Ciberseguridad en la identidad digital y la reputación online

Guía de recomendaciones para empresas

Financiado por la Unión Europea NextGenerationEU

Gobierno de España · Vicepresidencia Primera del Gobierno · Ministerio de Asuntos Económicos y Transformación Digital · Secretaría de Estado de Digitalización e Inteligencia Artificial

Plan de Recuperación, Transformación y Resiliencia

España | digital 2026

incibe_ Instituto Nacional de Ciberseguridad

protege tu empresa

Índice

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 le contribuyen, además de las comunicaciones por correo electrónico y mensajería instantánea (WhatsApp, SMS...), la presencia en Internet mediante una página web, portal o tienda online y la presencia en redes sociales [REF-1] tanto de la empresa como de sus empleados (X, Instagram, LinkedIn, Facebook...).

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

Las empresas, conscientes de esa importancia, utilizan las redes sociales de manera profesional, planificando previamente su estrategia de comunicación en ellas. Además, 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 y publicación de los productos o servicios de la empresa, ya que implican una gran llegada al público. En segundo lugar, la presencia de las empresas en redes sociales mejora la difusión de la propia actividad y la comunicación tanto con el cliente, como con otros profesionales.

¿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 del uso de la tecnología, como correo electrónico, página web, redes sociales…. Surge un nuevo escenario en el que los incidentes se intensifican por el incremento de amenazas 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 reseña negativa sobre la misma? Esta guía busca dar respuesta a éstas y otras muchas 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 y perfiles 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 la Red 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 página web corporativa constituye un canal masivo de comunicación para las empresas, y las redes sociales representan una herramienta mediante la cual las organizaciones disponen de un feedback en tiempo real de clientes y usuarios.

Las organizaciones son conscientes de la importancia de estar presentes en los medios sociales. Así, 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, 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, mientras que la reputación online, puede definirse como la valoración alcanzada por una empresa a través del uso de las herramientas 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:** ésta es la primera etapa de la investigación. Se realizará un registro de las opiniones de los usuarios 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, 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.

«Cada vez son más las organizaciones que gestionan de forma profesional su identidad digital corporativa y su 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 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 nuevos perfiles profesional: Social Media Manager o Community Manager. Estos profesionales desempeñan roles activos y especializados en la gestión de la presencia online de la organización teniendo en cuenta su idiosincrasia.

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 [REF - 2]. 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 DOLLSS S.A. está recibiendo numerosas quejas por parte de los consumidores. Buena parte de ellas son a través de las redes sociales. La razón, es que un tercero malintencionado está enviando correos electrónicos y mensajes a través de las redes sociales simulando ser la empresa DOLLSS S.A. 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 un incidente de seguridad que deben gestionar ya que su imagen se está viendo perjudicada.

La suplantación de identidad de la empresa en Internet [REF - 3] 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 en redes sociales o cuenta de correo electrónico de una empresa o entidad 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 cometer fraude online. Para ello, recurren a diferentes técnicas:

Phishing: el ciberdelincuente usurpa la identidad (correo electrónico, perfil en redes sociales, etc.) 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, datos bancarios, 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. Hoy en día, son muy 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. Además, este tipo de incidentes pueden acarrear consecuencias legales [REF - 4].

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 ciberdelincuentes 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 acce- der a una página web (por ejemplo **incibe.es**) y que está asociado a una dirección IP (Internet Protocol) [REF - 5].

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*** [REF - 6], también puede producirse si la empresa se olvida de renovar el nombre de dominio, o si aparece una nueva extensión TLD[2] (como por ejemplo «.online» o «.xyz») y el propietario de la marca no realiza el correspondiente registro.

En todo caso, este registro fraudulento 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 dicha página.

- Extorsionar al titular legítimo de la marca, solicitándole un precio muy 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.

«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*** [REF - 7] 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 llevar al usuario a una web maliciosa.

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 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[3].

4.3 Ataques de denegación de servicio distribuido «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.

Un ataque de denegación de servicio distribuido, o ataque DDoS [REF - 8], 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 provocando su colapso, al no poder éste responder a tal flujo de peticiones.

Los equipos utilizados para lanzar el ataque DDoS suelen formar parte de una *botnet* [REF - 9] o red de ordenadores zombis, que el ciberatacante controla de forma remota sin que los propietarios sean conscientes de ello.

Como consecuencia, la página web empresarial deja de funcionar, acarreándole un perjuicio a la identidad digital (el negocio en la Red deja de estar disponible para los clientes) 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.

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

4.4 Fuga de información

Caso 4

La gestoría GESTONLINNE 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. Este incidente tendrá tanto consecuencias legales como reputacionales para la organización.

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 ban- caria de la empresa y sus clientes, o al extorsionar al propietario de los datos a cambio de un rescate para no hacerlos públicos), aunque también existen 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** [REF - 10], bien por error accidental de algún empleado, mala praxis por desconocimiento de las medidas de seguridad, o de forma consciente para causar algún perjuicio. A estas personas se les conoce comúnmente por el término insider. 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, entre otras acciones.

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

La infección por *malware* [REF - 12] para el 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, entre otras acciones.

Los ataques *Man in the Middle* [REF - 14] son 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.

