universidad de león

aeiseguridad
Agrupación Empresarial Innovadora para la seguridad de las redes y los sistemas de información

INTECO
Instituto Nacional de Tecnologías de la Comunicación

MÁSTER PROFESIONAL EN TECNOLOGÍAS DE SEGURIDAD

TERCERA EDICIÓN

Definición e implantación de la Reputación Web

Ángel Castellanos González

Índice

Índice de Ilustraciones

Abstract

En este proyecto se ha realizado una investigación teórica sobre los aspectos que afectan a la Reputación Web y la especial importancia que, dentro de estos, tienen aquellos que afectan a la Seguridad Informática. La investigación se plantea sobre el contexto actual de la Web 2.0 y sus aspectos diferenciadores (inmediatez, globalización de la información y facilidad en la generación de contenido por parte de los usuarios finales). Ante estos aspectos potencialmente peligrosos para la Reputación Web se ha investigado sobre los métodos de protección más eficaces, tanto aquellos empleados en la actualidad, como los que presumiblemente serán implementados en un futuro cercano para dar respuesta a las nuevas amenazas.

Keywords

Reputación Web, Web 2.0, Seguridad Web, Seguridad Informática, Amenazas, Vulnerabilidades

1 Introducción

Entendiendo por reputación:

Reputacion:

1. *Opinión o consideración en que se tiene a alguien o algo*
2. *Fama, prestigio*

Podemos definir **Reputación Web** o **Reputación Online** como el reflejo del prestigio de una persona, entidad o marca en Internet. Aunque en un principio se incluía dentro de la reputación general de una entidad, la importancia que está cobrando en la actualidad hace que cada vez más se tome como un concepto diferenciado a tener muy en cuenta.

La Reputación Web de una entidad es fabricada por el conjunto de los usuarios que sobre ella opinen en Internet y es difícilmente controlable por parte de la propia entidad. Si ya de por si es difícil para una entidad controlar la opinión vertida por los internautas con el auge de la **Web 2.0**, que permite la creación de contenidos por parte de cualquier usuario, se torna una labor prácticamente imposible.

Otro de los aspectos diferenciadores de la Reputación Web respecto al concepto tradicional de Reputación es precisamente su carácter online. Internet ofrece un canal de distribución en el cual la información está disponible en cualquier parte del mundo de manera inmediata. De esta manera las opiniones que antes quedaban inscritas en un entorno reducido (amigos, familia, trabajo)

ahora son potencialmente accesibles a cualquier persona en cualquier parte del mundo.

Es importante destacar los consumidores son cada vez más sensibles a las opiniones de otros usuarios a la hora de comprar un producto o servicio, dándolas importancia por encima incluso de las campañas publicitarias.

Por todos estos aspectos la Reputación Web debe ser considerada un arma de doble filo. Puede ser el mejor aliado ofreciendo un canal de distribución inmediato sin límite geográfico a muy bajo coste para los productos de una entidad o para las opiniones positivas del público; sin embargo, también puede ser el mayor enemigo de la imagen de una compañía ya que cualquier incidente, problema u opinión negativa tendrá una gran difusión entre el gran público, pudiendo afectar al negocio de la entidad.

En este sentido la Seguridad Informática es uno de los factores que más puede afectar negativamente a la reputación Web, si no el que más. Por ello debería ser uno de los ejes centrales en la gestión de la Reputación Web, definiendo los métodos de protección adecuados al ámbito de actuación de cada entidad.

Cabe resaltar también que debido al contexto en continuo cambio en que se mueven, los métodos de protección ante problemas de seguridad informática deben ser altamente adaptables.

Finalmente es necesario plantear el desarrollo futuro de la Seguridad Informática en el ámbito de la Web 2.0, teniendo en cuenta las previsiones de futuro de esta, con la incertidumbre que lleva asociada.

2 Contexto Actual: Web 2.0

El contexto actual de Internet es muy diferente al de hace apenas unos años. Hasta hace unos años los datos de la Red eran generados por un reducido número de “creadores” especializados en este aspecto y eran consumidos por el gran público.

En la actualidad han desaparecido los roles de “creador” y “consumidor” de información en que hasta ahora habían existido; en lugar de ello hoy en día cualquier persona puede ser tanto creadora como consumidora de información. Es lo que Tim O’Reilly distinguió como Web 2.0 en contraposición a la Web 1.0 tradicional [1];

Tim O’Reilly concluyó que la Web 2.0 se sostiene sobre 7 conceptos básicos:

- La *World Wide Web* como plataforma de trabajo.
- El fortalecimiento de la inteligencia colectiva.
- La gestión de las bases de datos como competencia básica.
- El fin del ciclo de las actualizaciones de versiones del software.
- Los modelos de programación ligera junto con la búsqueda de la simplicidad.
- El software no limitado a un solo dispositivo.
- Las experiencias enriquecedoras de los usuarios.

