

# Gestión de riesgos en la identidad digital

**Author :** a.h.

**Categories :** [Auditoría, Certificación y Calidad de Sistemas Informáticos](#)

**Date :** 21 noviembre, 2018

La probabilidad de que ocurra un contratiempo o de que alguien o algo sufra algún tipo de perjuicio o daño es algo inevitable. Esta ineludible posibilidad se denomina "riesgo". Una vez comprendemos que el riesgo 0 es imposible, nuestra labor es tratar de **reducir la probabilidad** de que el contratiempo ocurra, **disminuir sus efectos** y **saber qué hacer** en caso de que pase. Y es de esto de lo que voy a hablar en este tercer post, dentro de la secuencia que estoy realizando sobre la identidad digital.

Primero de todo, mencionar que se debe actuar sobre 3 elementos diferentes a la hora de gestionar una buena reputación online y son los siguientes: el contenido online que yo genero, el contenido que se genera sobre nosotros por parte de terceros y el contenido que se genera en el marco de las relaciones con los demás.

Otra cosa que debemos tener en cuenta es que la identidad es contextual. Esto significa que puede generar un impacto negativo si se emplea en un contexto erróneo. Es por ello que mantener las identidades analógica y digital separadas entre sí es positivo [1].

-

Es el momento de volver a mencionar conceptos previamente citados en la introducción realizada en el primer post sobre Identidad Digital, pero esta vez explicando a fondo dichos riesgos.

1. **Suplantación de identidad digital.** Esto ocurre cuando una persona se hace pasar por otra con el fin de obtener un beneficio [2]. Una posible aplicación de este hecho delictivo podría ser que alguien se hiciera pasar por la organización COMIDA y que bombardeara a clientes habituales de esta empresa por email o RRSS. Estos emails o mensajes pedirán al cliente que done una cantidad simbólica a un número de cuenta determinado para colaborar con un comedor social. De esta forma, la entidad COMIDA se vería afectada a pesar de posiblemente no ser consciente del suceso.
2. **Utilización de derechos de propiedad industrial por terceros no autorizados.** Los derechos de propiedad industrial tienen una doble dimensión; permitir a su propietario su utilización e impedir a terceros usarlo. Si se infringe esto por un tercero, la entidad propietaria se convierte en víctima y deben denunciar a las autoridades. Esto puede ser cometido debido a la falsa sensación de que en Internet “todo vale” o por terceros malintencionados para divulgar elementos del negocio como patentes o secretos industriales.
3. **Amenazas a la reputación online.** Esta amenaza se refiere a las acciones que pueden crear una opinión negativa en el *target* sobre una determinada organización o persona. Esto puede ser producido por diferentes entes:
  1. Por la empresa o persona en sí.
  2. Por terceros que publican información del sujeto.
  3. Por los internautas con los que nos relacionamos.

Estos tres puntos son los que he mencionado anteriormente que se debe actuar para lograr una buena reputación online, pero que también pueden hacernos lograr justo lo opuesto.

4. **Registro abusivo del nombre de dominio.** Hoy en día, la mayoría de las empresas cuenta con una página web. Esta página suele tener como nombre el de la marca en sí o el de sus productos. De esta forma, los usuarios pueden identificar de forma rápida la organización detrás de la página web. El problema está en que no existe ningún control a la hora de registrar el nombre del dominio. Por lo tanto, terceros pueden registrar de manera malintencionada nombres de dominio que coincidan con entidades reconocidas para confundir a los internautas. Esto se conoce como **cybersquatting** en el caso de que se extorsiona a la entidad *target* para vender el dominio por un valor mayor al real. Si el objetivo es que los usuarios entren por escribir mal el dominio (como por ejemplo, “facebok” en lugar de “facebook”) se denomina **typosquatting**. Este último ataque se realiza como base de *phising*.
5. **Fuga de información.** La imagen de una organización puede verse comprometida debido a una fuga de contenido sensible. El objetivo principal de esta práctica por parte del atacante suele ser extorsionar a la entidad. El origen de esta dañina fuga puede ser interno (*insider threats*) o externo (mediante *malware* o técnicas como la mencionada y popular *phising*) [3].

