Ciberseguridad en la identidad digital **y la reputación online**

Una guía de aproximación para el empresario

INSTITUTO NACIONAL DE CIBERSEGURIDAD

SPANISH NATIONAL CYBERSECURITY INSTITUTE

10 incibe_ 2006-2016 TRABAJANDO POR LA CONFIANZA DIGITAL

Ciberseguridad en la identidad digital **y la reputación online**

Una guía de aproximación para el empresario

INCIBE_PTE_AproxEmpresario_004_IdentidadyReputacion-2016-v1

índice

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

1 Introducción

La **identidad corporativa** permite a las empresas diferenciarse de las demás y esto es también cierto en el mundo digital e interconectado actual. En este entorno cobran especial importancia algunas características de la comunicación, en particular las relativas a: la inmediatez, visibilidad, credibilidad, influencia y permanencia de la información.

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.

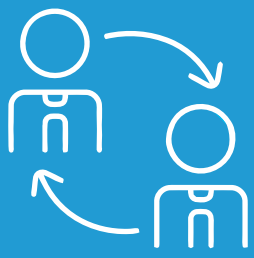
A la identidad digital corporativa contribuyen, además de las comunicaciones por correo electrónico y mensajería instantánea (WhatsApp, SMS..), la presencia en Internet mediante una página, portal o tienda online y la presencia en las redes sociales tanto de la empresa como de sus empleados (Twitter, Facebook, Pinterest, LinkedIn…).

«A la identidad digital corporativa contribuyen la presencia en Internet mediante una página, portal o tienda online y la presencia en las redes sociales»

Las empresas, conscientes de esa importancia, utilizan las redes sociales de manera profesional planificando previamente su estrategia de comunicación en ellas. Además, las redes sociales permiten a las empresas construir mediante la interacción con clientes y otros agentes su «marca social» de forma colaborativa. La reputación online es una medida de la opinión que ofrece la marca en el mundo digital y está formada por valores como: actualidad, relevancia, confianza, credibilidad, seguridad, respeto, transparencia y honestidad. En este sentido, las redes sociales son un perfecto termómetro para que las empresas puedan medir su reputación en la red.

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

1 Introducción



"¿Qué hacer cuando suplantan la identidad de mi organización en la Red?"

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 su incursión en los medios sociales (correo electrónico, pagina web, redes sociales…). 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. 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 éstas 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.

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.

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. Ni siquiera 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.

«La identidad digital corporativa se ve complementada con lo que los propios usuarios y clientes opinan sobre la empresa en Internet»

La web 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. Cualquier empresa o profesional puede tener presencia digital gracias a una página web, a través de la cual puede interactuar con clientes y usuarios.

Las organizaciones son conscientes de la importancia de estar presentes en los medios sociales. Así, 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.

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 puede 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.

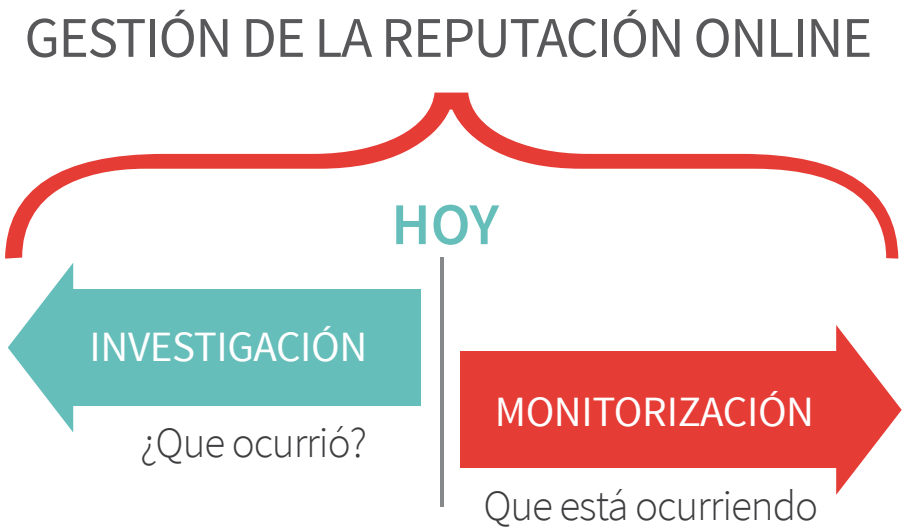


Fig. 1: Mapa de gestión de la reputación online

Investigación de la reputación online (Qué ocurrió)

La investigación consiste en un análisis retrospectivo de la reputación online de una empresa. Este análisis se divide en dos fases:

- Fase cuantitativa: esta es la primera etapa de la investigación, se realizará un registro de las opiniones de los usuarios y de los medios sobre la empresa que se encuentran en blogs, foros, redes sociales, etc.

- 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.

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,

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

marcas comerciales, productos, personas y otros activos sujetos a su propiedad industrial e intelectual.

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 posicionamiento en los motores de búsqueda (*Search Engine Optimization, SEO*), la gestión de las comunicaciones en redes sociales (SMO - Social Media Optimization) y la gestión de los enlaces patrocinados (*Search Engine Marketing, 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.