Para conocer cómo gestionar una fuga de información, en INCIBE disponemos de la guía «Cómo gestionar una fuga de información: una aproximación para el empresario[4]» en la que se indican los pasos a seguir para gestionarla de forma correcta y minimizar su repercusión.

En INCIBE disponemos de la 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 la red social XY, se ha convertido en trending topic (tema de actualidad). Debido a esta acusación, la empresa ha registrado una importante bajada 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 las redes sociales 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 un lenguaje irrespetuoso.

En principio, las críticas a las entidades son parte de la interactuación que ofrecen las plataformas colaborativas. El hecho de que una falta de atención un error en el servicio o 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 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 dañinos. Estos aspectos son analizados en el apartado siguiente, al dibujar el marco legal de la reputación online de las empresas.

A pesar de las medidas reactivas a aplicar (retirada de comentarios, acciones legales, etc.), la capacidad de difusión de estos canales aumenta el daño sobre la reputación 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 automáticamente 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 SSUPREMA descubre que una empresa de la competencia utiliza su imagen corporativa modificándola con el lema: Una experiencia más que ssuprema. Los dueños de LA SSUPREMA 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: diseños industriales, marcas y nombres comerciales, patentes y modelos de utilidad (invenciones), y topografías de semiconductores (circuitos integrados).

Estos derechos tienen una doble dimensión: permiten a su propie- tario su utilización e impiden que un tercero lo haga. Si se están utilizando o comercializando a través de Internet de forma no au- torizada, 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 [REF - 14].

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

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 im- pacto 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.

La marca y el nombre comercial son parte de la identidad digital y puede ser objeto de abuso, que ocurre cuando alguien utiliza una grafía, logo o imagen corporativa o de algún producto con un gran parecido a nuestra marca. Esto supone un riesgo para la identidad y reputación de una empresa, asociado con el uso por terceros no autorizados de los derechos de propiedad industrial. En caso de conflicto, siempre que hayamos registrado la marca, podemos acudir a los tribunales.

5. Marco legal

«La empresa que haya visto dañada su imagen o reputación online dispone de un marco legal que salvaguarda los derechos e intereses de las empresas en estas situaciones, con el fin de reparar los daños ocasionados».

La empresa que haya visto dañada su imagen o reputación online dispone de un marco legal que salvaguarda los derechos e intereses de las empresas en estas situaciones, con el fin de reparar los daños ocasionados.

El análisis de la normativa que afecta a la reputación online ligeramente difiere 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 llegase a ser retirada, 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 la posibilidad de que un intento de ocultamiento de cierta información en Internet resulte contraproducente para su reputación, ocasionando el efecto contrario si ésta llegase a ser publicada. Es por ello por lo que las entidades, deberán ser diligentes y transparentes, generando así confianza en la propia empresa, clientes, socios y otros terceros.

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

La Constitución Española reconoce en su artículo 18.1 el derecho al honor, a la intimidad personal y familiar y a la propia imagen [REF - 15].

Además, el Tribunal Constitucional incluye a las empresas y organizaciones entre los titulares del derecho al honor, reconociendo 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».

En muchas 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 el artículo 20.1 de la Constitución Española, que ampara a todo aquel que exprese o manifieste un pensamiento, idea y opinión, mediante cualquier medio de reproducción. Por tanto, las empresas y organizaciones, en defensa de su derecho al honor, pueden iniciar acciones legales para solicitar la retirada de la Red de informaciones que produzcan un perjuicio a su reputación.

Así, las empresas pueden recurrir a normativa específica para salvaguardar su imagen. Tanto la **vía civil como la vía penal** serán vías efectivas para proteger el derecho al honor de las personas jurídicas, sin embargo, la vía más efectiva será la **vía civil**, al tratarse la vía penal de un cauce más restrictivo y aplicarse como ultima ratio, es decir, el último recurso para la protección de bienes jurídicos, además de constituir una solución menos versátil que requiere un encaje específico en un tipo penal concreto. No obstante, los **tipos delictivos** que podrían encajar con la emisión de información falsa sobre la empresa donde se menoscabe su honor y reputación empresarial, podrían ser los siguientes:

- **Delito de odio** (artículo 510 y ss. del Código Penal) [REF - 16]
- **Delito de descubrimiento y revelación de secretos** (artículo 197 y ss. CP)
- **Delito contra la integridad moral** (artículo 173 y ss. CP)
- **Delito de estafa** (artículo 248 y ss. CP)
- **Delito de injurias y calumnias** (artículo 205 y ss. CP)
- **Delitos relativos a la propiedad intelectual** (artículos 270 y ss. CP, así como lo regido en el Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el texto refundido de la Ley de Propiedad Intelectual,) [REF - 17]
- **Delitos relativos a la propiedad industrial** (artículos 273 y ss. CP, así como lo dispuesto en la Ley 24/2015, de 24 de julio, de Patentes y en la Ley 17/2001, de 7 de diciembre, de Marcas). [REF - 18]
- **Delitos de competencia desleal** (artículos 197 y ss. Y 278 y ss. CP, así como lo dispuesto en la Ley 3/1991, de 10 de enero, de Competencia Desleal).

Referente a la **vía civil**, la defensa al derecho al honor se encuentra amparada en la Ley Orgánica 1/1982, 5 de mayo, de protección civil del derecho al honor, intimidad personal y familiar y propia imagen.