La Web 2.0 ha hecho que la cantidad de información existente en la Web haya crecido de manera exponencial.

En la **Figura 1** se muestra la evolución del crecimiento de los sitios Web en los últimos 8 años. A raíz de la expansión de la Web 2.0 la pendiente de crecimiento se ha ido incrementando gradualmente. En la **Figura 2** se muestran varios ejemplos gráficos del crecimiento esperado de la información en el ámbito de Internet. Se puede ver que, aunque en estos años la Web ha experimentado un crecimiento muy grande, en los años venideros se prevé un crecimiento aún mayor impulsado por el desarrollo de la Web 2.0.

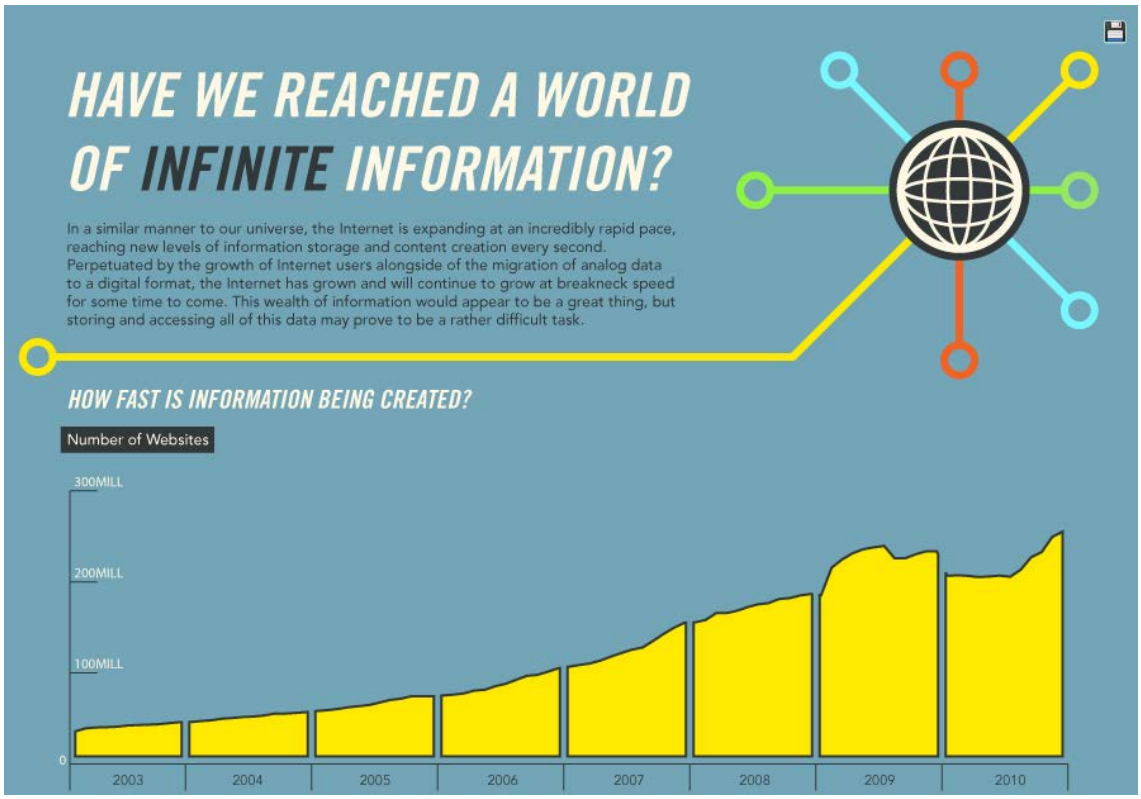

Figura 1- Evolución del número de WebSites *[2]*

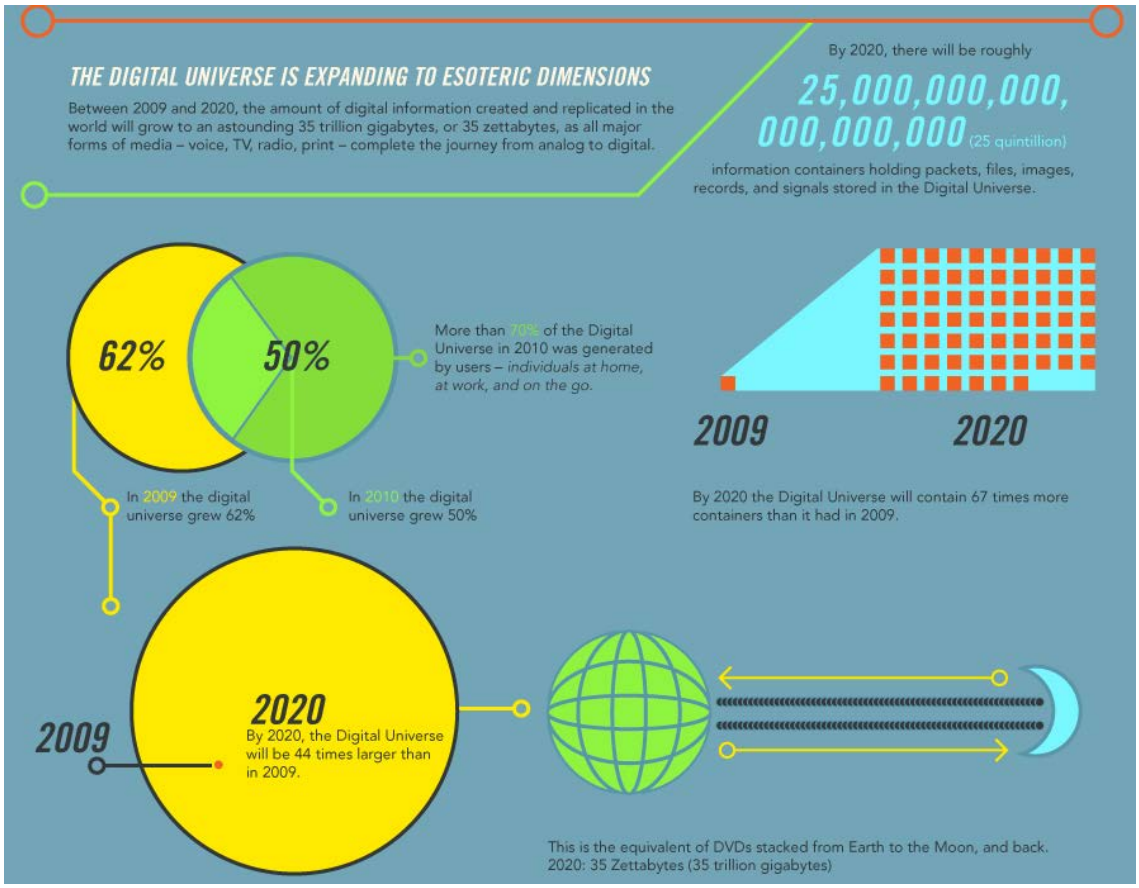

Figura 2- Crecimiento de la información presente en Internet *[2]*

2.1 Software Social

En este contexto han aparecido nuevas herramientas cuyo funcionamiento se basa en el desarrollo colaborativo por parte de sus usuarios. Es lo que se conoce como Software Social. El Software Social a menudo presenta las siguientes características:

- Admiten la participación colectiva, permitiendo:
    - Compartir información entre los usuarios.
    - Interactuar unas personas con otras, por ejemplo, mediante sistemas de mensajes.
    - Colaborar entre usuarios. La información compartida unido a la interacción entre los usuarios debe permitir la creación conjunta de contenidos
- El uso del recurso es gratuito.
- Permite recuperar la información mediante suscripción (sindicación) al que se puede añadir el etiquetado (folksonomía).

En la **Tabla 1** se pueden ver la evolución de la Web 1.0 a la 2.0 a través de las herramientas utilizadas en cada una de ellas y como se ha ido migrando de aplicaciones estáticas que no permitían apenas interacción con el usuario a herramientas de Software Social.

En la **Figura 3** se muestra un mapa categorizando las principales herramientas características de la Web 2.0

WEB 1.0	WEB 2.0
DoubleClick	AdSense
Ofoto	Flickr
Terratv	Youtube
Akamai	BitTorrent
Enciclopedia Británica	Wikipedia
Web personales	Blogging
Sistema de gestión de contenidos	Wiki
Hotmails	Facebook
Directorios (Taxonomía)	Etiquetas (folcsonomía)

