y reputación

Al mismo tiempo que la presencia de la empresa en medios sociales (por sí misma o por la acción de terceros) le reporta efectos positivos, existen diferentes amenazas que pueden generar impactos negativos en su imagen y reputación online. Una pérdida de confianza en la marca a partir de comentarios perjudiciales sobre un producto es un ejemplo de ello.

Además, el efecto multiplicador de Internet posibilita que un incidente aislado (incluso generado fuera de la Red) se convierta en una situación de difícil solución. En este sentido, cada vez es más frecuente descubrir noticias sobre crisis reputacionales en Internet, que impactan de tal forma en la imagen de la empresa, que los efectos perduran en el tiempo. Un ejemplo de ello es el caso de la campaña de publicidad "Más por menos"[7] de Metro de Madrid, que no tuvo la acogida esperada y generó una intensa polémica en redes sociales con incluso llamamientos al boicot del servicio.

A continuación se describen las principales amenazas para la identidad digital y reputación online desde el punto de vista de la seguridad. Dado que estas amenazas son múltiples y en ocasiones se encuentran interrelacionadas, un mismo riesgo se puede observar desde diferentes perspectivas.

4.1 SUPLANTACIÓN DE IDENTIDAD

Caso 1: La empresa juguetera DOLLS S.A. está recibiendo numerosas quejas por parte de los consumidores, buena parte de ellas a través de las redes sociales. La razón es que un tercero malintencionado está enviando correos electrónicos y mensajes a través de Facebook simulando ser la empresa DOLLS, en los que se apela a la buena fe de los destinatarios solicitando que realicen donaciones para el envío de juguetes a niños desfavorecidos. Esta campaña resulta ser una estafa y la empresa, aunque no es la responsable, se ve inmersa en una crisis online.

La suplantación de identidad de la empresa en Internet es la usurpación de los perfiles corporativos por terceros malintencionados, actuando en su nombre. Dentro de este riesgo se contempla la creación o el acceso no autorizado al perfil de una empresa o entidad en un medio social y la utilización del mismo como si se tratara de la organización

[7] Más información: "Una campaña de Metro de Madrid desata las críticas de los usuarios". Disponible en: http://ccaa.elpais.com/ccaa/2012/01/03/madrid/1325586372_171195.html

suplantada. Por ejemplo, el Tribunal Superior de Justicia de la Comunitat Valenciana fue objeto de suplantación en Twitter a través de la cuenta falsa @TSJ_CV[8].

Los atacantes crean perfiles falsos con varios propósitos, destacando el robo de información sensible de los usuarios de la empresa suplantada para la comisión de fraude online. Para ello, recurren a diferentes técnicas:

- ***Phishing***: el estafador o phisher usurpa la identidad de una empresa o institución de confianza para que el receptor de una comunicación electrónica aparentemente oficial (vía email, redes sociales, SMS, etc.) crea en su veracidad y facilite, de este modo, los datos privados que resultan de interés para el estafador[9]. Para dar credibilidad a la suplantación, utiliza imágenes de marca originales o direcciones de sitios web similares al oficial. Cada vez son más frecuentes los casos de phishing a través de redes sociales, como por ejemplo, el sufrido por la página de fans del Fútbol Club Barcelona[10].

- ***Pharming***: el atacante modifica los mecanismos de resolución de nombres sobre los que el usuario accede a las diferentes páginas web tecleando la dirección en su navegador. Esta modificación provoca que cuando el usuario introduce en el navegador la dirección del sitio web legítimo, automáticamente es dirigido hacia una página web fraudulenta[11] que suplanta a la oficial.

Las consecuencias de la suplantación de la identidad de empresas en Internet y de los ataques derivados son diversas (confusión con la identidad original, robo de información de clientes, fraude online, extorsión, etc.), pero en todo caso suponen un perjuicio en la reputación generada por la empresa sobre su actividad, sus productos y/o servicios, tanto dentro como fuera de la Red. Como se aborda en el apartado 5.1 DERECHO AL HONOR DE LAS EMPRESAS Y ACCIONES LEGALES PARA SU DEFENSA, estas conductas tienen implicaciones legales.

Para finalizar, es necesario distinguir entre suplantación de identidad y parodia. Crear una página o perfil que suponen una caricatura de la realidad es una práctica cada vez más

[8] Fuente: "Twitter cerró el perfil falso del TSJCV tras la orden judicial". Disponible en: http://blog.abusoenlared.com/delitos-informaticos/twitter-cerro-el-perfil-falso-del-tsjcv-tras-la-orden-judicial/

[9] Más información sobre phishing: http://www.inteco.es/wikiAction/Seguridad/Observatorio/area_juridica_seguridad/Enciclopedia/Articulos_1/Phishing_1

[10] Fuente: "Ataque de Phishing a FC Barcelona Fans". Disponible en: http://www.electro-imagen.com/noticias/45/11584-ataque-de-phishing-a-fc-barcelona-fans

[11] Más información sobre falsas páginas web: http://cert.inteco.es/Formacion/Fraude_en_Internet/paginas_falsas_web/

extendida en medios sociales. Los creadores no actúan en nombre de la empresa o marca recreada, sino que generalmente utilizan estos perfiles o páginas como forma de crítica. En tanto no vulneren lo establecido en la Ley, son fórmulas totalmente lícitas.

4.2 REGISTRO ABUSIVO DE NOMBRES DE DOMINIO

Caso 2: Los responsables del comercio EL DESTORNILLADOR han decidido crear la página web de la empresa. Sin embargo, al intentar registrar el nombre de dominio, descubren que ya están ocupados tanto eldestornillador.com como eldestornillador.es (aunque no operativos en la Red). Poco después, los ciberocupantes les solicitan importantes sumas de dinero por "devolverles" dichos nombres de dominio. Los clientes ya han manifestado en foros su descontento por la falta de operatividad de las páginas.

El nombre de dominio es la denominación fácilmente recordable que utilizan los usuarios para acceder a una página web (por ejemplo, **inteco.es**). Este nombre de dominio está asociado a una dirección IP (*Internet Protocol*), o códigos que utilizan los ordenadores para comunicarse entre sí.

Las empresas tratan de identificarse adecuadamente al público, eligiendo el nombre de dominio que coincida con sus signos distintivos, esto es, el nombre comercial o la marca de sus productos o servicios[12].