En lo relativo a la defensa de tutela judicial efectiva, el artículo 9.2 de la ley indica que ésta comprenderá “la adopción de todas las medidas necesarias para poner fin a la intromisión ilegítima de que se trate” y, en particular, las necesarias para:

El restablecimiento del perjuicio causado al perjudicado, obligando al cese de la intromisión y la reposición al estado anterior.	Indemnización de los daños y perjuicios causados. Apropiación del lucro obtenido de la intromisión ilegítima.

5.1.1. Responsabilidad de los prestadores de servicios de sociedad de la información

Por otro lado, es importante tener en cuenta que las entidades que hayan visto menoscabado su honor y reputación online, podrán dirigirse ante los propios prestadores de servicios online, los cuales pueden albergar dicha información en sus sistemas, además de desempeñar un papel esencial en la difusión de información. Destacamos las siguientes normativas:

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

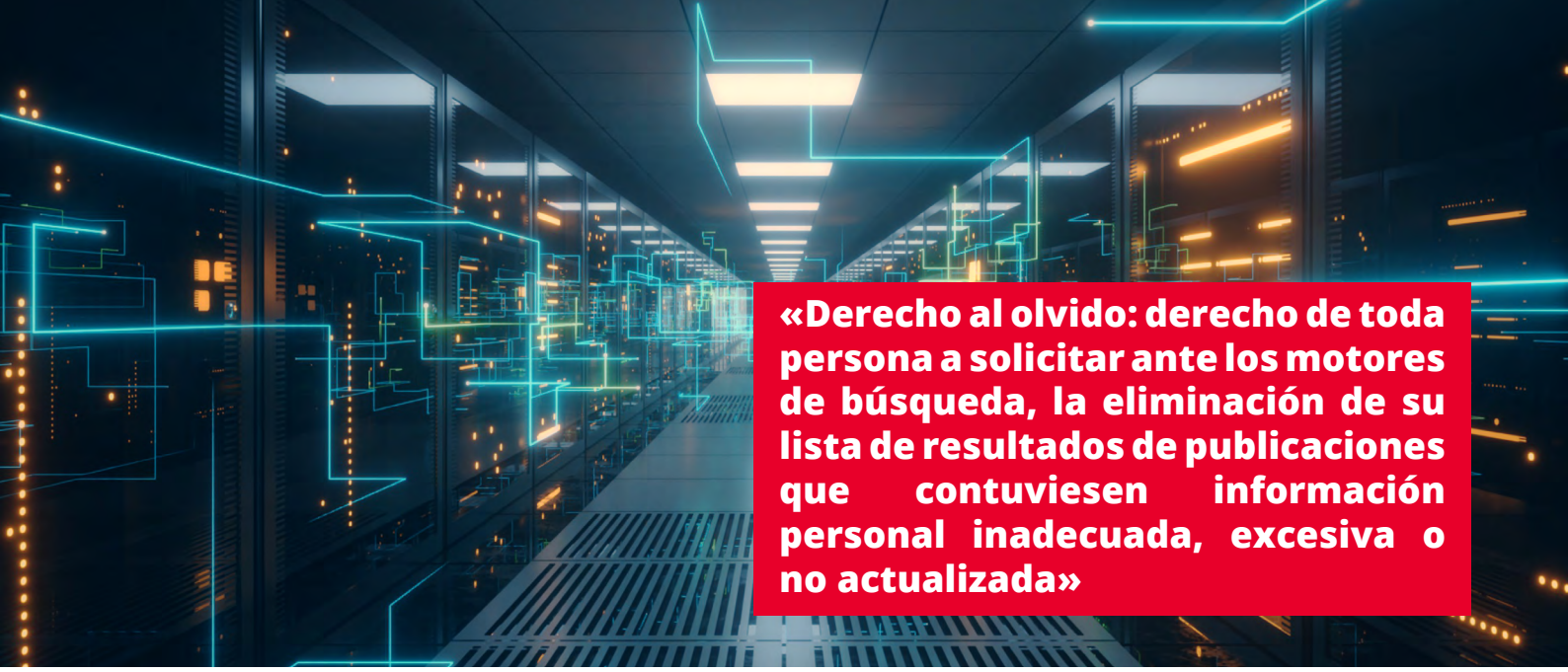
La Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y Comercio Electrónico (LSSI) [REF - 19] regula el régimen de responsabilidad de los prestadores de servicios de la Sociedad de la Información (artículos 13 y ss.), en cuyo ámbito de aplicación se encuentran las redes sociales y plataformas en línea, por la información almacenada o alojada en sus servidores, entre otros servicios.

- El artículo 16 establece los supuestos de exención de responsabilidad a los prestadores de servicios de alojamiento o almacenamiento de datos siempre que:
  - No tengan conocimiento efectivo de que la actividad o la información es ilícita o lesiona bienes o derechos de un tercero susceptibles de indemnización o;
  - Si lo tienen, actúen con diligencia para retirar los datos o hacer imposible el acceso a ello.

En febrero de 2024 entra en vigor el **Reglamento 2022/2065, de Servicios Digitales** [REF - 20], cuyo objetivo es contribuir al correcto funcionamiento de los servicios intermediarios, mejorando los mecanismos de eliminación y control de contenidos ilícitos, estableciendo normas armonizadas para todos los países miembros de la UE,

- En lo relativo a la responsabilidad de los servicios de intermediación en línea, la Ley establece, de igual modo, que las plataformas no serán responsables del comportamiento ilícito de sus usuarios, salvo que tengan conocimiento efectivo de los actos ilícitos y no los impidan. En los supuestos en los que tengan conocimiento del ilícito, estarán exentos de responsabilidad cuando actúen de manera diligente para retirar dichos contenidos.