Tabla 1- Comparativa de Herramientas 1.0 y 2.0

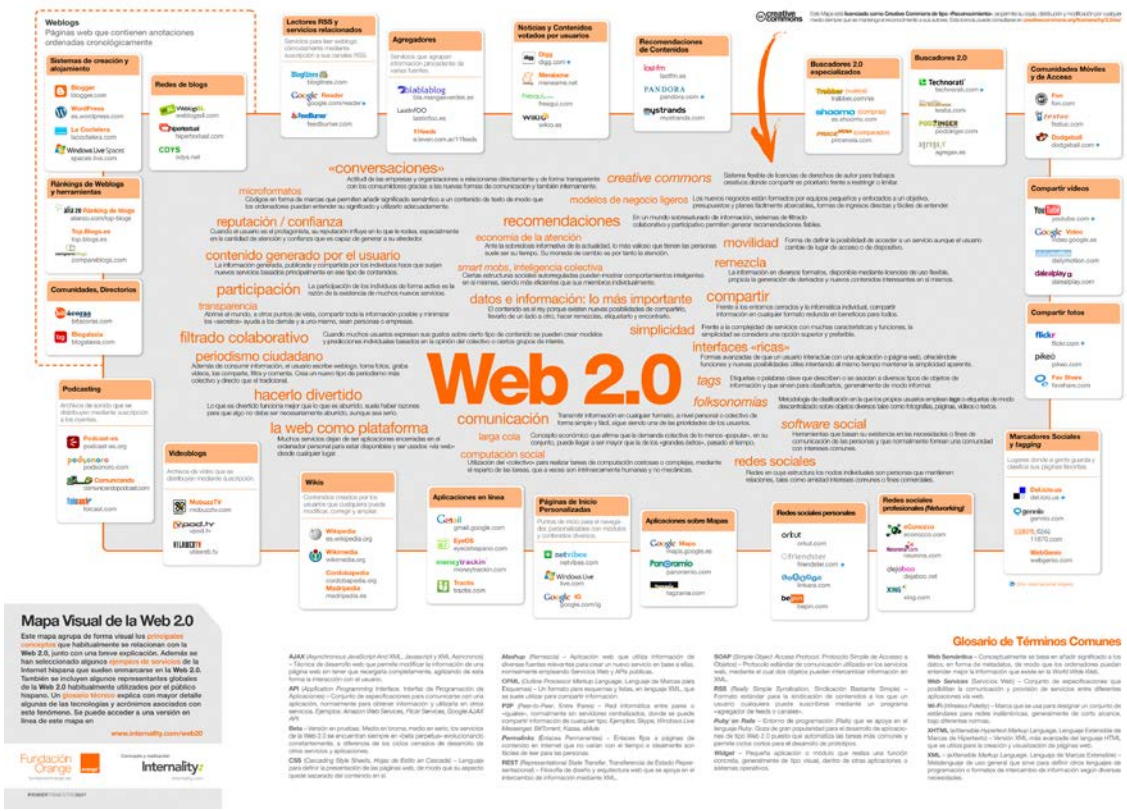

Figura 3- Mapa de la Web 2.0

2.2 Clasificación de la información

Como se ha visto la Web 2.0 ha ofrecido a los usuarios nuevas formas de creación y edición de información. Esto hace que sea necesario también desarrollar nuevas maneras de gestionar esta información para facilitar el acceso a ella.

Esta situación se ha convertido en un arma de doble filo. Aunque teóricamente se puede acceder a prácticamente cualquier información a través de Internet, se plantea el problema de filtrar la ingente cantidad de datos presentes en la Red para seleccionar únicamente aquellos que sean de interés. En este sentido se han desarrollado gran cantidad de trabajos orientados a intentar tratar con el enorme flujo de información derivado de la Web 2.0 [3]

Uno de los conceptos más importantes a este respecto es el de **folcsonomía;** esto es, la capacidad del usuario para etiquetar un contenido determinado según su criterio, frente al concepto tradicional de **taxonomía**, en el cual las categorías estaban ya definidas. La principal ventaja que aporta este nuevo enfoque es el *feedback* entre usuarios que es posible con el concepto de folcsonomía.

A menudo se ha planteado el uso de folcsonomías como medio para la clasificación de información [4; 5] Se presenta como el método más lógico, en un contexto en que los contenidos son generados mayoritariamente de manera "social" parece lógico que la clasificación se haga también de manera social por parte de los propios usuarios; sin embargo, la libertad en la elección de

etiquetas hace que los resultados devueltos puedan ser inconsistentes (apariciones de etiquetas sinónimas o polisémicas)

2.3 Reputación Web en la Web 2.0

Como se ha planteado la Web 2.0 domina el escenario actual de Internet y su importancia parece que no dejará de aumentar en el futuro. Por tanto, es necesario adaptarse a las peculiaridades que la Web 2.0 conlleva: grandes cantidades de información, dificultad de clasificación, inmediatez, generación social de contenidos, globalización… .

Todas estas peculiaridades definen un escenario en el cual controlar la reputación Web se hace una tarea prácticamente imposible y al que sin embargo es indispensable adaptarse. La gestión de la reputación en la Web 2.0 se centra en 2 aspectos principales:

- **Usar la Web 2.0 para crear o mejorar la reputación Web:**

  De un informe realizado por Cone en EEUU se extraen los siguientes datos:

  - 93% de los estadounidenses piensa que las empresas deben tener presencia en la Web 2.0
  - 85% piensa que no solo deberían tener presencia si no que deberían interactuar con sus clientes a través de la Web 2.0

  De estos datos se desprende la importancia que para los usuarios tiene la presencia de las empresas en los medios sociales.