El problema se origina durante el proceso de registro del nombre de dominio, al no existir ningún control o vigilancia por parte de las autoridades encargadas de dicho registro, a efectos de impedir que se violen derechos de propiedad industrial. En el caso de cometerse alguna infracción con el registro y uso del dominio, el único responsable es el solicitante del registro.

La amenaza se produce cuando terceros malintencionados registran uno o varios nombres de dominio que coinciden con la marca de la empresa, impidiendo a esta última utilizar dichas denominaciones en su negocio. Este ataque, conocido como **cybersquatting**, también puede producirse si la empresa se olvida de renovar el nombre de dominio, o si aparece una nueva extensión TLD[13] (como .inf o .geo) y el propietario de la marca no realiza el correspondiente registro.

[12] Fuente: José Ramos López: "Los conflictos entre los nombres de dominio y las marcas. El Cybersquatting". Disponible en: *http://bloguerlaw.blogspot.com.es/2009/04/los-conflictos-entre-los-nombres-de.html*

[13] TDL o *Top Level Domain*: Dominio de nivel superior. Más información: www.icann.org

En todo caso, el ataque puede tener dos finalidades concretas:

- Atraer visitantes a la página web o blog ocupadas, aprovechándose de la reputación de la empresa propietaria de la marca. Generalmente, obtienen beneficios derivados de la publicidad que incluyen en la página.

- Extorsionar al titular legítimo de la marca, solicitándole un precio superior al pagado por el extorsionador en el registro a cambio de la transferencia del dominio, como ocurre en el caso de partida. No hay que confundir esta extorsión con la actividad de los "domainers" o personas dedicadas a la inversión en dominios con el fin de venderlos, alquilarlos, etc.

Por su parte, el ***typosquatting*** es una variante del cybersquatting, que consiste en el registro de nombres de dominio parecidos a la marca registrada, explotando confusiones típicas al teclear o visualizar una dirección. Por ejemplo, resulta lógica la equivocación al escribir "*Facebok"* en lugar de *Facebook*, o en acceder a "lamoncloa.gov.es" en lugar de a la página legítima "lamoncloa.gob.es". En este caso, el objetivo suele ser la comisión de un fraude[14].

Por tanto, ambas acciones ilegales plantean un conflicto entre los nombres de dominio y los signos distintivos de la empresa: se produce un impacto, tanto en la identidad de la empresa (al crear confusión en el nombre de la página o blog empresarial que coincide con la marca o nombre comercial), como en la reputación online (buscando un lucro en base al prestigio obtenido por la empresa y sus marcas). Este perjuicio conlleva unas implicaciones jurídicas, que se analizan en el apartado 5.1 DERECHO AL HONOR DE LAS EMPRESAS Y ACCIONES LEGALES PARA SU DEFENSA.

[14] Ejemplo: "El negocio del typosquatting". Disponible en: http://www.ticbeat.com/analisis/negocio-typosquatting-errores-teclear-dominio/

4.3 ATAQUES DE SEGURIDAD DDOS

Caso 3: El periódico digital EL ROTATIVO ONLINE sufre un ataque de seguridad a su sitio web. En poco tiempo, el servidor recibe tantas peticiones de conexión simultáneas que se satura y deja de funcionar.

El riesgo ejemplificado en el caso de partida consiste en el denominado Ataque de Denegación de Servicio Distribuido, o ataque DDoS, o conjunto de técnicas que tienen por objetivo dejar un servidor inoperativo, hablando en términos de seguridad informática[15].

Para poder llevar a cabo el ataque, se requiere que varios equipos trabajen coordinadamente para enviar peticiones masivas a un servidor concreto, por ejemplo accediendo a la página web y descargando archivos, realizado visitas, etc. Así consiguen saturar dicho servidor y provocar su colapso, al no poder este responder tal flujo de peticiones.

Además, los equipos utilizados para lanzar el DDoS suelen formar parte de una botnet o red de ordenadores zombis[16], que el ciberatacante controla de forma remota sin que los propietarios sean conscientes de ello. La complejidad para afrontar estos ataques masivos es muy alta, ya que proceden de numerosos equipos.

Como consecuencia, la página web empresarial deja de funcionar, acarreándole un perjuicio a la identidad digital (la manifestación del negocio en la Red deja de existir) y a la reputación online, puesto que el hecho de ser atacada proyecta una imagen de vulnerabilidad frente al público, junto con la falta de operatividad que se provoca. Estos ataques están cobrando cada vez más relevancia pública como forma de ciberprotesta[17].

4.4 FUGA DE INFORMACIÓN

Caso 4: La gestoría GESTONLINE dispone en su sitio web de una intranet a través de la cual presta servicio a sus clientes. El sitio es atacado y datos especialmente sensibles de sus clientes (entre ellos, nombres, direcciones, información económica y números de cuenta) aparecen publicados en Internet. Esto le supone a la empresa una inspección por parte de la Agencia Española de Protección de Datos (AEPD).

[15] Más información: http://www.inteco.es/wikiAction/Seguridad/Observatorio/area_juridica_seguridad/Enciclopedia/Articulos_1/Ataque_de_Denegacion_de_Servicio

[16] Fuente: *Botnet, ¿qué es una red de ordenadores zombis?* Disponible en: http://www.inteco.es/Seguridad/Observatorio/Articulos/Articulo_botnet

[17] Por ejemplo: "Un ciberataque masivo tumba a la SGAE y al Ministerio de Cultura". Disponible en: http://www.rtve.es/noticias/20101007/sgae-ministerio-cultura-victimas-ciberataque-masivo/359603.shtml

En este caso, la buena imagen y el prestigio de una entidad puede verse comprometida por el robo de información sensible y/o confidencial (como por ejemplo, datos personales de trabajadores y clientes, datos bancarios, informaciones estratégicas de la organización, etc.) y su revelación en Internet[18].

De nuevo, el objetivo suele ser el lucro (por ejemplo, al obtener información bancaria de la empresa y sus clientes, o al extorsionar a la propietaria de los datos a cambio de un rescate), aunque también se distinguen otros motivos, como el espionaje industrial o el desprestigio a la organización.

Se distinguen dos manifestaciones de este riesgo:

- Desde el interior de la organización, bien por error accidental de los empleados, bien por una acción consciente e intencionada. En el primer caso, el extravío de un pendrive o un dispositivo móvil o el error en el envío de comunicaciones son causas de pérdida de información. En el segundo caso, un empleado descontento o que ha sido despedido puede tomar represalias contra la empresa difundiendo documentos o datos a los que ha tenido acceso.