- Sin embargo, respecto de la información que fuese generada por la propia plataforma y no por los intermediarios, esta tendría responsabilidad directa.



«Derecho al olvido: derecho de toda persona a solicitar ante los motores de búsqueda, la eliminación de su lista de resultados de publicaciones que contuviesen información personal inadecuada, excesiva o no actualizada»

5.2 Derecho al olvido

El **derecho al olvido** puede definirse como el derecho de toda persona a solicitar ante los motores de búsqueda de Internet, la eliminación de su lista de resultados de publicaciones que contuviesen información personal inadecuada, excesiva o no actualizada, exclusivamente cuando dicha búsqueda se haya realizado introduciendo su nombre.

Este derecho se recoge expresamente en el **artículo 17 del Reglamento General de Protección de Datos (RGPD)**, así como en los artículos 93 y 94 de la Ley 3/2018, de 5 de diciembre, de Protección de Datos y garantía de los derechos digitales (LOPDGDD) [REF - 21].

El derecho al olvido únicamente podrá ser ejercitado por personas físicas y no por personas jurídicas, pero entonces: ¿podrán las empresas solicitar que sea eliminada de Internet cierta información empresarial que afecta de manera negativa a su reputación?

La respuesta será sí, pero no mediante la vía de protección de datos, sino mediante las vías ordinarias que hemos visto anteriormente.

Además, habrá que tener en cuenta una serie de consideraciones:

La **empresa** podrá **solicitar** directamente al responsable/administrador de la web donde está publicada la i**nformación falsa, inexacta** o aquella que la entidad considera que está menoscabando su **derecho al honor y reputación online**, que rectifique o elimine dicho contenido, siempre y cuando no prevalezcan los principios de publicidad registral y de interés público.

En todo caso, si entendemos que dicha difusión de información empresarial pudiera ser constitutiva de cualquiera de los delitos enumerados en el apartado anterior, **la empresa podrá interponer una denuncia** a través de la **vía penal**. Además, la entidad podrá optar, en todo caso, por **exigir la responsabilidad civil** ante la Jurisdicción Civil, la cual comprenderá la restitución.

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 pautas son una serie de medidas preventivas de gestión, que contribuyen a construir una imagen sólida de la empresa, y medidas reactivas, 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.

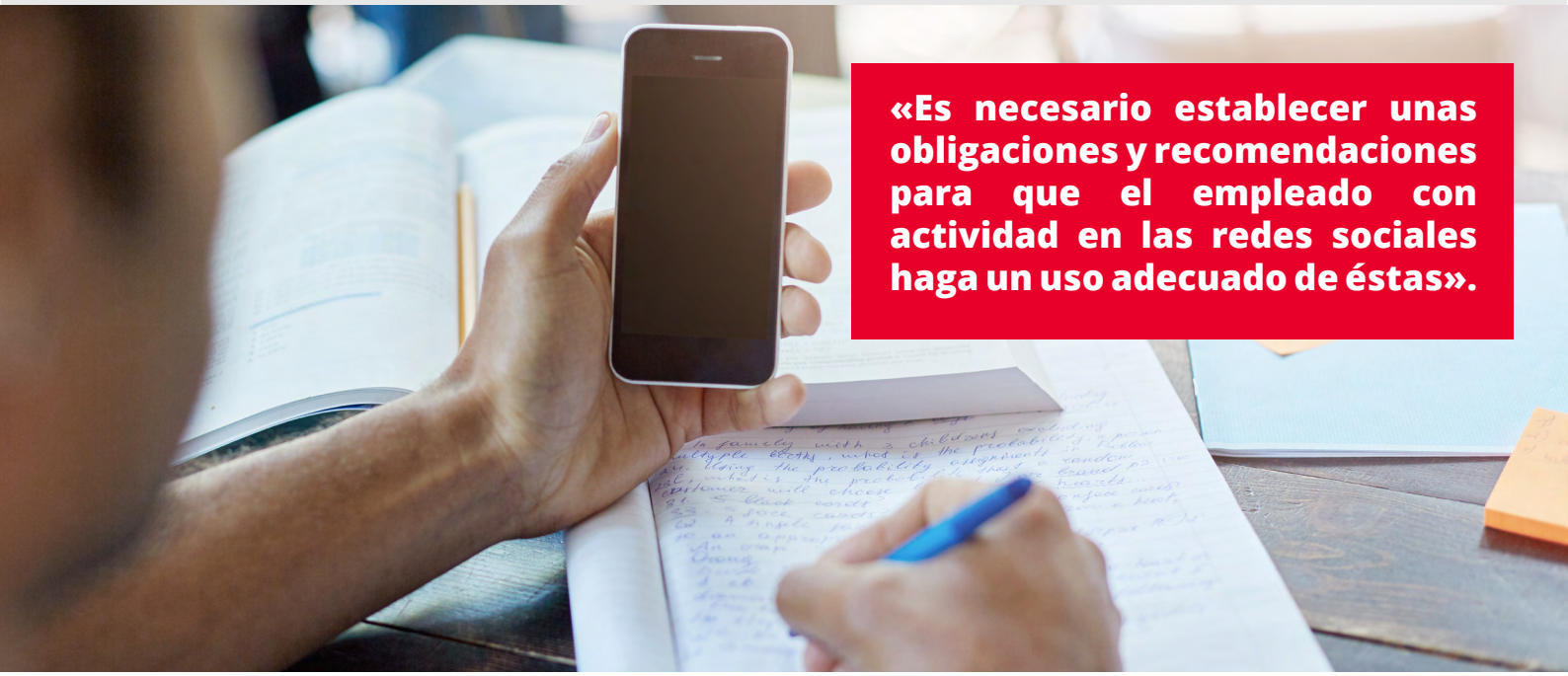
El primer paso para la gestión efectiva de la reputación de una empresa en Internet es que exista una estrategia clara por parte de la organización respecto a la definición de una identidad corporativa. ¿Qué somos como empresa?, ¿qué queremos ser? Son preguntas que la organización debe responderse, y 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 las figuras del *Community Manager* o *Social Media*.

