E-BOOK GUÍAS TIC

GUÍA DE CIBERSEGURIDAD Y REPUTACIÓN ONLINE PARA DESPACHOS DE ABOGADOS

Abogacía Española
CONSEJO GENERAL

incibe_

1 INTRODUCCIÓN

1.1 - ¿Por qué los despachos de abogados entran en redes sociales?

1.2 - La identidad digital

2 LA REPUTACIÓN *ONLINE*

3 RIESGOS EN LA GESTIÓN DE LA IDENTIDAD DIGITAL Y LA REPUTACIÓN *ONLINE*

3.1 - Suplantación de identidad

3.2 - Registro abusivo de nombre de dominio

3.3 - Ataques de denegación de servicio DDoS

3.4 - Fuga de información

3.5 - Publicaciones por terceros de informaciones negativas

3.6 - Utilización no consentida de derechos de propiedad industrial

4 MARCO LEGAL

4.1 - Derecho al honor de las empresas y acciones legales para su defensa

4.2 - ¿Derecho al olvido de los despachos de abogados?

5 RECOMENDACIONES PARA LA GESTIÓN DE LA IDENTIDAD DIGITAL DEL DESPACHO Y DE SU REPUTACIÓN *ONLINE*

5.1 - Recomendaciones preventivas

- 5.1.1 - Definición de una estrategia de identidad corporativa
- 5.1.2 - Interacción con los usuarios
- 5.1.3 - Redes Sociales
- 5.1.4 - Cumplimiento normativo
- 5.1.5 - Adopción de medidas de seguridad
- 5.1.6 - Monitorización y seguimiento de la reputación *online*

5.2 -Recomendaciones reactivas

- 5.2.1 - Utilización de canales de denuncia internos
- 5.2.2 - Denuncia judicial frente a atentados a la reputación
- 5.2.3 - Recuperación del nombre de dominio

1 Introducción

En el actual entorno digital cobran especial importancia la comunicación, la publicidad y las relaciones públicas

- Los despachos de abogados son cada vez más conscientes de la importancia de la comunicación a través de medios digitales

- La identidad digital corporativa es el conjunto de información sobre un despacho expuesta en Internet

Por todos es sabido que la identidad corporativa ha sido, tradicionalmente, un elemento que permite a los despachos de abogados diferenciarse de los demás.

En el actual entorno digital e interconectado, en el que también se encuentra la abogacía, **cobra especial importancia la comunicación, la publicidad y las relaciones públicas.** Y, dentro de estos aspectos, pueden destacarse extremos como la inmediatez, la visibilidad, la credibilidad, la influencia y la permanencia de la información.

Por eso es cada vez más importante para los despachos de abogados crearse una identidad digital corporativa basada en una estrategia de comunicación sólida, gracias a la cual logren alcanzar un buen posicionamiento en el entorno digital, para poder –de este modo- comunicarse mejor con sus clientes (actuales y potenciales), proveedores, colegios, organismos e instituciones, y público en general.

Además de por un uso acertado del correo electrónico y de la mensajería instantánea, contribuyen de forma destacada a este objetivo de lograr una adecuada identidad digital corporativa del despacho su presencia en Internet mediante una página web, y la actividad en las redes sociales (Twitter, Facebook, Pinterest, LinkedIn…), tanto del propio despacho como de algunos o todos sus integrantes (abogados, socios, juniors…).

En el momento actual puede afirmarse que **los despachos de abogados son cada vez más conscientes de la importancia de la comunicación a través de medios digitales,** motivo por el cual utilizan las redes sociales con mayor habitualidad y profesionalidad. De hecho, algunos utilizan los medios sociales planificando previamente su estrategia de comunicación en ellos, sabedores del potencial y de la eficacia de estos canales, que permiten a los despachos construir, mediante la interacción con clientes y otros agentes, su "marca social" de forma colaborativa.

La reputación *online* del despacho se convierte, así, **en una medida de la opinión que los demás tienen de la marca en el mundo digital.** Y para lograr la sostenibilidad de este reconocimiento suele ser fundamental que incluya valores del tipo: actualidad, relevancia, confianza, credibilidad, seguridad, respeto, transparencia y honestidad. En este sentido, las redes sociales son un perfecto termómetro para que los despachos puedan medir su reputación en la red, por lo que es aconsejable monitorizar lo que se dice de nuestra marca, con independencia de que hayamos decidido no tener una presencia activa en dichas redes.

1.1 ¿Por qué los despachos de abogados entran en redes sociales?

Las motivaciones que mueven a aquellos a tener presencia en estos medios son diversas.

En primer lugar, las redes sociales representan **una de las vías más importantes de promoción** de los productos o servicios del despacho, ya que permiten lograr una mayor y más rápida llegada al público a un menor coste.

En segundo lugar, la presencia de los abogados en redes sociales **mejora la difusión de la propia actividad** y la comunicación con el cliente y con otros profesionales e instituciones.

Y es que la presencia en redes sociales brinda a los despachos de abogados numerosas ventajas. En efecto, si lo comparamos con los medios tradicionales, las redes sociales **permiten acercarse a los clientes objetivo y dialogar con ellos**.

Pero también los despachos deben ser conscientes y valorar los posibles riesgos derivados de su incursión en los medios sociales (correo electrónico, pagina web, redes sociales…).

De ahí surge un nuevo 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 actividad normal del negocio, sino también pérdidas económicas, de imagen y reputación *online*. En este sentido, todo despacho se debe preguntar qué hacer en el caso de sufrir una suplantación de su identidad en la red, o cómo debe proceder si alguien ajeno al despacho (o relacionado con aquél) publica una información negativa sobre el mismo.

El objetivo que persigue la presente guía es el de desarrollar un análisis riguroso de los conceptos de identidad digital y reputación *online* en el ámbito de los despachos de abogados 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***.

1.2 La identidad digital

Hoy en día, los despachos de abogados y organizaciones colegiales difunden su imagen en Internet mediante herramientas tales como páginas web, blogs, perfiles y páginas en redes sociales.