Estos son los principales riesgos que tiene la identidad digital hoy en día. Como *spoiler* de mi próximo post, la imagen que se muestra a continuación da una breve explicación de las pautas de prevención y reacción que se deben de llevar a cabo para hacer frente a los riesgos.

**inteco** **IDENTIDAD DIGITAL**  
LA REPUTACIÓN ONLINE DE LAS EMPRESAS  
Instituto Nacional de Tecnologías de la Comunicación

**IMPORTANCIA DE GESTIONAR LA PRESENCIA EN INTERNET**



**1 de cada 2 empresas** está presente en Internet...

**@**  
... de forma activa

... o por lo que clientes o usuarios publican

Las empresas tienen una **reputación online**, basada en la valoración de los internautas.

**ATAQUES A LA REPUTACIÓN ONLINE CORPORATIVA**

**Suplantación** en el envío de emails a nombre de la empresa. 

---

Registro no autorizado del nombre de dominio o **ciberocupación del dominio**. 

---

**Ataques de seguridad** que provocan la caída de la web de la empresa. 

---

Filtración en Internet de información confidencial del negocio o **fuga de información**. 

---

**Comentarios falsos o negativos** en redes sociales que perjudican a la compañía. 

---

Utilización no consentida de la **propiedad intelectual** de la empresa. 

**RECOMENDACIONES PARA LA ADECUADA GESTIÓN DE LA IDENTIDAD DIGITAL Y LA REPUTACIÓN ONLINE CORPORATIVAS**

**PAUTAS DE PREVENCIÓN**

- ✓ Define una estrategia de identidad corporativa clara
- ✓ Interactúa y establece relaciones de confianza con los usuarios
- ✓ Cumple las normas para tener una buena salud reputacional
- ✓ Adopta medidas de seguridad para evitar ataques online
- ✓ Haz un seguimiento planificado de tu reputación online

**PAUTAS DE REACCIÓN**

- ✓ Establece una estrategia de actuación para hacer frente a situaciones de crisis online
- ✓ Utiliza los canales de denuncia internos de las plataformas de medios sociales
- ✓ Acude a la Policía y/o la Guardia Civil para denunciar los posibles delitos informáticos
- ✓ Solicita la recuperación del nombre del dominio ante las autoridades competentes

**MÁS INFORMACIÓN**

Guía para empresas: identidad digital y reputación online.  
[http://www.inteco.es/Seguridad/Observatorio/Guias/Guia\\_Identidad\\_Reputacion\\_Empresas](http://www.inteco.es/Seguridad/Observatorio/Guias/Guia_Identidad_Reputacion_Empresas)

**inteco**

- [1] "Identidad digital los riesgos de no administrarla", acceso el 21 de noviembre de 2018. [http://www.academia.edu/9552365/Identidad\\_digital\\_los\\_riesgos\\_de\\_no\\_administrarla](http://www.academia.edu/9552365/Identidad_digital_los_riesgos_de_no_administrarla)
- [2] "El delito de suplantación de identidad", acceso el 21 de noviembre de 2018. <https://juiciopenal.com/delitos/suplantacion/delito-suplantacion-identidad/>
- [3] "Ciberseguridad en la identidad digital y la reputación online" , acceso el 21 de noviembre de 2018.  
[https://www.incibe.es/extfrontinteco/img/File/empresas/guias/guia\\_ciberseguridad\\_identidad\\_online.pdf](https://www.incibe.es/extfrontinteco/img/File/empresas/guias/guia_ciberseguridad_identidad_online.pdf)
- [4] "Infografía", acceso el 21 de noviembre de 2018. <https://www.incibe.es/protege-tu-empresa/blog/infografia-id-empresas>