Para establecer una estrategia de comunicación en redes sociales la empresa debe planificar y desarrollar una acción clara y coherente para mejorar su presencia en ellas.

- **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.
- **Realizar auditorías periódicas** de la presencia en línea para evaluar el impacto de las estrategias y acciones, con el objetivo de detectar posibles riesgos o identificar posibles áreas de mejora.
- **Monitorizar la reputación en línea:** realizar búsquedas periódicas de la organización en los motores de búsqueda para verificar la información existente sobre la empresa. Si hubiese contenido negativo o perjudicial, puede gestionarse ya sea solicitando su eliminación o respondiendo de manera constructiva.



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

6.1.1. 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. Esto obliga a las empresas a considerar una serie de pautas:

- **Definir qué modelos de comunicación** se desea adoptar en las interactuaciones con los usuarios en las plataformas colaborativas. En concreto, la empresa debe reflexionar acerca de, al menos, los siguientes aspectos:

- ¿Qué tipo de contenido se priorizará en las publicaciones en línea para mantener el interés y la participación de los seguidores? ¿Qué mensaje desea transmitir la empresa a sus seguidores?
- ¿Qué medidas se implementarán para garantizar un ambiente seguro y respetuoso en las interacciones con los usuarios en línea?
- ¿En qué casos se va a proporcionar respuesta a los usuarios?
- ¿Cómo se va a establecer la comunicación y el dialogo con los seguidores en las RRSS?,¿qué tipo de respuesta —personalizada, pública, privada— se va a ofrecer?, ¿la empresa o marca «dialoga» con sus seguidores?
- ¿Qué tono se va a utilizar (amigo, experto, etc.) en la relación con los usuarios?
- ¿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 para tener una estrategia que abarque las cuestiones anteriormente planteadas. 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.

6.1.2. 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, impactos económicos significativos como la disminución de ventas, costes de reparación de la reputación, desgaste en la lealtad de los clientes e impacto en la valoración de la marca.

Como ya hemos comentado, para gestionar la identidad online de las empresas, está 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 [REF - 22] por el uso de las redes sociales lo primero que debemos hacer es establecer una **política interna de uso de redes sociales** [REF - 23]. 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.

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».

- Contar con una contraseña de acceso robusta y habilitar siempre que sea posible el doble factor de autenticación [REF - 24]. De esta manera, además de tener que conocer el usuario y la contraseña para acceder a la cuenta, será necesario estar en posesión de un segundo factor, lo que aumenta considerablemente su seguridad.

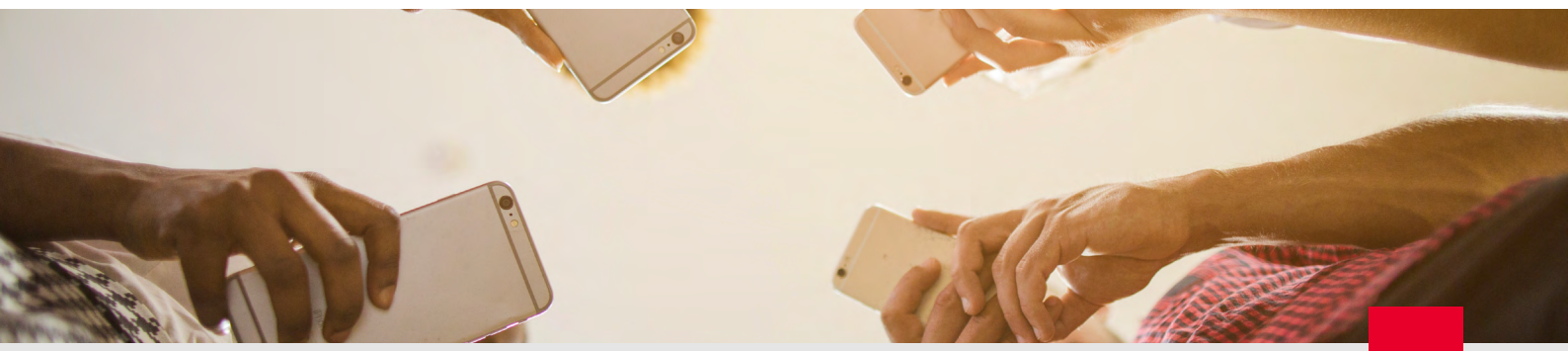
- Configurar los parámetros de privacidad de forma que permita interactuar con el público sin descuidar la seguridad y privacidad del perfil empresarial.