Pero más allá de lo que la propia organización publique y dé a conocer de sí misma, la identidad digital corporativa se ve complementada con las opiniones de los terceros, esto es, lo que los propios colegiados y clientes opinan en Internet sobre el despacho y sobre los profesionales que lo componen. Ni siquiera es necesario que un despacho o un abogado tengan presencia activa en Internet para que puedan surgir este tipo de opiniones sobre él. Así pues, puede concluirse que el contenido generado por terceros forma parte de su identidad digital de la misma manera que el creado por el propio despacho y sus integrantes.

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

«La identidad digital corporativa se ve complementada con lo que los propios usuarios y clientes opinan sobre el despacho y sobre sus abogados en Internet»

La web constituye un nuevo canal masivo de comunicación para cualquier despacho y profesional, y las redes sociales representan una herramienta mediante la cual aquellos disponen de un valioso *feedback* en tiempo real de clientes y usuarios.

2 La reputación *online*

La reputación *online* es la valoración alcanzada por una empresa derivada del uso de las posibilidades de Internet

- La gestión es la fase transversal de la reputación *online* que comprende la fase de investigación y la de monitorización
- Cada vez son más los despachos que gestionan de forma profesional su identidad digital corporativa

La reputación corporativa es el concepto que mide cuál es la valoración que hace el público de una persona, física o jurídica. Esta definición es trasladable al mundo de Internet y a la denominada Web Social, también conocida como Web 2.0, donde aparece la idea de reputación *online* corporativa.

La reputación *online* puede definirse como **la valoración alcanzada por una empresa, derivada del uso, o del mal uso, de las posibilidades que ofrece Internet.**

Para entender la noción de reputación *online* de un despacho de abogados 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 una adecuada identidad digital para el despacho.

Investigación de la reputación *online* (Qué ocurrió)

La investigación consiste en un análisis retrospectivo de la reputación *online* de un despacho.

Este análisis se divide en dos fases:

a) Fase cuantitativa: ésta es la primera etapa de la investigación, en la cual se realizará un registro de las opiniones de los clientes y de los medios sobre el despacho que se encuentran disponibles en blogs, foros, redes sociales, etc.

b) Fase cualitativa: en esta segunda etapa se identifican las fortalezas y áreas a mejorar de la entidad, a través de las opiniones positivas y negativas, respectivamente.

«Cada vez son más los despachos que gestionan de forma profesional su identidad digital corporativa y su reputación en Internet»

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

La monitorización de la reputación *online* es el seguimiento regular de la identidad digital del despacho. Esta monitorización incluye el registro de las informaciones, los comentarios y opiniones que se generan en Internet sobre la organización, sus integrantes, sus servicios y actividades, sus valores, marcas comerciales, productos, personas y otros activos.

Esta tarea de gestión de la reputación *online* legal se apoya, cada vez más, en profesionales y 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 posicionamiento** en los motores de búsqueda (*Search Engine Optimization* o SEO), la gestión de las **comunicaciones en redes sociales** (SMO - *Social Media Optimization*) y **la gestión de los enlaces patrocinados** (*Search Engine Marketing*, comúnmente conocido como SEM), el marketing, 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 la construcción de una marca *online* (que viene siendo conocido en el sector como *Brand Reputation*).

Otro aspecto relevante en la gestión de la reputación de los despachos es el 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 Socio Director del despacho o un desliz de uno de los abogados revelando información sensible son ejemplos de situaciones que pueden poner en serio peligro el prestigio del despacho y de su marca.

Por último, la gestión de la reputación en Internet requiere de una estrategia que abarque la totalidad de áreas de negocio del despacho, comenzando por la dirección y pasando por la gestión con los clientes, proveedores, instituciones, incluso los procesos de selección interna.

Cada vez son más los despachos y otras organizaciones institucionales de la abogacía que gestionan de forma profesional su identidad digital corporativa y su reputación en Internet, tanto 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: el *Social Media Manager* o el *Community Manager*. Estos profesionales desempeñan un rol activo y especializado en la generación de "conversación" e interactuación desde los despachos, manteniendo una interlocución directa y constante con los clientes o usuarios[1].

[1] La Asociación Española de Responsables de Comunidades Online y Profesionales del Social Media (AERCO-PSM) es la asociación que aglutina a este tipo de profesionales en España. (www.aercomunidad.org).

3 Riesgos en la gestión de la identidad digital y la reputación *online*

Internet tiene un efecto multiplicador

- A la vez que la presencia en medios sociales reporta efectos positivos, existen amenazas que pueden generar efectos negativos en la imagen y reputación *online*
- Un incidente aislado se puede convertir en una situación de difícil solución

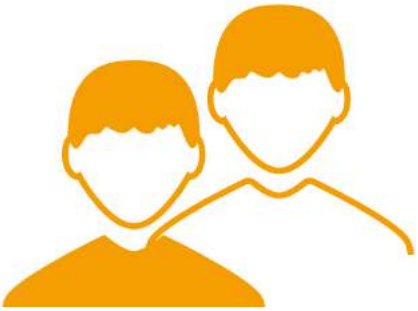
Al mismo tiempo que la presencia del despacho en medios sociales (por sí mismo o por la acción de terceros) **le reporta efectos positivos, existen diferentes amenazas que pueden generar impactos negativos en su imagen y reputación *online*.** Una pérdida de confianza en la marca a partir de comentarios perjudiciales sobre un servicio concreto de los que presta la organización 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 de reputación en Internet, las cuales impactan de tal forma en la imagen del despacho, y donde sus efectos pueden perdurar por largo tiempo. Por poner un ejemplo, podemos remitirnos al caso del despacho panameño Mossack Fonseca tras el incidente sufrido en el año 2015.

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.

3.1 Suplantación de identidad

Caso 1.



El despacho comienza a recibir numerosas quejas por parte de clientes y 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 redes sociales simulando ser nuestro despacho. En estos mensajes 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 el despacho, aunque no es el responsable, se ve inmerso en una grave crisis online.