  Para evitar estas situaciones, las organizaciones utilizan medidas como el establecimiento de políticas de seguridad o la incorporación de cláusulas de confidencialidad en los contratos laborales.

- Desde el exterior, utilizando diferentes técnicas para robar información de los equipos y sistemas de la entidad atacada, como por ejemplo:

  a. La infección de malware para robo de datos. Una vez que el software malicioso es instalado en el equipo de la víctima, se dedica a recopilar información y remitírsela al atacante, sin que el usuario se percate.

  b. Los ataques *Man in the Middle*, en los que el atacante se posiciona entre el servidor web de la entidad y el equipo que solicita la conexión a dicho servidor, desde donde puede leer, filtrar e incluso modificar la información que se está transfiriendo sin dejar rastro de su acción.

[18] Un ejemplo de este tipo de incidentes ha sido el robo de datos de usuarios a la multinacional Sony, que ha implicado un gran perjuicio a la marca PSP. Fuente: "Sony investiga el robo de datos de 77 millones de cuentas de PlayStation": http://www.lavanguardia.com/internet/20110427/54146138829/sony-investiga-el-robo-de-datos-de-77-millones-de-cuentas-de-playstation.html

4.5 PUBLICACIONES POR TERCEROS DE INFORMACIONES NEGATIVAS

Caso 5: La empresa de venta online TUTIENDA.COM, ha sido falsamente acusada de estafar a sus clientes. La repercusión del comentario ha tenido tanto alcance, que el hashtag #tutiendafraude en Twitter se ha convertido en *trending topic* (tema de actualidad). Debido a esta acusación, la empresa ha registrado una importante devolución de pedido, con la consecuente caída del negocio.

A través de los medios sociales, las empresas obtienen un *feedback* directo de usuarios, clientes y público en general sobre la empresa y sus productos o servicios.

¿Qué ocurre cuando esta respuesta es negativa y puede afectar a su reputación online? Los *hashtags* o etiquetas de Twitter permiten que una corriente de comentarios se agrupe y tenga mayor visibilidad. Cuando el sentimiento generado en el público es negativo, las posibilidades de que ese flujo se intensifique aumentan. En este sentido, los *trolls* son aquellos usuarios que se dedican a avivar el sentimiento negativo hacia otros usuarios o empresas, utilizando, si es necesario, fórmulas molestas como las burlas, los insultos o las interrupciones en la conversación[19].

En principio, las críticas a las entidades son parte de la interactuación que ofrecen las plataformas colaborativas: no solo se está en la Red, sino que se conversa en ella. El hecho de que una falta de atención, un error en el servicio, un defecto en un producto, etc., sea comentado en Internet es igualmente una información valiosa para la empresa, que puede corregir el fallo en base a estos comentarios negativos. En estos casos, la diligencia de la empresa para dar una respuesta apropiada permitirá solucionar o aliviar la corriente de crítica que se ha generado y, en consecuencia, la recuperación de su imagen y reputación online.

La realización de comentarios negativos o falsos sobre una organización puede tener consecuencias legales. La legislación española contempla acciones tanto civiles como penales (en caso de que la ofensa en cuestión sea considerada una injuria o una calumnia) dirigidas a proteger el honor y reputación de la empresa. La responsabilidad puede alcanzar incluso al propietario del sitio web donde se realizan los comentarios nocivos. Todos estos aspectos serán analizados en el apartado 5, al dibujar el Marco Legal de la reputación online de las empresas.

A pesar de las medidas reactivas a aplicar (retirada de comentarios, acciones legales, etc.), la capacidad de difusión de estos canales aumenta el daño sobre la reputación

[19] Fuente: http://elpais.com/diario/2007/10/23/sociedad/1193090401_850215.html

online de las entidades. Volviendo al ejemplo inicial, la campaña de descrédito que sufre TUTIENDA.COM implica que su negocio se vea seriamente afectado al perder clientes.

Por último, es necesario tener en cuenta que la información en Internet no desaparece con el tiempo. La acción de los buscadores, que permite visualizar informaciones pasadas, puede tener consecuencias negativas sobre la valoración que los internautas tengan de las empresas, al hacer que determinados hechos sigan generando un impacto negativo, a pesar de estar solucionados. Un ejemplo destacado es el caso del camping Alfaques, que en julio de 2011 presentó una demanda a Google España por desplegar, entre los primeros resultados de búsqueda relacionados con el establecimiento, entradas que aluden a una tragedia ocurrida en 1978.

En este sentido, el llamado "derecho al olvido" que la sociedad reclama para las personas no es posible en el caso de las empresas, como se desarrolla en el apartado 5.2.

4.6 UTILIZACIÓN NO CONSENTIDA DE DERECHOS DE PROPIEDAD INDUSTRIAL

Caso 6: La hamburguesería LA SUPREMA descubre cómo una empresa de la competencia utiliza su imagen corporativa, modificándola con el lema *Una experiencia más que suprema*. Los dueños de LA SUPREMA recurren a ayuda legal para evitar que este acto siga suponiendo un perjuicio para su imagen y valoración en Internet.

Por último, se refleja el riesgo para la identidad y reputación de una empresa asociado con el uso por terceros no autorizados de los derechos de propiedad industrial. Entre estos derechos están las invenciones, los diseños industriales y los signos distintivos registrados (el nombre comercial y la marca).

Estos derechos tienen una doble dimensión: permiten a su propietario su utilización e impiden que un tercero lo haga, salvo que le ampare la correspondiente licencia de uso otorgada por el primero. Si se están utilizando o comercializando a través de Internet de forma no autorizada, la empresa propietaria de sus derechos se convertiría en víctima de un delito contra los derechos de propiedad industrial y posiblemente, en un delito de competencia desleal (Ver capítulo 5 MARCO LEGAL).

Así, en Internet resulta relativamente sencillo copiar, modificar y reutilizar contenidos que forman parte de la propiedad industrial de la empresa, como por ejemplo, utilizar un logotipo o una imagen de marca ajenos.