- Restricciones de acceso. Existen ciertas aplicaciones que por ciertos motivos (de gestión, estadísticos, publicitarios, etc.) solicitan acceso y ciertos permisos en los perfiles de nuestras redes sociales, y que debemos analizar detalladamente antes de concederles estos privilegios. De lo contrario, esta práctica puede suponer un riesgo para la privacidad, ya que podría permitir el acceso a determinados datos (como información de seguidores o clientes), que deben ser privados, o permitir la publicación de contenido no supervisado por la empresa.

- Verificar la información antes de compartirla para evitar que se produzcan rumores, *fake news*, o información que pueda dañar la reputación de la empresa.

- Elegir un responsable de publicación. Si se permite que todos los empleados tengan acceso y publiquen de forma indiscriminada, la imagen de la empresa puede verse dañada, además de aumentar el riesgo de sufrir un incidente de seguridad [REF - 25].

Definir unas normas de publicación. La organización debe definir la imagen que quiere reflejar, qué se publica y qué no, en qué tono o lenguaje, cómo se responde a las consultas de los clientes y a las quejas, etc. Hay que tener especial cuidado con el uso que se les da a nombres, logotipos y marcas de la empresa, ya que son distintivos registrados. Descuidar estas normas puede influir negativamente en la opinión que los clientes se forman sobre la empresa.



- No emitir opiniones personales de carácter político, religioso o ideológico. Estas opiniones son personales y no deben representar a la empresa.
- Evitar criticar de manera irresponsable y sin argumentos produc- tos o proyectos de la competencia.
- Responder a las consultas, preguntas, sugerencias, etc. de los seguidores de manera oportuna y personalizada para demostrar la atención hacia el cliente y fomentar una interacción positiva.
- 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 datos que pueda usar la competencia.

Es importante que los empleados conozcan tanto la política, normativa, buenas prácticas y en definitiva las reglas definidas, como 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, una para el trabajo y otra para su uso extra laboral que pueda estar vinculado con su actividad profesional como puede ser el caso de LinkedIn. 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.

6.1.3. Cumplimiento normativo

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

El incumplimiento de la legislación puede tener como consecuencia sanciones penales y económicas, con el consiguiente daño de imagen y la pérdida de confianza de nuestros clientes. Las pymes y autónomos en Internet deben cumplir las leyes que regulan aspectos como la protección de datos personales, el comercio electrónico y las transacciones online o la propiedad intelectual:

- LOPDGDD (Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales) y el reglamento europeo de protección de datos RGPD [REF - 26], para proteger la vida privada de las personas y sus datos en las comunicaciones electrónicas.
- LSSI-CE (Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico) [REF - 27] que regula los aspectos jurídicos de las actividades económicas o lucrativas del comercio electrónico, la contratación en línea, la información y la publicidad y los servicios de intermediación.
- LPI (Ley de Propiedad Intelectual), que regula los derechos relativos a las creaciones literarias, artísticas o científicas, en formatos tradicionales (fotografía, pintura, literatura...) y en formatos digitales (imágenes, videos, contenido multimedia, libros digitales...), incluido el software.
- Leyes de Propiedad Industrial [REF - 28] , que protegen diseños industriales, marcas y nombres comerciales, patentes y modelos de utilidad.
- Reglamento europeo de identificación electrónica y servicios de confianza en el mercado interior [REF - 29], para reforzar la confianza en las transacciones electrónicas entre ciudadanos, empresas y las AAPP en el marco del Mercado Único Digital Europeo.

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

6.1.4. Adopción de medidas de seguridad

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

- 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 [REF - 30], que abarquen no sólo aspectos técnicos, sino también de organización y reputacionales, orientados hacia la adopción, implementación y certificación de un Sistema de Gestión de la Seguridad de la Información.

6.1.5. Monitorización y seguimiento de la reputación online

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

- **La verificación** debe abarcar aspectos de relevancia (es decir, cuál es la posición de la empresa en los resultados ofrecidos por los buscadores en la búsqueda de materias relacionadas con las áreas de especialización de la organización o marca) y de contenido (signo positivo o negativo de la información destacada por los buscadores).

- **En el análisis**, no se deben descuidar las informaciones publicadas en foros de consumidores, medios de comunicación, sitios especializados, redes sociales, etc.

6.2 Recomendaciones reactivas

Qué ocurre cuando la empresa experimenta una crisis de reputación online o es víctima de alguna situación que exige una reacción inmediata? Seguidamente, se indican una serie de recomendaciones a seguir en estos casos. [REF - 31]

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.
Se proponen una serie de 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 las 18 horas	
FASE DE EVALUACIÓN	• Reunión del gabinete de crisis. • Principales pasos a seguir. • Tareas y planificación.	Antes de las 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 las 24 horas	*Community Manager*, Dpto. Comunicación

Tabla 1: Esquema de actuación frente a una crisis online

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 (Instagram, X, Facebook, etc.) disponen de una Política de suplantación 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:

«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».