- **Usar la Web 2.0 para monitorizar la reputación que perciben los usuarios sobre una entidad.**

  La Web 2.0 es una herramienta excelente para pulsar la opinión de los usuarios de una determinada compañía. Las opiniones personales que antes quedaban circunscritas a un ámbito privado ahora son expresadas en Internet, por lo que cualquiera puede tener acceso a ellas y servir como aprendizaje.

  Las conclusiones extraídas de la monitorización servirán como *feedback* para mejorar la reputación en la Web 2.0.

  En este sentido existen trabajos que pretenden establecer medios para medir cuantitativamente la reputación web [6]

3 Factores que afectan a la Reputación Web

Hasta ahora se ha planteado el contexto actual de la Web 2.0, el enorme potencial que tiene asociado y las oportunidades asociadas a este potencial. Sin embargo, como suele ocurrir, las grandes oportunidades de la Web 2.0

tienen asociadas unas amenazas igualmente importantes, especialmente fijándose en el ámbito de la Reputación Web.

Al igual que se magnifica la capacidad de distribución de nuestra información con la Web 2.0, también se magnifican los errores. Además, puesto que la información es generada de manera distribuida por los usuarios, es imposible controlar el flujo de información una vez puesto en marcha. Se debe tener en consideración la persistencia de esta información, a diferencia de otros medios Internet permite que una vez publicada una información esta perdure en el tiempo.

Un fenómeno que también se debe tener en cuenta es que los usuarios cada vez otorgan más importancia a las opiniones que otros usuarios ofrecen a través de la red:

> *"El 84% de los americanos reconocen que las críticas on-line influyen en sus decisiones de compra."*

A ojos de los usuarios finales cualquier circunstancia negativa asociada a una entidad puede enturbiar totalmente la imagen de la compañía. Hay que tener en cuenta que una mala reputación Web puede ser un factor determinante para el fracaso de una entidad, ya no solo a nivel online, sino a nivel general.

Con todo esto se dibuja una situación en la que la información que afecta a la reputación Web de una empresa es generada, en cantidades masivas y sin posibilidad alguna de control, por los propios usuarios, siendo esta información altamente valorada por el gran público y además si esta información es negativa puede incluso llevar a una entidad a la quiebra.

Se hace por tanto necesario llevar una monitorización como ya hemos comentado para evitar casos que dañen la reputación web. Existen numerosos casos en los cuales la mala gestión de la reputación web (o la falta de esta) por parte de algunas entidades ha causado grandes perjuicios a estas:

- **Caso Pixmanía[1]:** Debido a un error en su tienda online, Pixmanía ofrecía uno de sus productos a un precio sensiblemente inferior a su precio de mercado (**Figura 4**). Esto se propago rápidamente por la red (de nuevo la inmediatez de la Web 2.0 sale a relucir) y cientos de personas compraron el producto.

  La reacción de Pixmanía fue cancelar todos los encargos y responsabilizar de esto a sus usuarios dejando su reputación online por los suelos.

[1] http://www.reputationmanagement.es/?p=15

Figura 4- Error en la tienda online de Pixmanía

- **Caso Actimel:** Las opiniones provenientes de un foro de usuarios en Argentina crearon un rumor acerca de los perjuicios de tomar este producto. La información se propagó rápidamente por la red y debido a que, como ya hemos comentado, a menudo los usuarios dan mucha credibilidad a las opiniones de otros usuarios, esta información fue tomada como real.

  El caso llega a tal punto que aún hoy en día si se busca la palabra *actimel* en Google, la segunda opción sugerida por Google Suggest es **perjudicial** (**Figura 5**).

  En este caso la pérdida de reputación web no viene de una mala actuación de la entidad (Danone en este caso), sino que se produce por una mala gestión de esta de su reputación web. Al no monitorizar la red en busca de este tipo de situaciones.