Por ejemplo, Coca-Cola vio afectados estos derechos cuando un internauta utilizó sus signos distintivos para crear una página de la marca en Facebook. La página, al obtener rápidamente millones de *"fans"*, hizo que una parte significativa de la relación empresa-consumidor y de la imagen de la marca estuvieran bajo el control de un tercero. La empresa, que hasta el momento no tenía página en la red social, aprovechó esta

situación para generar una respuesta positiva, contratando al internauta que utilizó indebidamente la marca. Este pasó a convertirse en administrador de la página[20].

Estos actos pueden estar motivados por una falsa sensación de que en Internet todo vale y no se vulnera ningún derecho, aunque también puede utilizarse por empleados descontentos y terceros malintencionados para divulgar elementos fundamentales para el negocio, como patentes o secretos industriales. En todo caso, este riesgo puede conllevar un impacto negativo para la identidad de la empresa en Internet y para su prestigio, ya que atenta contra los elementos que más caracterizan a la empresa de cara a sus consumidores y usuarios.

[20] Fuente: Guillaume Perret: "La protección de la propiedad Industrial e Intelectual en Internet". Disponible en: http://www.asociacion-eurojuris.es/publicaciones/la-proteccion-de-la-propiedad-industrial-e-intelectual-en-internet/

5. Marco legal

La empresa que haya visto dañada su reputación online tiene a su disposición una serie de herramientas que la legislación española contempla para que su imagen se vea reparada.

El análisis de la normativa que afecta a la reputación online no difiere sustancialmente del que se haría al considerar la imagen y reputación corporativa en el mundo offline. La Red no altera el contenido esencial de los derechos de las personas jurídicas.

Sin embargo, sí existen particularidades específicas derivadas del entorno online que las empresas deben tener en cuenta a la hora de gestionar su reputación:

- En primer lugar, el daño derivado del ataque a la reputación de una empresa realizado a través de Internet es difícilmente reparable de manera total. La difusión de una información publicada en la Red no tiene límites y, aun en el caso de que la información en cuestión sea retirada (por contravenir los derechos de la empresa), siempre se pueden mantener copias, pantallazos o descargas realizados antes de la eliminación.

- En segundo lugar, y relacionado con lo anterior, las empresas deben considerar el llamado "efecto *Streisand*"[21], fenómeno en el que un intento de ocultamiento de cierta información en Internet resulta siendo contraproducente, ya que ésta acaba siendo ampliamente divulgada, recibiendo mayor publicidad de la que habría tenido si no se la hubiese pretendido acallar.

5.1 DERECHO AL HONOR DE LAS EMPRESAS Y ACCIONES LEGALES PARA SU DEFENSA

El punto de partida del análisis se sitúa en el artículo 18 de la Constitución española, que reconoce el derecho al honor, a la intimidad personal y familiar y a la propia imagen.

El tribunal Constitucional incluye a las empresas y organizaciones entre los titulares del derecho al honor, esto es, a la reputación corporativa. Así, reconoce expresamente que *la persona jurídica también puede ver lesionado su derecho al honor a través de la divulgación de hechos concernientes a su entidad, cuando la difame o la haga desmerecer en la consideración ajena*.[22]

Por tanto, las empresas y organizaciones, en defensa de su derecho al honor, pueden iniciar acciones civiles o penales para solicitar la retirada de la Red de informaciones que produzcan un perjuicio a su reputación. En la mayoría de las ocasiones nos encontraremos ante supuestos donde entran en conflicto, de un lado, el derecho al honor

[21] Más información: http://es.wikipedia.org/wiki/Efecto_Streisand

[22] Sentencia del Tribunal Constitucional 139/1995.

de la empresa cuya reputación ha sido dañada y, de otro, el derecho a la libertad de expresión e información, recogidos en el artículo 20 de la Constitución española, que ampararían al autor de las informaciones.

Así, las empresas pueden recurrir a normativa específica para salvaguardar su imagen. En concreto, de manera no exhaustiva:

- Ley Orgánica 1/1982, de 5 de mayo, de Protección Civil del derecho al honor.
- Ley Orgánica 2/1984, de 26 de marzo, sobre el derecho de rectificación.
- Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico (LSSI).
- Ley 3/1991, de 10 de enero, de Competencia desleal.
- Código penal, artículos 205 a 216, que regula los delitos contra el honor (calumnias e injurias).

A continuación se realiza un tratamiento individualizado de cada uno de los textos en lo que afecta a la reputación online corporativa.

Ley Orgánica 1/1982, de 5 de mayo, de Protección Civil del derecho al honor

La LO 1/1982 protege a las empresas frente a todo género de intromisiones ilegítimas que pudieran menoscabar su reputación, tanto en el mundo físico como en el entorno online.

La entidad que vea afectado su honor (por ejemplo, a través de comentarios falsos publicados por un usuario online) podrá iniciar un proceso civil ordinario con la finalidad de que se adopten las medidas necesarias para que se ponga fin a la intromisión ilegítima.

Ley Orgánica 2/1984, de 26 de marzo, sobre el derecho de rectificación

El art. 1 de la LO 2/1984 manifiesta: *Toda persona, natural o jurídica, tiene derecho a rectificar la información difundida, por cualquier medio de comunicación social, de hechos que le aludan, que considere inexactos y cuya divulgación pueda causarle perjuicio*.

Se trata de una acción (compatible con la de la LO 1/1982) que tiene por único objetivo la publicación de la rectificación de la información que puede afectar a la reputación de la empresa o, en su caso, su denegación. Por este motivo, la doctrina considera que se

trata realmente de un *derecho de réplica*, más que de un derecho de rectificación en sentido estricto.

El ejercicio de este derecho se limita a informaciones difundidas por los medios de comunicación social, con lo que se excluyen, por ejemplo, opiniones vertidas en un foro de consumidores y usuarios, y plantean dudas casos como los blogs, ¿deben ser considerados medios de comunicación social?

Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico (LSSI)

Esta ley, transposición al ordenamiento jurídico español de la directiva 2000/31/CE del Parlamento Europeo y del Consejo, de 8 de junio, regula el régimen de responsabilidad de los prestadores de servicios que actúan como intermediarios de la Sociedad de la Información, permitiendo atribuirles responsabilidad civil por intromisiones al derecho al honor.

En el caso que nos ocupa, se trataría de determinar la responsabilidad de los prestadores de servicios de alojamiento o almacenamiento de datos por la información almacenada o alojada en sus servidores, con contenidos que vulneran el derecho al honor de una empresa.