- Denunciar perfiles falsos de Facebook
- Denunciar una cuenta que se está haciendo pasar por ti en Instagram
- Denunciar cuentas de suplantación de identidad en X
- Denunciar perfiles falsos en Linkedin

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.

Puedes ampliar esta información en el artículo: Suplantación y robo de identidad en las redes sociales, un riesgo para las empresas

6.2.2. 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, incluyendo la competencia desleal o difamación para menoscabar la credibilidad de la empresa en el mercado.

Se recomienda, por tanto, analizar la situación desde el punto de vista jurídico e iniciar las acciones que, en cada caso, procedan para proteger la imagen y los intereses comerciales de la empresa afectada.

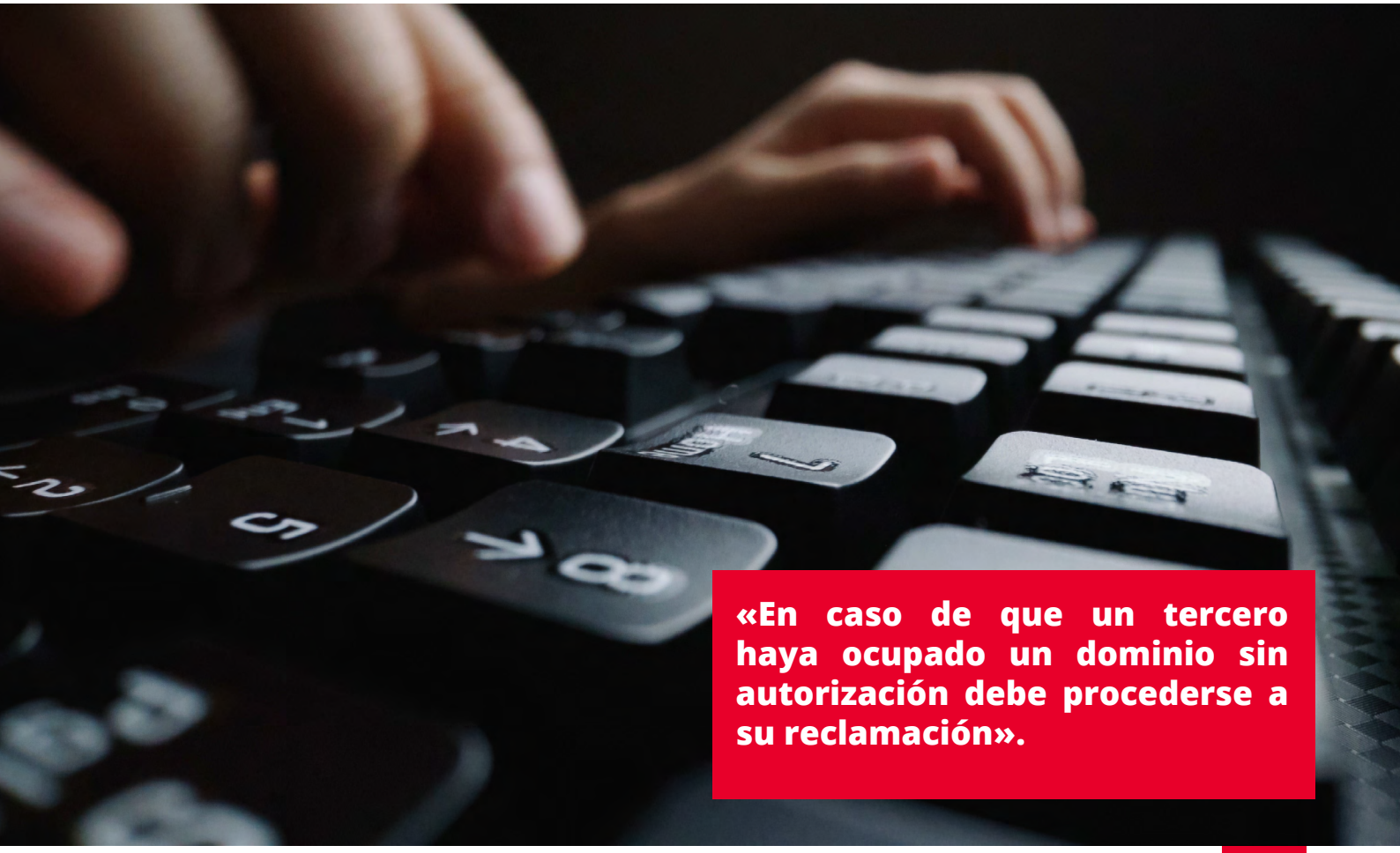
6.2.3. Recuperación del nombre de dominio

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. 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 [REF - 32].

- En segundo lugar, existe un procedimiento equivalente de la ICANN, denominado política uniforme de resolución de conflictos (UDRP) [REF -33], 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 además de la Ley 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, como es en algunos casos la utilización fraudulenta de nombres de dominio.