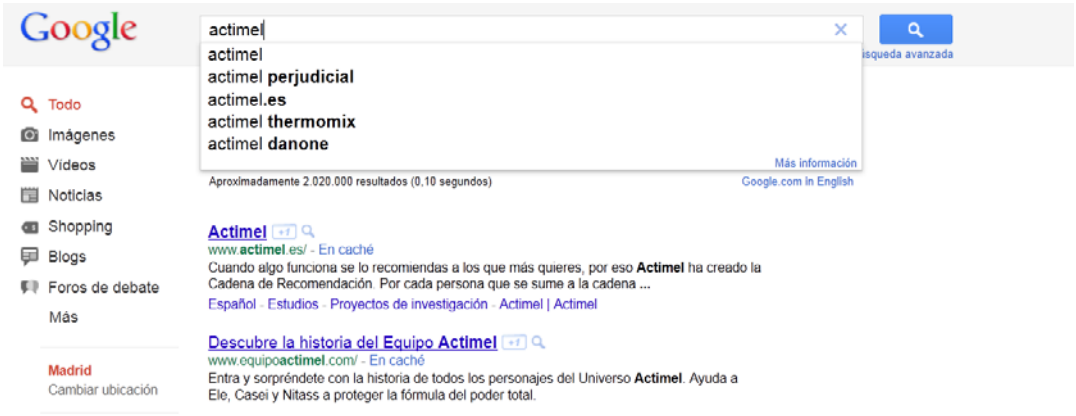

Figura 5- Resultados de Google Suggest para actimel

- **Caso Equipo de Obama:** Un miembro del equipo de Barack Obama (Jon Favreu) fue descubierto en una foto en una actitud irrespetuosa con la entonces rival de Obama, Hillary Clinton (**Figura 6**)

Esta foto fue descubierta en Facebook y aunque inmediatamente se retiró, esto no evitó su difusión por todo Internet.

En este caso el afectado por la pérdida de reputación web no fue una entidad sino un particular, algo que en el futuro ocurrirá cada vez con más frecuencia. La gestión de la reputación online va a ser algo que también tengan que tener en cuenta los usuarios de Internet, especialmente si estos usuarios tienen una visibilidad pública como en este caso.

Este caso también sirve para mostrar los "peligros" de las redes sociales. En ellas es difícil saber quién accede a la información mostrada en ellas por lo que se hace difícil mantener como **privado** un contenido que se haya subido a alguna de las distintas redes sociales. Los usuarios de estos servicios tienen que tener especial cuidado con los contenidos compartidos.

Figura 6 - Imagen de la polémica de Jon Favreu

Por todo ello se hace patente que la Reputación Web es uno de los aspectos a los que las entidades deben prestar más atención, por lo que deben tener bajo control todos y cada uno de los aspectos que puedan influir en ella tanto positiva como negativamente. Los factores que afectan en mayor medida a la reputación Web y que por tanto más deben tener en cuenta son:

- **Operaciones de Negocio "cuestionables":** Se producen cuando una compañía actúa, en su funcionamiento diario, de forma negativa contra sus clientes o socios. Los clientes verán rebajada su confianza en la compañía al no considerar ético su comportamiento.

  El caso de Pixmanía es un ejemplo de esto. La compañía responsabiliza de un fallo suyo a sus clientes haciendo que estos pierdan la confianza depositada.

- **Movimientos corporativos:** Relativo a los movimientos económicos realizados por la empresa. El público puede considerar, al igual que en el caso anterior, que no son todo lo transparentes que deberían ser.

  Estos movimientos suelen estar relacionados con los acuerdos comerciales con otro tipo de entidades de dudosa reputación.

- **Procesos legales:** La entidad se ve involucrada en un proceso judicial por alguna desavenencia con un tercero. Es uno de los factores que más pueden afectar a la Reputación de una empresa ya que los clientes tienden a pensar que las actividades de la empresa van en contra de la legalidad. Aún en el caso de salir victorioso del proceso judicial es muy difícil “limpiar” la imagen y recuperar la reputación perdida.

- **Rumores:** Informaciones falsas negativas sobre una entidad. Se suelen difundir por parte de competidores con la motivación de dañar la imagen de la compañía. Si los usuarios los toman como verdaderos pueden dañar seriamente la reputación de la entidad; sin embargo, son más sencillos de rebatir al estar basados en informaciones falsas.

  Este es uno de los casos donde con mayor claridad se ve la importancia que tiene tener una buena reputación Web. Si la entidad posee un bagaje en la Web y su credibilidad es buena, el simple hecho de desmentir el rumor reducirá el daño sobre su reputación. Además, el hecho de tener una presencia importante en la Web ayudará a difundir la réplica al rumor.

  También es necesario como se ha visto en el caso Acitmel, monitorizar la red constantemente en busca de este tipo de informaciones, ya que cuanto antes se descubran menos difusión tendrán y más fácil será atacar el problema.

- **Escándalos:** Son similares a los rumores, se trata de informaciones que afectan directamente a la reputación de una entidad y suelen estar relacionadas con una actuación de esta o de uno de sus empleados. A diferencia de los rumores los escándalos están basado en pruebas contrastadas y son difícilmente subsanables.

  El caso del miembro del equipo de Barack Obama es un claro ejemplo de este tipo. En él la actuación de una única persona puede afectar a la reputación web de toda una organización o campaña, por lo que las organizaciones tienen que concienciar a todos sus empleados (especialmente a aquellos de mayor visibildad) de la importancia de gestionar su reputación web.

4 Impacto de la Seguridad Informática en la Reputación Web

Incluir en alguna parte introducción sobre SI

Se entiende por Seguridad Informática al área de la Informática en la cual se estudia la protección de los sistemas (físicos y lógicos) contra ataques, internos y externos, que afecten a su funcionamiento, ya sean estos ataques fortuitos o deliberados. La Seguridad Informática abarca un gran número de campos (programación, redes, criptografía) relacionados en mayor o menor medida con la Informática.