El art. 16 de la Ley 34/2002 exime de responsabilidad a los prestadores de servicios siempre *que no tengan conocimiento efectivo de que la actividad o la información es ilícita o lesiona bienes o derechos de un tercero susceptibles de indemnización o, si lo tienen, actúen con diligencia para retirar los datos o hacer imposible el acceso a ellos*.

La clave, por tanto, está en probar el *conocimiento efectivo* que el prestador de servicios tiene o no. En la definición de *conocimiento efectivo* debe tenerse en cuenta la jurisprudencia del Tribunal Supremo.[23]

[23] En especial, deben considerarse el caso SGAE (Sentencia TS nº 773/2009) y el caso Quejasonline (Sentencia TS nº 316/2010)

Ley 3/1991, de 10 de enero, de Competencia desleal y Ley 17/2001, de 7 de diciembre, de Marcas

La ley tiene por objeto la protección de la competencia en interés de todos los que participan en el mercado, y a tal fin establece la prohibición de los actos de competencia desleal. En el caso que nos ocupa, el estudio legal de los ataques al honor de la empresa, los tribunales españoles en ocasiones han recurrido a la Ley de Competencia desleal en casos de utilizaciones fraudulentas de nombres de dominio (ver apartado 4.2 REGISTRO ABUSIVO DE NOMBRES DE DOMINIO) En otros casos, se han decantado por evaluar la utilización de los nombres de dominio en relación con el signo distintivo afectado, aplicando la ley de Marcas.

La práctica de cibersquatting o su variante typosquatting puede afectar a la identidad y reputación en Internet de una empresa. Imaginémonos, por ejemplo, que el ocupador reproduce la imagen corporativa, diseño y contenidos del sitio original, creando un sitio web clonado que además tendrá un nombre de dominio muy parecido. El internauta puede llegar a interactuar con el sitio web falso pensando que se trata del original. Así, se han conocido casos de laboratorios farmacéuticos, que han visto cómo terceros utilizaban dominios con permutaciones de sus marcas protegidas, con la intención de vender productos médicos. También el sector turístico español se ha visto afectado por prácticas de cibersquatting, con ocupaciones de dominios de agencias de viaje importantes, con intención de desviar las visitas a los sitios falsos, que ofrecen ofertas similares.

En estos casos, ¿se puede exigir responsabilidad jurídica al atacante, de acuerdo con la legislación española de competencia desleal? La Ley de Competencia desleal establece que *se reputa desleal todo comportamiento que resulte objetivamente contrario a las exigencias de la buena fe*, y regula específicamente supuestos en los que se genera confusión y explotación de la reputación ajena.[24]

[24] Art. 6: se considera desleal todo comportamiento que resulte idóneo para crear confusión con la actividad, las prestaciones o el establecimiento ajenos.

Art. 12: Se considera desleal el aprovechamiento indebido, en beneficio propio o ajeno, de las ventajas de la reputación industrial, comercial o profesional adquirida por otro en el mercado. En particular, se reputa desleal el empleo de signos distintivos ajenos o de denominaciones de origen falsas acompañados de la indicación acerca de la verdadera procedencia del producto o de expresiones tales como modelos, sistema, tipo, clase y similares.

Los Tribunales españoles también han optado por aplicar la normativa reguladora de los signos distintivos, es decir, la Ley 17/2001, de Marcas. Así en el artículo 34.3 e) de la norma se considera absolutamente prohibida la utilización de la denominación de una marca en forma de nombre de dominio, sin el consentimiento del legítimo titular de la marca.

Existen, por último, procedimientos extrajudiciales para la recuperación de dominios. Cuando se trata de dominios ".es", la entidad pública empresarial Red.es ha desarrollado un procedimiento para la recuperación de dominios. Para el resto de los casos, la ICANN (*Internet Corporation for Assigned Names and Numbers*) ha definido una serie de políticas para la resolución de disputas sobre el registro y el uso de nombres de dominio. Se profundiza en ellos en el apartado 6.2.4, al ofrecer recomendaciones de actuación a las empresas que hayan sido víctimas de cibersquatting.

Código penal, artículos 205 a 216, que regulan los delitos contra el honor (calumnias e injurias)

En determinadas circunstancias, las actuaciones que vulneren el honor y la reputación online de una empresa pueden ser constitutivas de delito. El Código penal regula en sus artículos 205 a 216 los delitos contra el honor. Así:

- *Es calumnia la imputación de un delito hecha con conocimiento de su falsedad o temerario desprecio hacia la verdad* (artículo 205 del Código penal).
- *Es injuria la acción o expresión que lesionan la dignidad de otra persona, menoscabando su fama o atentando contra su propia estimación* (artículo 208 del Código penal).

De considerarse la existencia de un delito de calumnia, la condena puede implicar una pena de prisión de hasta dos años para el acusado.

5.2 ¿DERECHO AL OLVIDO DE LAS EMPRESAS?

El derecho al olvido puede definirse, de acuerdo con Ricard Martínez, como la facultad que se atribuye al individuo de obtener la eliminación de una determinada información, particularmente en el contexto de Internet.

¿Puede una persona jurídica solicitar que sea eliminada de Internet cierta información que afecta de manera negativa a su reputación? Se trataría, por ejemplo, del caso analizado en el apartado 4.5 PUBLICACIONES POR TERCEROS DE INFORMACIONES NEGATIVAS, en el que el camping Alfaques presentó una demanda a Google España por vulneración del derecho al honor. El camping alegaba que el buscador no aplicaba el derecho al olvido, ya que los primeros resultados de la búsqueda de *camping Alfaques* son entradas referidas a una tragedia ocurrida en 1978, cuando murieron 243 personas. La demanda fue desestimada, ante el argumento de Google España que defiende la neutralidad del algoritmo responsable del despliegue de los resultados.

En estos momentos, el derecho al olvido no existe como tal en el ordenamiento jurídico español, y solo es posible obtener cierto "olvido" a través de las herramientas que proporciona el derecho fundamental a la protección de datos, esto es, derecho de oposición al tratamiento que buscadores, proveedores de contenidos y medios de comunicación hacen de los datos *personales*. Ahora bien, el derecho a la protección de datos ampara exclusivamente a las personas físicas… ¿qué ocurre con las empresas?