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

7. Referencias

[REF - 1] **TemáTICa Redes Sociales** - https://www.incibe.es/empresas/tematicas/redes-sociales

[REF - 2] **Fraude y Gestión de la Identidad Online** - https://www.incibe.es/empresas/que-te-interesa/fraude-gestion-identidad-online

[REF - 3] **Suplantación y robo de identidad en las redes sociales, un riesgo para las empresas** - https://www.incibe.es/empresas/blog/suplantacion-y-robo-identidad-las-redes-sociales-riesgo-las-empresas

[REF - 4] **Cumplimiento legal** - https://www.incibe.es/empresas/que-te-interesa/cumplimiento-legal

[REF - 5] **Glosario de términos de ciberseguridad** - https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_glosario_ciberseguridad_2021.pdf

[REF - 6] **Cybersquatting, qué es y cómo protegerse** - https://www.incibe.es/empresas/blog/cybersquatting-y-protegerse

[REF - 7] **Typosquatting** - https://www.incibe.es/aprendeciberseguridad/typosquatting

[REF - 8] **Ataques DDoS: ¿qué son y qué puedo hacer para proteger mi empresa?** - https://www.incibe.es/empresas/blog/ataques-ddos-que-son-y-que-puedo-hacer-para-proteger-mi-empresa

[REF - 9] **Qué es una botnet y cómo saber si tu empresa forma parte de ella** - https://www.incibe.es/empresas/blog/botnet-y-saber-si-tu-empresa-forma-parte-ella

[REF - 10] **Insiders: cómo atacan desde dentro** - https://www.incibe.es/empresas/blog/insiders-como-atacan-desde-dentro

[REF - 11] **Políticas de seguridad para la pyme** - https://www.incibe.es/empresas/herramientas/politicas

[REF - 12] **TemáTICas Malware** - https://www.incibe.es/empresas/tematicas/malware

[REF - 13] **El ataque del "Man in the middle" en la empresa, riesgos y formas de evitarlo** - https://www.incibe.es/empresas/blog/el-ataque-del-man-middle-empresa-riesgos-y-formas-evitarlo

[REF - 14] **BOE, Ley 3/1991, de 10 de enero, de Competencia Desleal** - https://www.boe.es/buscar/act.php?id=BOE-A-1991-628

[REF - 15] **Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen** - https://www.boe.es/buscar/act.php?id=BOE-A-1982-11196

[REF - 16] **BOE, Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal**

[REF - 17] **BOE, Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el texto refundido de la Ley de Propiedad Intelectual, regularizando, aclarando y armonizando las disposiciones legales vigentes sobre la materia** - https://www.boe.es/diario_boe/txt.php?id=BOE-A-1996-8930

[REF - 18] **BOE, Ley 17/2001, de 7 de diciembre, de Marcas** - https://www.boe.es/buscar/act.php?id=BOE-A-2001-23093

[REF - 19] **BOE, Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico** - https://www.boe.es/buscar/act.php?id=BOE-A-2002-13758

REF - 20] **BOE, Reglamento (UE) 2022/2065 del Parlamento Europeo y del Consejo de 19 de octubre de 2022 relativo a un mercado único de servicios digitales y por el que se modifica la Directiva 2000/31/CE (Reglamento de Servicios Digitales) -** https://www.boe.es/buscar/doc.php?id=DOUE-L-2022-81573

[REF - 21] **BOE, Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales -** https://www.boe.es/buscar/act.php?id=BOE-A-2018-16673

[REF - 22] **Cómo gestionar una fuga de información. Una guía de aproximación al empresario -** https://www.incibe.es/empresas/guias/guia-fuga-informacion

[REF - 23] **Política de Buenas prácticas en redes sociales -** https://www.incibe.es/sites/default/files/contenidos/politicas/documentos/buenas_practicas_rrss.pdf

[REF - 24] **Asegura tus cuentas de usuario con la autenticación de doble factor -** https://www.incibe.es/empresas/blog/asegura-tus-cuentas-usuario-autenticacion-doble-factor

[REF - 25] **Reporta tu incidente -** https://www.incibe.es/empresas/te-ayudamos/reporta-tu-incidente

[REF - 26] **Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) -** https://www.boe.es/buscar/doc.php?id=DOUE-L-2016-80807

[REF - 27] **LSSI -** https://lssi.mineco.gob.es/paginas/Index.aspx

[REF - 28] **Propiedad Industrial -** https://www.boe.es/biblioteca_juridica/codigos/codigo.php?id=067_Propiedad_Industrial&tipo=C&modo=2

[REF - 29] **BOE, REGLAMENTO (UE) No 910/2014 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 23 de julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE -** https://www.boe.es/doue/2014/257/L00073-00114.pdf

[REF - 30] **Política de Continuidad de negocio -** https://www.incibe.es/sites/default/files/contenidos/politicas/documentos/continuidad-negocio.pdf

[REF - 31] **¿Cómo defender la reputación de mi negocio frente a las reseñas falsas? -** https://www.incibe.es/empresas/blog/como-defender-la-reputacion-de-mi-negocio-frente-las-resenas-falsas

[REF - 32] **Recupera tu dominio -** https://www.dominios.es/es/gestiona-tu-dominio/recupera-tu-dominio

[REF -33] **ICANN, UDRP -** https://www.icann.org/resources/pages/enforcing-udrp-2013-07-16-es

Financiado por la Unión Europea NextGenerationEU

Gobierno de España · Vicepresidencia Primera del Gobierno · Ministerio de Asuntos Económicos y Transformación Digital · Secretaría de Estado de Digitalización e Inteligencia Artificial

Plan de Recuperación, Transformación y Resiliencia

España | digital 2026

incibe_ Instituto Nacional de Ciberseguridad

protege tu empresa