La **suplantación de identidad del despacho en Internet** se produce, en este caso, mediante la usurpación de los perfiles corporativos por un tercero, quien pretende actuar, de forma ilícita, en su nombre. Este riesgo incluye la creación o el acceso no autorizado al perfil de la entidad en un medio social, así como la utilización del mismo como si se tratara de la organización suplantada.

En el caso que ahora nos ocupa, los atacantes crean perfiles falsos con varios propósitos, entre los cuales destaca el robo de información sensible de los clientes del despacho suplantado para la comisión de fraude *online*. Para ello, recurren a diferentes técnicas, entre las que destacan:

***Phishing*:** el estafador o *phisher* usurpa la identidad (correo electrónico, perfil en redes sociales…) del despacho para que el receptor de una comunicación electrónica aparentemente cierta (vía email, redes sociales, SMS, etc.) y confiando en su veracidad, facilite los datos privados (credenciales, cuentas, etc.) que resultan de interés para el estafador. Para dar credibilidad a la suplantación, suele utilizar 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.

***Pharming*:** el atacante modifica los mecanismos de resolución de nombres mediante los que el usuario accede a las diferentes páginas web por medio de su navegador. Esta modificación provoca que cuando el usuario introduce la dirección web legítima del despacho, automáticamente es dirigido hacia una página web fraudulenta que suplanta a la oficial.

Las consecuencias de la suplantación de la identidad de un despacho de abogados en Internet y de los ataques derivados de la misma pueden ser 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 el despacho, y por los abogados que lo componen, y también sobre su actividad, sus productos y servicios, tanto dentro como fuera de la red.

Estas conductas tienen implicaciones legales.

3.2 Registro abusivo de dominio

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

Los despachos de abogados tratan de identificarse adecuadamente ante su público eligiendo el nombre de dominio que coincida con sus signos distintivos, como el nombre comercial o la marca de sus productos o servicios.

El problema se origina durante el proceso de registro del nombre de dominio, ya que no existe un control previo por parte de las autoridades encargadas de dicho registro, a diferencia de lo que ocurre, por ejemplo, en el caso del registro de marcas 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 del despacho, impidiéndole utilizar dichas denominaciones en su negocio. Este ataque, conocido como ***cybersquatting***, también puede producirse si el despacho se olvida de renovar el nombre de dominio, o si aparece una nueva extensión TLD[2] (como ".info", ".abogado" o ".eu") y el propietario de la marca no realiza el correspondiente registro.

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

- **Atraer visitantes a la página web o blog** que han sido ilícitamente ocupados, aprovechándose de la reputación de la marca del despacho original. 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.

[2] *Top Level Domain*

Caso 2.

Los responsables del nuevo despacho han decidido crear la página web del bufete. Sin embargo, al intentar registrar el nombre de dominio, descubren que ya están ocupados tanto el dominio .com como el dominio .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.

«La amenaza se produce cuando terceros malintencionados registran uno o varios nombres de dominio que coinciden con la marca del despacho»

Por su parte, **el *typosquatting* es una variante del *cybersquatting***, que consiste en el registro de nombres de dominio parecidos a la marca registrada por el despacho en cuestión, explotando confusiones típicas al teclear o visualizar una dirección. Por ejemplo, resulta lógica la equivocación al escribir el nombre del despacho con una pequeña errata, tanto en su cuerpo principal como en el de la extensión del propio dominio.

Por tanto, ambas acciones, eventualmente ilícitas, plantean un conflicto entre los nombres de dominio y los signos distintivos del despacho: se produce un impacto, tanto en la identidad del despacho (al crear confusión en el nombre de la página o blog corporativo que coincide con la marca o nombre comercial), como en la reputación *online* (buscando un lucro en base al prestigio obtenido por la denominación del despacho en el mercado). Este perjuicio conllevará unas implicaciones jurídicas, que serán analizadas más adelante.

3.3 Ataques de denegación de servicio DDoS

El objetivo de un ataque de denegación de servicio distribuido, o ataque DDoS, consiste en -hablando en términos de seguridad informática- un conjunto de técnicas que tienen por objetivo dejar un servidor inoperativo.

Para poder llevar a cabo el ataque **se requiere que varios equipos trabajen coordinadamente para enviar peticiones masivas al servidor del despacho**, 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 éste responder a tal flujo de peticiones.

Los equipos utilizados para lanzar el DDoS suelen formar parte de una botnet –o red de ordenadores zombis-, 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. No es suficiente con filtrar las peticiones procedentes de un único origen o con un formato concreto.

Como consecuencia, la página web del despacho deja de funcionar, acarreándole un perjuicio a la identidad digital 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.

Caso 3.

El despacho 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.

Este tipo de ataques están cobrando cada vez más relevancia pública como forma de ciberprotesta (*ciberhacktivismo* en el argot), que puede provenir de algún caso o asunto en el que el despacho pueda estar involucrado.

La página web del despacho deja de funcionar, acarreándole un perjuicio a la identidad digital y a la reputación *online*, puesto que el hecho de ser atacada proyecta una imagen de vulnerabilidad frente al público

3.4 Fuga de información

En el caso de una **fuga de información,** la buena imagen y el prestigio del despacho puede verse comprometida por la publicación en internet de información sensible y/o confidencial (como por ejemplo, datos personales de empleados y clientes, datos bancarios, informaciones estratégicas de la organización, etc.).

El objetivo suele ser el lucro (por ejemplo, al obtener información bancaria del propio despacho y sus clientes, o extorsionar al propietario 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 posibles orígenes de la fuga de información:

- **Desde el interior de la organización,** bien por error accidental de los abogados y otros 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 el despacho**, 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, la **infección con *malware*** para robo de datos (lo que habitualmente se conoce por troyano). 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.

  Otra técnica son los **ataques *Man in the Middle*** *(ataque de intermediario)*, 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.

Caso 4

El despacho ABOGONLINE 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).

«La buena imagen y el prestigio de una entidad puede verse comprometida por la publicación en internet de información sensible y/o confidencial»

Una situación intermedia se produce cuando una mala praxis de un empleado deja al descubierto información crítica para la empresa.