> *Las organizaciones no se privilegian del derecho a la protección de datos de carácter personal, aplicable solo a las personas físicas.*

Por tanto, en la práctica, las empresas que quieran que se retire una información sobre ellas solo podrían hacerlo si esa información vulnera su derecho al honor, y en ese caso tendrían a su disposición las acciones que el Derecho español pone a su disposición, analizadas en el apartado 5.1 DERECHO AL HONOR DE LAS EMPRESAS Y ACCIONES LEGALES PARA SU DEFENSA.

6. Recomendaciones para la gestión de la identidad digital y reputación online

Una identidad digital adecuada y una reputación online sana requieren implicación y dedicación. Ofrecemos a continuación una serie de pautas preventivas de gestión, que contribuyen a construir una imagen sólida de la empresa, y pautas de reacción, que pueden ayudar a la empresa que vea vulnerada su reputación online.

6.1 RECOMENDACIONES PREVENTIVAS

La construcción de una identidad digital empresarial robusta y solvente, que permita que los usuarios perciban la imagen que la empresa desea transmitir, requiere un trabajo constante. Las siguientes pautas de actuación pueden ayudar a las organizaciones a gestionar su reputación online de manera integral.

Estrategia de identidad corporativa	• Definir los objetivos en materia de identidad corporativa. • Diseñar una imagen de marca coherente. • Seleccionar el nombre de dominio. • Aportar los recursos materiales y humanos necesarios (Community Manager). • Formar y promover la implicación de los miembros de la organización.

Interacción con usuarios	• Establecer una política de interacción con usuario que contemple:
	  • Hábitos de respuesta y diálogo.
	  • Tono empleado en la relación.
	  • Mensaje a ofrecer a usuarios.
	  • Existencia de control previo, moderación o denuncia.
	• Aportar los recursos materiales y humanos necesarios (Community Manager).

Cumplimiento normativo	• Cumplir estrictamente la normativa relativa a:
	  • Comercio electrónico y servicios de la sociedad de la información.
	  • Protección de datos de carácter personal.
	  • Propiedad industrial e intelectual.

Medidas de seguridad	• Prever posibles escenarios de crisis y los procedimientos de respuesta. • Considerar los aspectos reputacionales de la empresa (junto con los técnicos) en las políticas de continuidad del negocio.
Monitorización y seguimiento	• Realizar un seguimiento efectivo de la reputación online de la empresa.

6.1.1 Definición de una estrategia de identidad corporativa

El primer paso para la gestión efectiva de la reputación de una empresa en Internet es que exista una estrategia clara por parte de la organización respecto a la definición de una identidad corporativa. ¿Qué somos como empresa?, ¿qué queremos ser? Son preguntas que la organización debe responderse, y definir actuaciones coherentes dentro y fuera de la Red.

En concreto, la empresa debe:

- Definir sus objetivos en materia de identidad digital.
- Diseñar una imagen de marca coherente.
- Seleccionar un nombre de dominio adecuado a su denominación social, marca o fines perseguidos. Se recomienda proteger el nombre de dominio con las herramientas que otorga el Derecho de propiedad intelectual e industrial, en las distintas jurisdicciones en la que se opere.
- Poner al servicio de la identidad digital los recursos materiales y humanos necesarios para ello, y en concreto la figura del Community Manager.
- Formar e implicar a todos los miembros de la empresa para que estén alineados con la estrategia corporativa de identidad digital. Por ello, al margen de la existencia de un Community Manager, es recomendable que los empleados conozcan las pautas de actuación y reglas de comportamiento cuando actúan en representación (formal o informal) de la empresa, y que sean respetuosos en el cumplimiento de las cláusulas de confidencialidad.

6.1.2 Interacción con los usuarios

La interacción con los usuarios en un entorno abierto como es la Web 2.0 permite el establecimiento de relaciones de confianza basadas en el diálogo, pero también expone a la empresa a las críticas de manera más abierta.

Ello obliga a las empresas a considerar una serie de pautas:

- Definir qué modelos de comunicación desea adoptar en la interactuación con los usuarios en las plataformas colaborativas. En concreto, la empresa debe reflexionar acerca de, al menos, los siguientes aspectos, que constituirán el *social media policy* de la organización:

    - ¿En qué casos se va a proporcionar respuesta a los usuarios?, ¿qué tipo de respuesta –personalizada, pública, privada- se va a ofrecer?, ¿la empresa o marca "dialoga" con sus seguidores?

    - ¿Qué tono va a utilizar –amigo, experto, etc.– en la relación con los usuarios?

    - ¿Qué mensaje desea transmitir la empresa a sus seguidores?

    - ¿Qué tipo de control –filtro previo, moderación posterior, etc. – se va a hacer de los comentarios realizados por los usuarios? ¿y qué canales de denuncia se establecen?

- Contar con el personal adecuado es clave. La figura del Community Manager permite hacer un seguimiento de las opiniones o denuncias manifestadas en el espacio y su gestión, dando respuesta y generando conversación con los usuarios y seguidores.

6.1.3 Cumplimiento normativo

La imposición de una sanción derivada del incumplimiento normativo tiene importantes efectos sobre la reputación online de la empresa. Por ello, el cumplimiento de la legislación aplicable al entorno digital es absolutamente clave para la buena salud de la reputación de una organización.

En concreto, resultan especialmente importantes los siguientes aspectos:

- Observar la legislación de comercio electrónico y servicios de la Sociedad de la Información: políticas de compra, contratación, información y derechos del consumidor; políticas de envío de comunicaciones comerciales, etc.

- Cumplir la normativa de protección de datos[25]: registro de ficheros, deber de información y solicitud de consentimiento, garantía de ejercicio de los derechos

[25] La Agencia Española de Protección de Datos ofrece la herramienta Evalúa, programa sencillo, anónimo y gratuito que permite a las empresas autoevaluar el grado de cumplimiento de la Ley Orgánica de Protección de Datos. Asimismo, se recomienda a las empresas la lectura de la Guía del responsable de ficheros, disponible en: http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/pdfs/guia_responsable_ficheros.pdf.

ARCO a los usuarios, implantación de medidas de seguridad de los datos, diseño de políticas de privacidad, establecimiento de contratos con terceros encargados del tratamiento de la información, formación de los empleados, etc.

- Acatar las reglas de protección de la propiedad intelectual, incluyendo el establecimiento de derechos de los usuarios y la implementación, si procede, de licencias *Creative Commons*.