- Otro aspecto relevante en la gestión de la reputación 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 la totalidad de áreas de negocio, comenzando por la dirección y los recursos humanos, así como la gestión con los proveedores, la comunicación, 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, 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 la reputación online

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, las cuales impactan de tal forma en la imagen de la empresa que los efectos perduran en el tiempo.

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 o whatsapp simulando ser la empresa DOLLS. 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 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 suplantada.

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 (correo electrónico, perfil en redes sociales…) 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 (credenciales, cuentas, etc.) que resultan de interés para el estafador. 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.

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 del sitio web legítimo, automáticamente es dirigido hacia una página web fraudulenta 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 servicios, tanto dentro como fuera de la Red. Estas conductas tienen implicaciones legales.

4.2 Registro abusivo de nombre 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[1] es la denominación fácilmente recordable que utilizan los usuarios para acceder a una página web (por ejemplo **incibe.es**). Este nombre de dominio está asociado a una dirección IP (*Internet Protocol*) o código que utilizan los ordenadores para comunicarse entre sí.

Las empresas 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, 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[2] (como «.info» 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 ocupados, 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.

1 http://www.oepm.es/es/propiedad_industrial/preguntas_frecuentes/FaqSignos04.html
2 TDL o Top Level Domain: dominio de nivel superior. Más información: www.icann.org

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

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[3].

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 conllevará unas implicaciones jurídicas, que serán analizadas más adelante[4].

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

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 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[5], 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 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 ata-

3 Ejemplo: «El negocio del typosquatting». Disponible en: http://www.ticbeat.com/analisis/negocio-typosquatting-errores-teclear-dominio/
4 Ver la sección 5.1, derecho al honor de las empresas y acciones legales para su defensa.
5 https://www.incibe.es/blogs/post/Empresas/BlogSeguridad/Articulo_y_comentarios/Historias_reales_mi_empresa_ataco_otra

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

ques están cobrando cada vez más relevancia pública como forma de ciberprotesta.

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).

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

El objetivo suele ser el lucro (por ejemplo, al obtener información bancaria de la empresa y sus clientes, o al 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 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:

- 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.

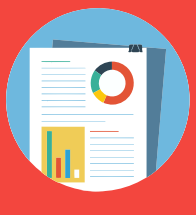
- Los ataques *Man in the Middle*, en los que el atacante se posiciona entre el servidor web de la entidad y el equipo que solicita la conexión a dicho servidor, desde donde puede leer, filtrar e incluso modificar la información que se está transfiriendo sin dejar rastro de su acción.

Una situación intermedia en la que una mala práxis de un empleado deja al descubierto información crítica para la empresa.

Para conocer cómo gestionar una fuga de información, en Incibe disponemos de una guía «Cómo gestionar una fuga de información: una aproximación para el empresario[6]» en la que se indican los pasos a seguir para gestionarla de forma correcta y minimizar su repercusión.

En Incibe disponemos de una guía «Cómo gestionar una fuga de información: una aproximación para el empresario»

4.5 Publicaciones por terceros de informaciones negativas

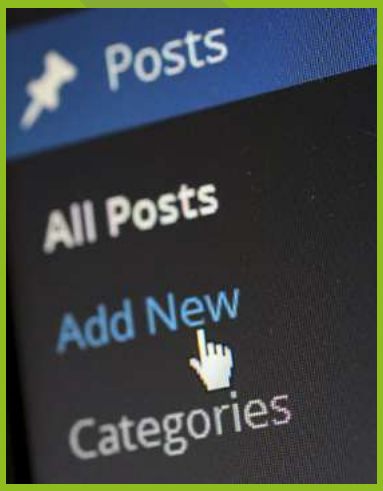


Caso 5 La empresa de venta online TUTIENDA.COM ha sido falsamente acusada de estafar a sus clientes. La repercusión del comentario ha tenido tanto alcance que el hashtag #tutiendafraude en Twitter se ha convertido en trending topic (tema de actualidad). Debido a esta acusación, la empresa ha registrado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

6 https://www.incibe.es/empresas/guias/Guia_fuga_informacion



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

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 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 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[7].

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 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 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.

4.6 Utilización no consentida de derechos de propiedad industrial

Caso 6 La hamburguesería LA SUPREMA descubre que 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).

7 Estos aspectos serán analizados en el apartado siguiente, al dibujar el Marco Legal de la reputación online de las empresas.

4

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

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

Estos derechos tienen una doble dimensión: permiten a su propietario su utilización e impiden que un tercero lo haga. 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[8].

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. Estos actos pueden 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.

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

8 Véase capítulo siguiente

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 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.

«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»

5.1 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, 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 de la empresa 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, las empresas 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»*

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

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.** 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[9].

9 http://boe.es/legislacion/codigos/codigo.php?id=67&modo=1&nota=0&tab=2

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

5.2 ¿Derecho al olvido de las empresas?

El derecho al olvido[10] 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 una empresa entre comillas en un buscador y éste ofrecerá un completo perfil de la información que sobre dicha empresa circula en la Red, ya sean buenas o malas noticias.

¿Puede una persona jurídica 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[11].