Centrándose en el concepto de la Seguridad Informática, esta afecta transversalmente a todos los factores relacionados con la Reputación Web expuestos en el punto anterior; sin embargo, si hay alguno al que pueden afectar en mayor medida es al de los escándalos.

Se suele relacionar a los escándalos con la actuación de alguna persona relacionada con la entidad, pero a menudo una fuente de escándalos son los fallos tecnológicos que afectan en mayor o menor medida a la actividad de la entidad.

Los fallos relacionados con la Seguridad Informática son una de las principales causas de estos fallos tecnológicos. Además hay que tener en cuenta que a menudo los problemas relacionados con la Seguridad Informática tienen un gran impacto en las actividades de negocio de una entidad y una repercusión enorme. Es por ello que si una entidad logra reducir o eliminar sus problemas debidos a fallos de Seguridad Informática, de manera indirecta, su reputación web se verá incrementada.

A continuación se muestran algunos ejemplos de problemas de seguridad informática que afectaron de manera negativa a la reputación web de los atacados:

- **Los hackers acceden al programa de cazas de EEUU:** Los hackers han accedido repetidamente al más costoso programa armamentístico del Pentágono, el proyecto Joint Strike Fighter, de unos 300.000 millones de dólares (unos 229.000 millones de euros)

  http://www.20minutos.es/noticia/464233/0/PENTAGONO/ESPIONAJE/

- **INTECO sufre el mayor ataque desde su creación:** Bajo el lema “que confianza online pueden ofrecer cuando ellos no son ni seguros”, un grupo de hackers ha asaltado la plataforma de formación online de INTECO, en lo que supone el mayor ataque desde su creación en 2005, y ha robado los datos personales de más de 20.000 usuarios. INTECO asegura, en su Web, que ha adoptado las medidas necesarias para minimizar los daños de los usuarios de la plataforma.

  http://www.idg.es/dealerworld/INTECO-sufre-el-mayor-ataque-desde-su-creacion/seccion-actualidad/noticia-110571

5 Protección ante amenazas de S.I. relacionadas Reputación Web

Como se ha expuesto en el punto anterior los fallos debidos a problemas de seguridad informática tienen una gran repercusión en la reputación web de una empresa y por ende en la actividad de negocio de esta. A continuación se exponen las más importantes de estas amenazas y se plantean los métodos de protección más habituales contra ellas.

5.1 Principales amenazas

- **Hacking:** Acciones ("ataques") llevadas a cabo por usuarios con grandes conocimientos en seguridad informática contra los sistemas de una determinada entidad. Estas acciones suelen ser desarrolladas por personas sin ánimo de atentar contra los intereses de la entidad, en su lugar están movidas por otra motivaciones (realización personal, alertar sobre vulnerabilidades, diversión…).

  A menudo no causan un impacto real sobre la actividad del atacado; sin embargo, tiene un impacto negativo en la Reputación Web al hacer ver a la comunidad de usuarios que los sistemas de la entidad atacada son vulnerables.

  Cuando el ánimo de estas acciones es el de causar algún perjuicio se denominan como **cracking***.* A diferencia del hacking, el cracking suele llevar implícito un gran impacto en la actividad del atacado, llegando incluso a paralizar sus sistemas. Su repercusión negativa en la reputación web es aún mayor ya que no solo se muestras que los sistemas de determinada compañía son vulnerables, sino que además, dichos sistemas pueden quedar inoperativos durante horas o días:

  - **Un joven de 19 años creador del virus Blaster:** Un joven estadounidense Jeffrey Lee Parson de 19 años se ha declarado culpable de crear y propagar el virus Blaster.b que infectó unas 400.000 computadoras.

    http://www.technewsworld.com/story/35820.html

- **Malware:** Programas cuyo funcionamiento está enfocado a realizar algún daño sobre el equipo víctima. Estos programas se pueden crear para tal fin o pueden ser programas lícitos cuyo código ha sido modificado.

  El malware es distribuido por la red de muy diversas maneras (correo electrónico, páginas fraudulentas, archivos infectados) o también de manera física (usb o discos ópticos infectados). El malware busca obtener acceso al equipo de la víctima (en este caso la entidad objetivo) y de esta manera acceder a todos los datos del equipo o modificar el funcionamiento de este para realizar acciones fraudulentas.

  A diferencia de hace unos años hoy en día el malware busca camuflarse en el ordenador de la víctima sin hacer notar su presencia. De esta forma la víctima a pesar de estar infectada no es consciente de ello.