Para conocer cómo gestionar una fuga de información, disponemos de la guía **«Cómo gestionar una fuga de información: una aproximación para el empresario»** en la que se indican los pasos a seguir para gestionarla de forma correcta y minimizar su repercusión.

«Cómo gestionar una fuga de información: una aproximación para el empresario»

3.5 Publicaciones por terceros de informaciones negativas

A través de los medios sociales, los despachos pueden obtener un *feedback* directo de usuarios, clientes y público en general sobre aquellos y sobre sus servicios jurídicos y de asesoramiento.

¿Qué ocurre cuando esta respuesta es negativa y puede afectar a su reputación *online*? Por poner un ejemplo, los memes ridiculizan a una empresa, o 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, existen usuarios que se dedican a avivar el sentimiento negativo hacia otros usuarios o empresas (comúnmente conocidos por *trolls*), utilizando, si es necesario, fórmulas molestas como las burlas, los insultos o las interrupciones en la conversación.

A través de los medios sociales, los despachos pueden obtener un *feedback* directo de usuarios, clientes y público en general sobre aquellos y sobre sus servicios jurídicos y de asesoramiento.

Caso 5

El despacho ha sido falsamente acusado en redes sociales de estafar a sus clientes. La repercusión del comentario ha tenido tanto alcance que el hashtag #despachofraude en Twitter se ha convertido en trending topic (tema de actualidad). Debido a esta acusación, el despacho ha registrado una importante reducción de encargos, con la consecuente caída del negocio.

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, sea comentado en Internet es también una información valiosa para el despacho, que puede corregir el fallo en base a estos comentarios negativos.

En estos casos, la diligencia del despacho 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 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.

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 *online* de las entidades. Volviendo al ejemplo inicial, la campaña de descrédito que sufre el despacho falsamente acusado 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 muestran a menudo informaciones pasadas, pueden 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.

«La realización de comentarios negativos o falsos sobre una organización puede tener consecuencias legales»

«Es necesario tener en cuenta que la información en Internet no desaparece con el tiempo»

3.6 Utilización no consentida de derechos de propiedad industrial

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 exclusiva e impiden, por tanto, que un tercero lo haga sin su autorización. 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 e, incluso, en una práctica comercial desleal.

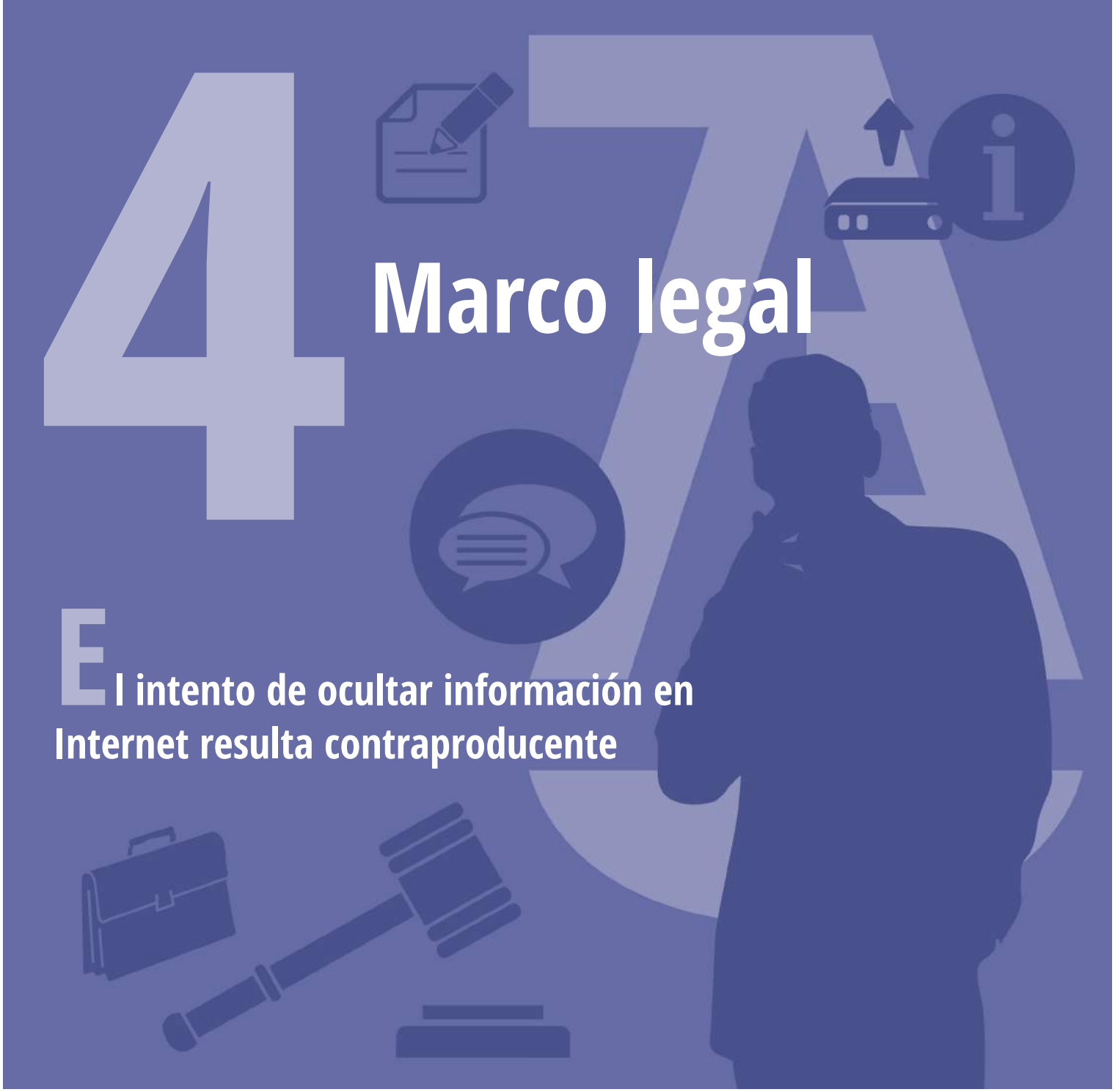
Estos actos pueden estar motivados por una falsa sensación de que en Internet todo vale y no se vulnera ningún derecho, aunque también puede utilizarse por empleados descontentos y terceros malintencionados para divulgar elementos fundamentales para el negocio, como secretos industriales. Estos actos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

También puede darse el caso de que este uso irregular de la imagen pudiera suponer un impacto positivo sobre el valor del despacho. Estas situaciones hay que saber medirlas y aprovecharlas para sacar un beneficio estratégico.