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. Para llevar a cabo esta tarea, Google cuenta con un comité de expertos que se encarga de asesorar a la compañía en todas las cuestiones referentes al derecho al olvido.

Así, en enero de 2015 la Audiencia Nacional reconoció por primera vez el derecho al olvido en España[12]. 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[13] que permite solicitar la eliminación de los datos personales que Google mantiene en sus bases de datos.

La UE recientemente ha aprobado una nueva norma de protección de datos, de aplicación directa en los estados miembros, por la cual los usuarios tendrán derecho a rectificar los datos que les afectan que sean incorrectos y las empresas están obligadas a notificar a sus clientes cualquier brecha de seguridad que pueda haberles afectado. 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.

10 http://boe.es/legislacion/codigos/codigo.php?id=94&modo=1&nota=0&tab=2
11 El País, «La UE obliga a Google a retirar enlaces con información lesiva». Disponible en: http://sociedad.elpais.com/sociedad/2014/05/12/actualidad/1399921965_465484.html . 12 de mayo de 2014
12 El País, «La Audiencia nacional reconoce por primera vez el 'derecho al olvido'», Disponible en: http://politica.elpais.com/politica/2015/01/23/actualidad/1422015745_590889.html
13 Google «Solicitud de retirada de resultados de búsqueda en virtud de la normativa de protección de datos europea». Disponible en: https://support.google.com/legal/contact/lr_eudpa?product=websearch&hl=es y las FAQ en https://www.google.com/intl/es/policies/faq/

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

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 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.

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.
- 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 internet 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:

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

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:

- ¿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 y dando respuesta a usuarios y seguidores.

6.1.3 Redes Sociales

Si en las redes sociales la identidad online de una empresa 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, surge 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 de la empresa. Es recomendable apoyarse de asesoramiento legal para que la política se ajuste a la normativa legal.

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, 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 de la empresa, 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 a la empresa.
- Evitar criticar de manera irresponsable y sin argumentos productos 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 usar la competencia.
- Evitar publicar fotos donde se muestre el logo o información de la empresa, 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, una para el trabajo y otra para su uso extralaboral que pueda estar vinculado con su actividad laboral.

Como particularidad para los perfiles asociados a nuestra marca de empresa, debemos tener presente que debemos hacerlo siempre utilizando un correo corporativo y nunca personal. En el caso de una pequeña empresa, 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.

6.1.4 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[14]: políticas de compra, contratación, informa-

14 http://www.boe.es/buscar/act.php?id=BOE-A-2002-13758

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

ción 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 transparencia y generar así confianza en los clientes, es una forma diferenciar las páginas ilegitimas.

- Cumplir la normativa de protección de datos[15]: 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[16], incluyendo el establecimiento de derechos de los usuarios y la implementación, si procede, de licencias *Creative Commons*[17].

6.1.5 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 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 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 reputacionales, orientados hacia la adopción, implementación y certificación de un Sistema de Gestión de la Seguridad de la Información.

6.1.6 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 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.

15 La Agencia Española de Protección de Datos ofrece varias herramientas de ayuda. Disponibles en: https://www.agpd.es/portalwebAGPD/canalresponsable/inscripcion_ficheros/herramientas_ayuda/index-ides-idphp.php.
16 http://www.boe.es/buscar/act.php?id=BOE-A-1996-8930
17 http://es.creativecommons.org/blog/

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.

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. 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.

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, otros dptos.)
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, 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

Tabla 1: Esquema de actuación frente a una crisis online

«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»

6.2.1 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.

Figura 2: 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.

6.2.2 Denuncia judicial frente a atentados a la reputación

Anteriormente se han identificado[18] 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.

6.2.3 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[19]. Para po-

18 En el apartado 5.1 Derecho al honor de las empresas y acciones legales para su defensa.
19 Véase en Red.es, «Sistema DRP». Disponible en: http://www.dominios.es/dominios/es/todo-lo-que-necesitas-saber/sobre-registros-de-dominios/recuperacion-de-dominios

der 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)[20], que contempla una serie de entidades internacionales acreditadas para realizar el arbitraje[21].

También es posible acudir ante la jurisdicción ordinaria invocando la legislación sobre competencia desleal o sobre marcas[22].

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

20 Véase en ICANN «Uniform Domain Name Dispute Policy». Disponible en: https://www.icann.org/resources/pages/policy-2012-02-25-en
21 Véase en ICANN «List of approved Dispute Resolution Service Providers». Disponible en: http://www.icann.org/en/dndr/udrp/approved-providers.htm
22 Según lo dispuesto en el apartado 5.1.

7 Referencias

- **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

- **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.

- **ÓSCAR DEL SANTO (2011).** Reputación Online para Tod@s: 10 lecciones desde la trinchera sobre tu activo más importante. http://dksignmt.com/download/Descargas/Reputaci%C3%B3n%20Online%20Para%20Todos.pdf

GOBIERNO DE ESPAÑA
MINISTERIO DE INDUSTRIA, ENERGÍA Y TURISMO

10 incibe_
2006-2016
TRABAJANDO POR LA CONFIANZA DIGITAL