6.1.4 Adopción de medidas de seguridad

La experiencia de ser víctima de un ataque informático puede tener graves consecuencias para la reputación corporativa. Por ello, es recomendable que las empresas prevean esta circunstancia cuando se trata de adoptar medidas de seguridad:

- Contemplar escenarios de crisis y procedimientos de respuesta: sistemas de denuncia y notificación de quiebras de seguridad; mecanismos de respuesta rápida ante las críticas; procedimientos de atención a peticiones, etc.

- Disponer de políticas de continuidad del negocio y recuperación ante desastres, que abarquen no sólo aspectos técnicos, sino también de organización y reputacionales, orientados hacia la adopción, implementación y certificación de un Sistema de Gestión de la Seguridad de la Información.

6.1.5 Monitorización y seguimiento de la reputación online

La presencia en Internet obliga a desarrollar estrategias de monitorización. En este sentido, es conveniente realizar un seguimiento constante y efectivo de la reputación de la empresa en Internet.

La verificación debe abarcar aspectos de relevancia (es decir, cuál es la posición de la empresa en los resultados ofrecidos por los buscadores en la búsqueda de materias relacionadas con las áreas de especialización de la organización o marca) y de contenido (signo positivo o negativo de la información destacada por los buscadores). En el análisis no se deben descuidar las informaciones publicadas en foros de consumidores, medios de comunicación, sitios especializados, redes sociales, etc.

6.2 RECOMENDACIONES REACTIVAS

¿Qué ocurre cuando la empresa experimenta una crisis de reputación online o es víctima de alguna situación que exige una reacción inmediata? A continuación se indican una serie de recomendaciones a seguir en estos casos:

Crisis de reputación online	• Detectar el incidente y avisar a la organización. • Evaluar el incidente ante el gabinete de crisis. • Poner en práctica acciones inmediatas para contener el incidente. • Planificar actuaciones de acompañamiento para garantizar la estabilidad en el futuro.
Canales de denuncia internos	• Reportar ante los proveedores de servicios de medios sociales los incidentes relacionados con la identidad y reputación online.
Acciones legales	• Iniciar acciones legales, por vía civil o penal, siempre que la actuación que vulnera la reputación online de la empresa constituya un ilícito.
Recuperación del nombre de dominio	• Si el dominio es ".es", solicitar el inicio del procedimiento de resolución extrajudicial de conflictos desarrollado Red.es. • Para el resto de dominios, solicitar el inicio del procedimiento equivalente de la ICANN. • Acudir ante la jurisdicción ordinaria, invocando la legislación sobre competencia desleal o sobre marcas.

Los siguientes epígrafes profundizan en cada una de estas recomendaciones.

6.2.1 Hoja de ruta frente a una crisis online

Uno de los episodios que más preocupa a las empresas es sufrir una crisis online, debido a la dificultad para controlar el incidente y las repercusiones para su reputación online, aumentadas por la viralidad de Internet.

A continuación, se proponen una serie pautas de actuación a poner en práctica cuando "estalla" la crisis en Internet, coordinadas por la figura del Community Manager de la organización. Es necesario aclarar que la siguiente hoja de ruta es orientativa, por lo que propuestas similares adaptadas a las circunstancias particulares de cada empresa pueden ser igualmente válidas. En todo caso, se trata de un patrón u orientación de cara a diseñar e implantar una estrategia interna que permita afrontar satisfactoriamente una situación grave de descrédito en medios sociales.

Esquema de actuación frente a una crisis online

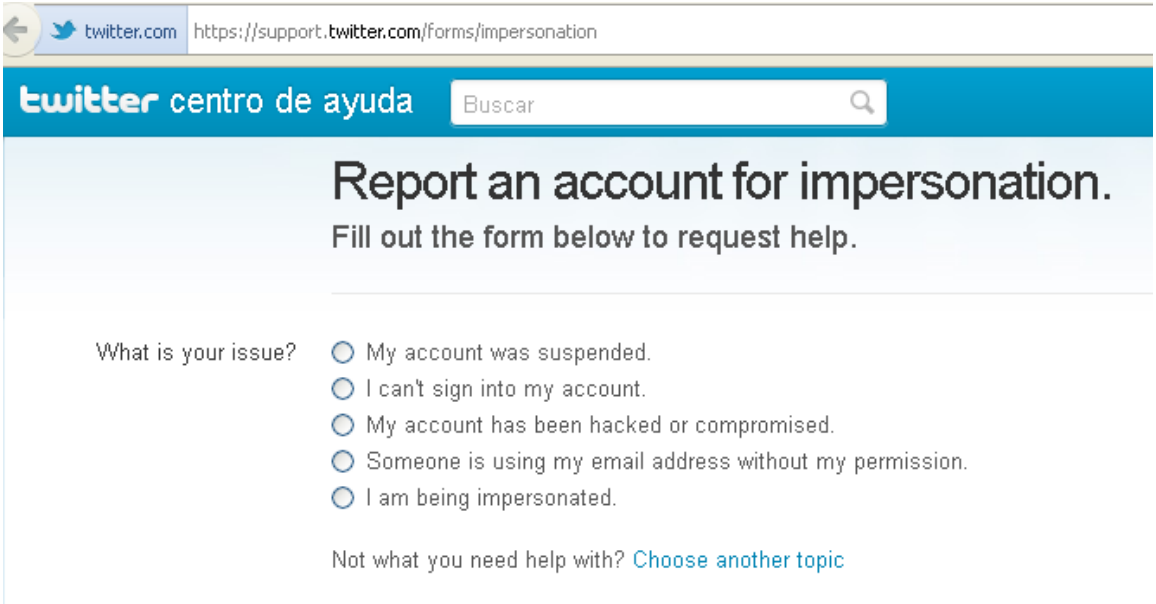
Fase	Descripción	Tiempo estimado	Responsable
FASE INICIAL	• Detección del incidente y recopilación de datos • Inicio del protocolo de gestión de la crisis: Alerta interna • Preparación de informe de situación	Antes de 6 horas	Community Manager
FASE DE EVALUACIÓN DEL INCIDENTE	• Reunión del gabinete de crisis • Presentación del informe de situación • Principales pasos a seguir • Tareas y planificación	A las 6 horas como máximo	Gabinete de Crisis (Community Manager, Dirección, Dpto. Comunicación, otros Dptos.)
FASE DE CONTENCIÓN (ACCIONES INMEDIATAS)	• Resolución de errores, si los hubiera • Actuación de denuncia • Publicación de respuesta oficial en canales propios • Respuestas individualizadas a los usuarios de redes sociales	Antes de 24 horas	Community Manager, Dpto. Comunicación
FASE DE ESTABILIZACIÓN (ACCIONES POSTERIORES)	• Publicación de hechos y respuesta oficial en medios de comunicación • Monitorización exhaustiva	A partir de 24 horas	Community Manager, Dpto. Comunicación

Fuente: INTECO

6.2.2 Utilización de canales de denuncia internos

Las plataformas colaborativas desarrollan herramientas específicas informativas y de denuncia para la gestión reactiva frente a incidentes que afecten a la imagen y reputación corporativas en medios sociales.