Caso 6

Una asesoría jurídica descubre que una empresa de la competencia utiliza su imagen corporativa modificándola con un lema que puede causar confusión con su marca en Internet. Los socios de la asesoría recurren a ayuda legal para evitar que este acto siga suponiendo un perjuicio para su imagen y valoración en Internet.

4 Marco legal



El intento de ocultar información en Internet resulta contraproducente

- **La empresa que vea dañada su reputación *online* tiene a su disposición herramientas de la legislación española para que su imagen sea reparada**
- **Sólo se retirará una información si esa información vulnera el derecho al honor**

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 un despacho 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 del despacho), siempre se pueden mantener copias, pantallazos o descargas realizados antes de la eliminación.

- **En segundo lugar,** y relacionado con lo anterior, los despachos deben considerar el fenómeno en el que un intento de ocultamiento de cierta información en Internet resulta siendo contraproducente, ya que ésta acaba siendo ampliamente divulgada, recibiendo, en ocasiones, mayor publicidad de la que habría tenido si no se la hubiese pretendido acallar.

«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»

4.1 Derecho al honor de las empresas y acciones legales para su defensa

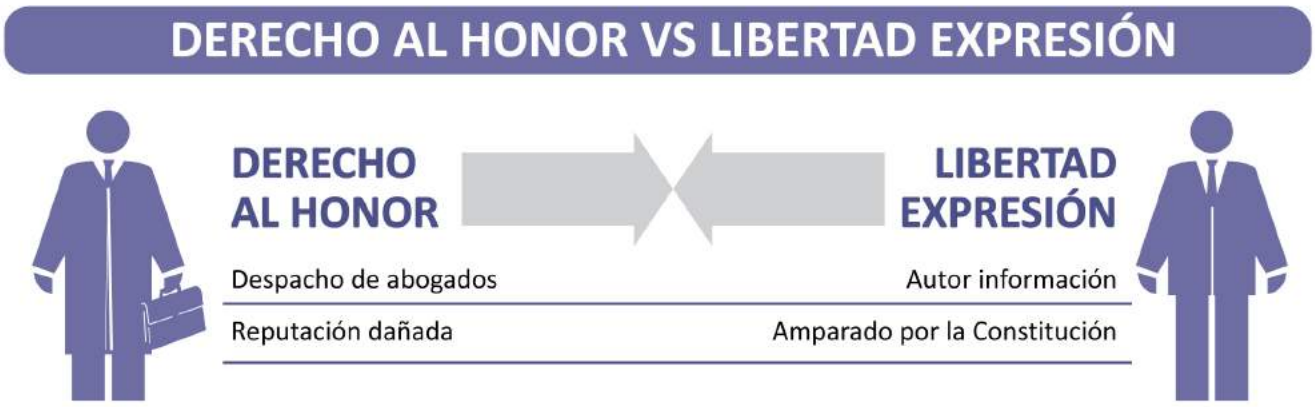
La Constitución Española reconoce el **derecho al honor, a la intimidad personal y familiar y a la propia imagen.**

El Tribunal Constitucional incluye a las empresas y organizaciones entre los titulares del derecho al honor. 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»

Por tanto, los despachos de abogados, 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 del despacho cuya reputación ha sido dañada y, de otro, el derecho a la libertad de expresión e información,** recogidos en la Constitución Española, que ampararían al autor de las informaciones.

Así, los despachos pueden recurrir a normativa específica para salvaguardar su imagen. En concreto, de manera no exhaustiva se comentan dos leyes:



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

Esta ley 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.

Así, trata 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** exime de responsabilidad a los prestadores de servicios siempre que:

a) 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,

b) si lo tienen, actúen con diligencia para retirar los datos o hacer imposible el acceso a ello.

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 un despacho de abogados –en cuanto empresa que son-, los tribunales españoles en ocasiones han recurrido a la Ley de Competencia desleal en casos de utilizaciones fraudulentas 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.

«Las empresas deben considerar el fenómeno en el que un intento de ocultamiento de cierta información en Internet resulta contraproducente»

4.2 ¿Derecho al olvido de los despachos de abogados?

El derecho al olvido puede definirse como la facultad que se atribuye a una empresa o individuo de obtener la eliminación de una determinada información, particularmente en el contexto de Internet.

Basta con poner el nombre de un despacho entre comillas en un buscador y éste ofrecerá un completo perfil de la información que sobre dicha empresa circula en la Red, ya sean noticias positivas o negativas.

¿Puede un despacho de abogados solicitar que sea eliminada de Internet cierta información que afecta de manera negativa a su reputación?

En Europa, desde 2014, **los buscadores tienen la obligación de eliminar de sus listas de resultados aquellos enlaces que violen ciertos derechos de un ciudadano o empresa**, a petición de éste, debido a una sentencia del Tribunal de Justicia de la Unión Europea.

Cada una de estas peticiones se valora de manera individual por parte de los responsables de los motores de búsqueda, que son los encargados de tomar la decisión de aceptar o rechazar las solicitudes.

En España, en enero de 2015 la **Audiencia Nacional** reconoció por primera vez el derecho al olvido. Este derecho a la protección de datos no ampara exclusivamente a las personas físicas, aunque las empresas que quieran que se retire una información sobre ellas solo podrían hacerlo si esa información vulnera su derecho al honor.

Desde esta fecha **Google**, proporciona un formulario que permite solicitar la eliminación de los datos personales que Google mantiene en sus bases de datos.

El **Reglamento Europeo de Protección de Datos**, de aplicación directa en los estados miembros, reconoce a los usuarios su derecho a rectificar los datos que les afectan y que sean incorrectos. Además, si una persona pide el borrado de sus datos, la empresa debe remitir la petición a otros sitios donde esta información se haya replicado.

No obstante, el derecho al olvido queda limitado por otras consideraciones, como el ejercicio de la libertad de expresión e información.

Su aplicación, en último caso, sigue estando en manos de las autoridades de protección de datos o tribunales.

«Las empresas que quieran que se retire una información sobre ellas solo podrían hacerlo si esa información vulnera su derecho al honor»

5 Recomendaciones para la gestión de la identidad digital del despacho y de su reputación *online*

Una identidad digital adecuada requiere implicación y dedicación

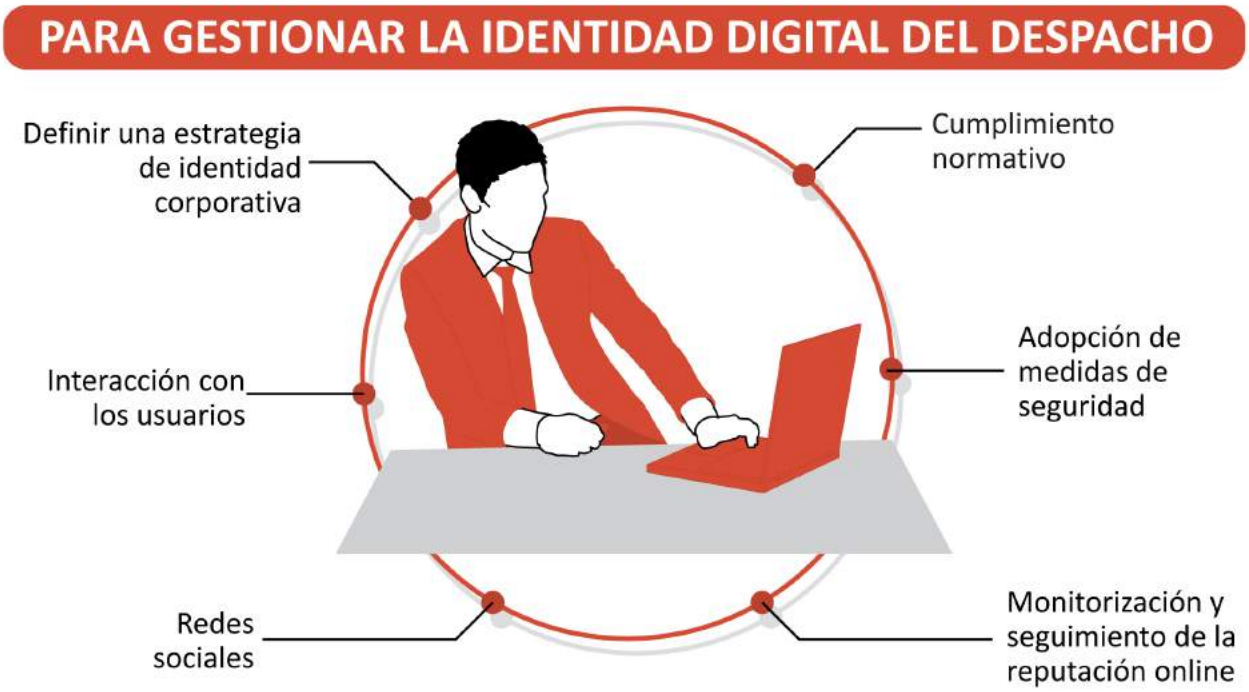
- **La interacción con usuarios en Internet permite el establecimiento de relaciones de confianza**
- **Si la identidad *online* no se gestiona adecuadamente pueden producirse daños en la imagen corporativa**

Una identidad digital adecuada y una reputación *online* sana requieren implicación y dedicación. Las siguientes son una serie de pautas preventivas de gestión, que contribuyen a construir una imagen sólida del despacho, y pautas de reacción, que pueden ayudar al despacho que vea vulnerada su reputación *online* a recuperar su buena imagen.

5.1 Recomendaciones preventivas

La construcción de una identidad digital empresarial robusta y solvente, que permita que los usuarios perciban la imagen que el despacho desea transmitir, requiere un trabajo constante.

Las siguientes pautas de actuación pueden ayudar a las organizaciones a gestionar su reputación *online* de manera integral.



5.1.1 Definición de una estrategia de identidad corporativa

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

En concreto, el despacho debe:

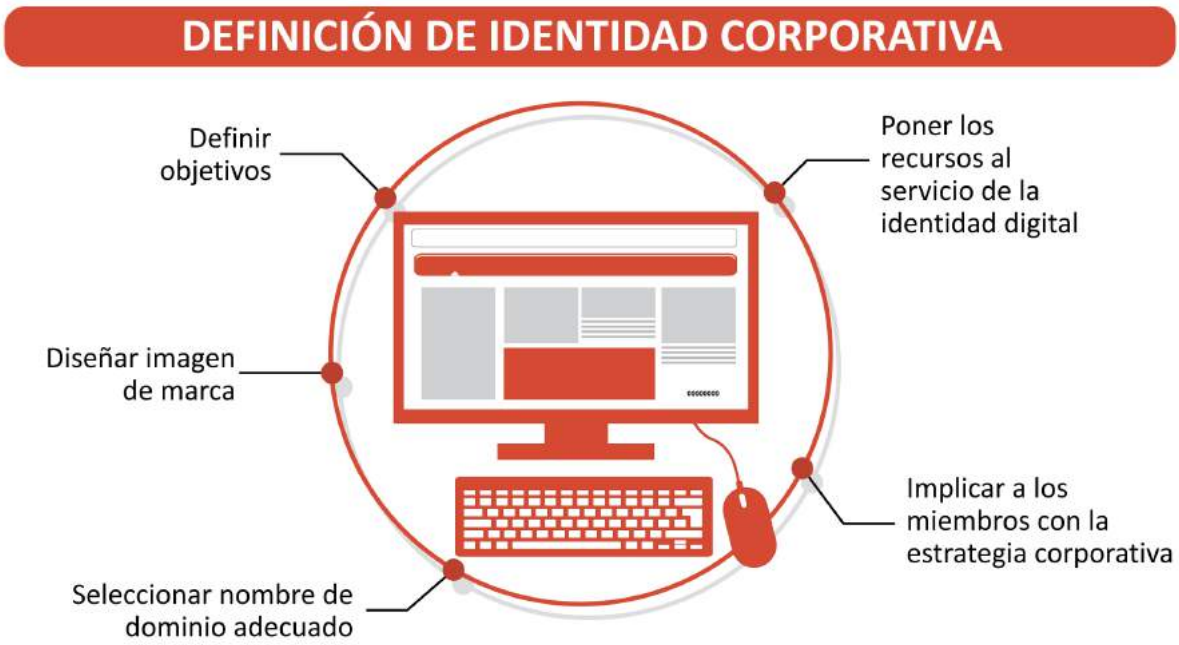
- **Definir sus objetivos** en materia de identidad digital.