Por ejemplo, Twitter dispone de una *Política de usurpación de identidad* en la que identifica qué considera suplantación de la identidad de personas y empresas. Asimismo, proporciona un formulario para reportar este incidente y que el proveedor pueda comprobar los datos y devolver la cuenta a su legítimo titular.



Formulario de denuncia de suplantación de perfil de Twitter

Estos canales de denuncia internos suponen el primer paso a la hora de reaccionar a un incidente, pudiendo ser complementados con las denuncias ante órganos judiciales y Fuerzas y Cuerpos de Seguridad del Estado.

6.2.3 Denuncia judicial frente a atentados a la reputación

En el apartado 5.1 DERECHO AL HONOR DE LAS EMPRESAS Y ACCIONES LEGALES PARA SU DEFENSA se han identificado las herramientas legales de ámbito civil y penal que las empresas pueden utilizar en caso de ver vulnerado su derecho al honor. Se recomienda, por tanto, analizar la situación desde el punto de vista jurídico e iniciar las acciones que, en cada caso, procedan.

Las Fuerzas y Cuerpos de Seguridad del Estado español disponen de unidades especializadas en delitos informáticos. Así, El Cuerpo Nacional de Policía cuenta con la

Brigada de Investigación Tecnológica[26] y la Guardia Civil dispone de efectivos especialistas en el Grupo de Delitos Telemáticos[27].

6.2.4 Recuperación del nombre de dominio

En caso de que un tercero haya ocupado un dominio sin autorización debe procederse a su reclamación. Para ello, se contemplan diferentes vías:

- En primer lugar, respecto de los dominios ".es" existe un procedimiento de resolución extrajudicial de conflictos desarrollado y coordinado por la Entidad Pública Empresarial Red.es[28]. Para poder iniciar esta reclamación arbitral es necesario acreditar estar en posesión de derechos previos sobre la denominación y justificar la mala fe del dominio registrado en lugar del que reivindicamos.

- En segundo lugar, existe un procedimiento equivalente de la ICANN, denominado política uniforme de resolución de conflictos (UDRP)[29], que contempla una serie de entidades internacionales acreditadas para realizar el arbitraje[30].

- También es posible acudir ante la jurisdicción ordinaria invocando la legislación sobre competencia desleal o sobre marcas, según lo dispuesto en el apartado 5.1.

[26] Disponible en: http://www.policia.es/colabora.php

[27] Más información en: https://www.gdt.guardiacivil.es/webgdt/pinformar.php

[28] Más información en: http://www.nic.es/procedimiento/article/1480 .

[29] Para más información, ver: http://www.icann.org/es/udrp

[30] Más información en: http://www.icann.org/en/dndr/udrp/approved-providers.htm

7. Bibliografía

- ANTONI RUBÍ (2010). *Derecho al honor online y responsabilidad civil de ISPs*. Indret. Revista para el análisis del Derecho. http://www.indret.com/pdf/776_es.pdf
- ANTONIO FUMERO, GENÍS ROCA y JESÚS ENCINAR (2007). *Web 2.0*. Fundación Orange España. http://fundacionorange.es/areas/25_publicaciones/publi_253_11.asp
- ARTEMI RALLO Y RICARD MARTÍNEZ (coord.) (2010). *Derecho y redes sociales*. Civitas, Cizur Menor.
- COMISIÓN EUROPEA (2011). *Safer Social Networking Principles for the EU*. http://ec.europa.eu/information_society/activities/social_networking/eu_action/implementation_princip_2011/index_en.htm
- EVA ANTÓN (2011). *Reputación online. Beneficios para las empresas*. Prestigia Online http://www.prestigiaonline.com/blog/wp-content/uploads/2008/09/reputacion-online.pdf
- FUNDACIÓN BANESTO en colaboración con el MINISTERIO DE INDUSTRIA TURISMO Y COMERCIO y la EMPRESA NACIONAL DE INNOVACIÓN (ENISA) (2011). *Observatorio sobre el uso de las redes sociales en las PYMEs españolas*. http://www.inteco.es/studyCategory/Seguridad/Observatorio/Biblioteca/observatorio_redes_sociales_FB
- INTECO (2010) *Botnet, ¿qué es una red de ordenadores zombis?* http://www.inteco.es/Seguridad/Observatorio/Articulos/Articulo_botnet
- INTECO (2012) *Estudio sobre seguridad de la información y continuidad de negocio en las empresas españolas* http://www.inteco.es/Seguridad/Observatorio/Estudios/Estudio_pymes_seguridad_2012
- JOSE RAMÓN LÓPEZ (2009). *Los conflictos entre los nombres de dominio y las marcas. El Cybersquatting.* http://bloguerlaw.blogspot.com.es/2009/04/los-conflictos-entre-los-nombres-de.html
- MICHAEL PETRI (2010). *Identidad Digital*.
- MIGUEL ÁNGEL HERNÁNDEZ (2011). *Delitos Informáticos en el Código penal Español* http://www.miguelangelhernandez.es/Articulos/DICPE.pdf
- ÓSCAR DEL SANTO (2011). *Reputación Online para Tod@s: 10 lecciones desde la trinchera sobre tu activo más importante*. http://www.oscardelsanto.com/reputacion-online-para-tods/

❖ VARIOS AUTORES *Identidad Digital y Reputación Online*. Evoca. *Cuadernos de comunicación*. http://www.evocaimagen.com/cuadernos/cuadernos5.pdf

Síguenos a través de:

Web

Envíanos tus consultas y comentarios a:

observatorio@inteco.es

Instituto Nacional
de Tecnologías
de la Comunicación