- Diseñar una **imagen de marca**.

- 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* y/o *Social Media Manager*.

- Formar e implicar a todos **los miembros de la organización 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 abogados del despacho conozcan las pautas de actuación y reglas de comportamiento cuando actúan en representación (formal o informal) de aquél y que sean respetuosos en el cumplimiento de las cláusulas de confidencialidad.



5.1.2 Interacción con los usuarios

La interacción con los usuarios en un entorno abierto como es Internet permite el establecimiento de relaciones de confianza basadas en el diálogo, pero también expone al despacho a las críticas de manera más abierta. Ello obliga a los despachos de abogados a considerar una serie de pautas. El primero, definir qué modelos de comunicación desea adoptar en la interactuación con los usuarios en las plataformas colaborativas. En concreto, el despacho debe reflexionar acerca de, al menos, los siguientes aspectos:

- **¿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, especialmente con aquel que tenga capacidades para hacer un seguimiento de las opiniones o denuncias manifestadas en el espacio y su gestión y dando respuesta a usuarios y seguidores.

5.1.3 Redes Sociales

Si en las redes sociales la identidad *online* de un despacho no se gestiona adecuadamente, pueden producirse daños importantes en su imagen corporativa, que derivarán en pérdidas de confianza de los clientes y provocará, en definitiva, pérdidas económicas.

Por este motivo, **para gestionar la identidad *online* de las empresas, surgió la figura de *Community Manager***. Esta figura, ya sea personal de la organización o subcontratado a un tercero, estará siempre sujeta a los procesos internos y directrices de seguridad de la empresa. Sin embargo, cuando hablamos de los empleados que usen redes sociales en su actividad profesional (por ejemplo, en el caso de perfiles en LinkedIn), la situación se vuelve algo más compleja.

Para evitar que se produzcan fugas de información corporativas por el uso de las redes sociales lo primero que debemos hacer es establecer una política interna de uso de redes sociales. Es necesario establecer unas obligaciones y recomendaciones para que el empleado con actividad en las redes sociales haga un uso adecuado de éstas sin poner en riesgo el funcionamiento, la reputación y la información del despacho. Es recomendable apoyarse en asesoramiento para que la política se ajuste a la normativa legal.

«Es necesario establecer unas obligaciones y recomendaciones para que el empleado con actividad en las redes sociales haga un uso adecuado de éstas»

Además, deberemos acompañar esta política de una guía de buenas prácticas, que establezca las reglas, recomendaciones y acciones concretas del *Community Manager* y en general de todo empleado que use las redes sociales. Entre las buenas prácticas recomendadas en dicha guía podemos mencionar:

«El cumplimiento de la legislación aplicable al entorno digital es absolutamente clave para la buena salud de la reputación de una organización»

- **Cambiar la contraseña** con cierta frecuencia y prohibir su reutilización en otros servicios, además de implantar una configuración adecuada de la privacidad.

- Tener especial **cuidado con el uso que se les da a nombres, logotipos y marcas de la empresa**, ya que son distintivos registrados.

- **Evitar escribir en las redes sociales dando a entender que se actúa como portavoz** de las opiniones o posición oficial del despacho, a no ser que se disponga de autorización para ello.

- **No emitir opiniones personales de carácter político, religioso o ideológico** en redes abiertas, profesionales o mixtas. Tales opiniones son personales y no deben representar al despacho.

- **Evitar criticar de manera irresponsable** y sin argumentos servicios o proyectos de la competencia.

- **Evitar entrar en debates y discusiones con clientes** o potenciales clientes a través de las redes sociales.

- **Evitar dar información confidencial** sobre la organización o información que pueda violar el código deontológico de la abogacía.

- **Evitar publicar fotos** donde se muestre el logo o información del despacho, siempre que no se esté autorizado para ello.

Es importante que los empleados conozcan la política, normativa, buenas prácticas y en definitiva las reglas definidas, los usos permitidos de las redes sociales y las posibles sanciones de un uso indebido. Además, es recomendable que en ellas se diferencien claramente dos escenarios de uso de las redes sociales, uno para el trabajo y otro para su uso extra-laboral que pueda estar vinculado con su actividad laboral.

Como particularidad para los perfiles asociados a nuestra marca de despacho, debemos tener presente que debemos hacerlo siempre utilizando un correo corporativo y nunca personal. En el caso de un despacho de reducido tamaño, esta recomendación se hace más relevante, y evitaremos mezclar los contactos profesionales con los personales, ya que no tenemos control sobre lo que pueden escribir nuestros amigos de nosotros.

5.1.4 Cumplimiento normativo

La imposición de una sanción derivada del incumplimiento normativo (legal o deontológico) tiene importantes efectos sobre la reputación *online* del despacho.

Por ello, el cumplimiento de la legislación aplicable al entorno digital es absolutamente clave para la buena salud de la reputación de una organización.

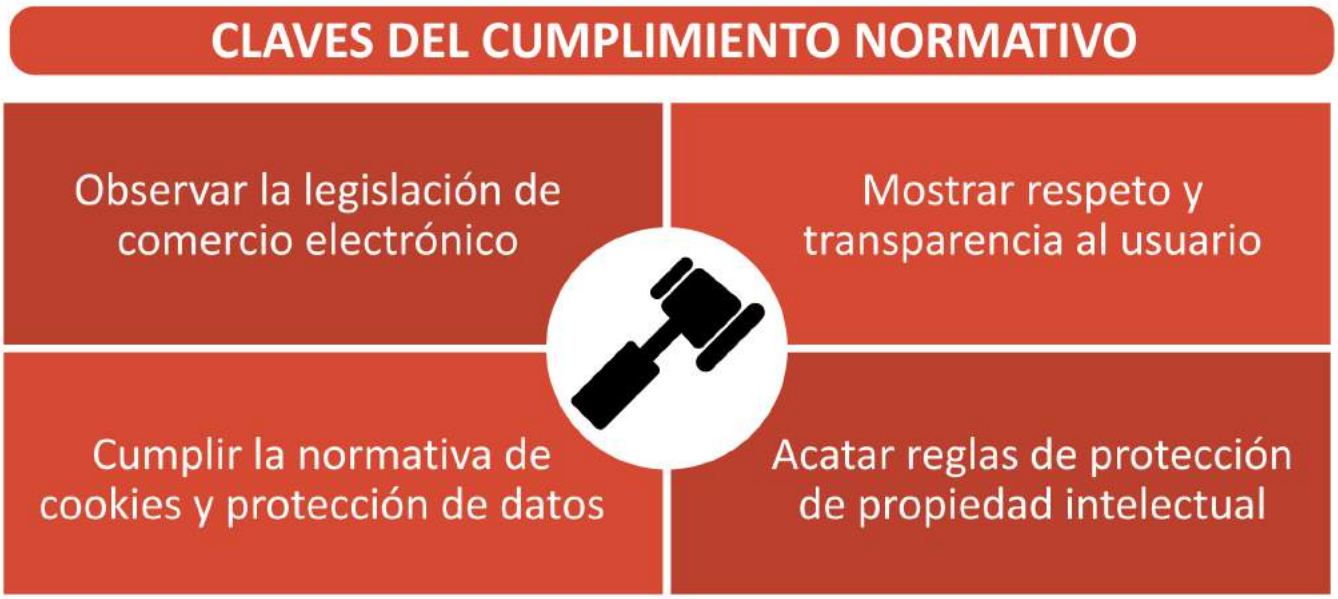
En concreto, resultan especialmente importantes los siguientes aspectos:

- **Observar la legislación de comercio electrónico** y servicios de la Sociedad de la Información: suministro de información, políticas de contratación, información y derechos del consumidor, políticas de envío de comunicaciones comerciales, etc. Esto, además, es una buena práctica que va a ser determinante para la supervivencia en la web.

- **Mostrar respeto por el usuario y apostar por la transparencia**. Estas dos acciones generan confianza en los clientes, lo que también puede ser una forma para diferenciar las páginas ilegitimas.

- **Cumplir la normativa de cookies y de protección de datos**: registro de ficheros, deber de información y solicitud de consentimiento, garantía de ejercicio de los derechos 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*.



5.1.5 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 los despachos 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 brechas 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 de reputación, orientados hacia la adopción, implementación y certificación de un Sistema de Gestión de la Seguridad de la Información (SGSI).

5.1.6 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 del despacho en Internet.

La verificación debe abarcar aspectos de relevancia (es decir, cuál es la posición del despacho 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.

«Ser víctima de un ataque informático puede tener graves consecuencias para la reputación corporativa»

5.2 Recomendaciones reactivas

¿Qué ocurre cuando el despacho experimenta una crisis de reputación *online* o es víctima de alguna situación que exige una reacción inmediata? Uno de los episodios que más preocupa a las empresas es, precisamente, 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 el área de comunicación, por el *Community Manager* o *Social Media 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 despacho pueden ser igualmente válidas. 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.

Hoja de ruta en crisis de reputación *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 lanzamiento	■ Reunión del gabinete de crisis ■ Presentación del informe de situación	**A las 6 horas como máximo**	Gabinete de Crisis (Community Manager, Dirección, Dpto Comunicación...)
Fase de auditoría	■ Realización de una auditoría interna y externa ■ Preparación de un informe preliminar	**Antes de 18 horas**	
Fase de evaluación	■ Reunión del gabinete de crisis ■ Principales pasos a seguir ■ Tareas y planificación	**Antes de 18 horas**	Gabinete de Crisis (Community Manager, Dirección, Dpto Comunicación...)
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

5.2.1 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.

Las principales redes sociales (Twitter, Facebook, etc.) disponen de una Política de usurpación de identidad en la que indican lo que consideran suplantación de la identidad de personas y empresas. Asimismo, proporcionan formularios para reportar incidentes de manera que el proveedor pueda comprobar los datos y devolver las cuentas suplantadas a su legítimo titular.

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.

«Las principales redes sociales proporcionan formularios para reportar incidentes de manera que el proveedor pueda comprobar los datos y devolver las cuentas suplantadas a su legítimo titular»

5.2.2 Denuncia judicial frente a atentados a la reputación

Anteriormente 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.

5.2.3 Recuperación del nombre de dominio

En caso de que un tercero haya ocupado un dominio de nuestro despacho 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.

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), que contempla una serie de entidades internacionales acreditadas para realizar el arbitraje.

También es posible acudir ante la jurisdicción ordinaria invocando la legislación sobre competencia desleal o sobre marcas.

«En caso de que un tercero haya ocupado un dominio del despacho sin autorización debe procederse a su reclamación»

E-BOOK GUÍAS TIC

GUÍA DE CIBERSEGURIDAD Y REPUTACIÓN ONLINE PARA DESPACHOS DE ABOGADOS

Abogacía Española
CONSEJO GENERAL

incibe_

www.abogacia.es @RedAbogacia @Abogacia_es