- **Ingeniería Social:** Se conoce como Ingeniería Social los métodos enfocados a engañar a los usuarios de modo que estos de manera voluntaria faciliten a un tercero (el atacante) información sensible o acceso a su equipo. No aprovecha fallos tecnológicos, en su lugar están enfocados a la psicología de los usuarios.

  Estos ataques suelen estar enfocados contra los usuarios de una entidad en lugar de contra la propia entidad

  Aunque la ingeniería social no es un fallo de seguridad al uso (no se explota ninguna vulnerabilidad técnica) es importante tenerla en cuenta. Es difícil protegerse ante este tipo de ataques por su naturaleza, los métodos de protección van enfocados a concienciar a los usuarios y alertarles ante posibles ataques de este estilo que puedan sufrir.

  A pesar de que un ataque de ingeniería social no este provocado por un fallo de la compañía como tal si no un error del usuario, a menudo tiene repercusión en la reputación web de las entidades ya que los usuarios tienden a culpar a la compañía del problema producido (ya sea por desconocimiento, interés u otros factores)

- **Fuga de Información:** Se trata de filtraciones de información sensible sobre las actividades de negocio de una entidad (futuros proyectos, secretos industriales, claves u otro tipo de información confidencial).

  Las fugas de información pueden ser provocadas por ataques externos o bien por fallos del propio personal de la empresa. Tradicionalmente las fugas de información se producían de manera física (documentos o archivos físicos en papel); sin embargo, con el crecimiento de las TIC cada vez más a menudos estas fugas se producen de manera digital (ordenadores personales, usb sin cifrar, terminales sin bloquear…)

  La repercusión en la reputación web varía según el tipo de información que se haya filtrado. A menudo las fugas de información son la principal fuente de escándalos.

  > El ejemplo más representativo de este tipo de amenaza es el caso **Wikileaks**[2][3], quizá uno de los casos que más haya afectado a la reputación de una entidad, en este caso el Gobierno americano. En este ejemplo información clasificada del Gobierno americano ha sido difundida en Internet. La fuente de toda esta información es un soldado americano que tuvo acceso a esta información a causa de un fallo de seguridad.

- **Otras amenazas:** En este punto se tienen en cuenta otro tipo de ataques informáticos que no son contemplados dentro de ninguno de los otros puntos.

  Dentro de este punto se pueden citar los ataques Dos (Denial of Service). Estos ataques se producen cuando un gran número de computadoras comienza a realizar un ingente número de peticiones a un

[2] http://wikileaks.org/
[3] http://www.elpais.com/documentossecretos/tema/wikileaks/

servidor especifico, llenando el ancho de banda de este y provocando su caída.

La fuente de este tipo de ataques pueden ser grupos de personas coordinadas para tal fin (el caso más representativo es el de Anonymous[4]) o bien redes de ordenadores infectados (botnets) que son controladas por un atacante.

Este tipo de ataques busca directamente perjudicar a la reputación web de una entidad. Al dejar los sistemas de una compañía inaccesibles durante un tiempo, se causa un perjuicio a los usuarios que pueda tener. Estos usuarios achacaran sus problemas a la entidad que les debería proporcionar el servicio y no lo hace con el consiguiente impacto en su opinión sobre esta.

Este tipo de ataques se ha generalizado en los últimos tiempos como método de protesta de cierto tipo de colectivos. Se pueden citar varios ejemplos de este tipo:

- **Caso PayPal:** Paypal sufre un ataque DoS por su apoyo al gobierno americano en el caso Wikileaks.

  http://www.eweek.com/c/a/Security/PayPal-PostFinance-Hit-by-DoS-Attacks-CounterAttack-in-Progress-860335/

- **Protesta contra la "Ley Sinde":** Varias páginas de partidos políticos fueron atacadas por su apoyo a la "Ley Sinde"

  http://noticias.lainformacion.com/arte-cultura-y-espectaculos/internet/ataque-masivo-contra-las-webs-de-psoe-ciu-pp-y-pnv-por-la-ley-sinde_1XA7p8IpcZs6EuZ2ptXaY1/

5.2 Métodos de protección

Las entidades cada vez más concienciadas de la importancia de protección ante amenazas de Seguridad Informática que puedan afectar a su reputación web buscan fortalecer sus sistemas para hacerlos "inmunes" ante amenazas de seguridad informática. Sin embargo lograr una inmunidad completa ante las amenazas de seguridad es hoy por hoy impensable. En su lugar se deben llevar a cabo una serie de procedimientos enfocados a reducir en el máximo grado posible estas amenazas.

Las actuaciones principales que toda entidad debería tener en cuenta a la hora de protegerse ante amenazas que afecten a su reputación web se exponen a continuación:

- **Análisis de Riesgo:** El análisis de riesgo es el primer paso que tiene que dar una compañía interesada en protegerse de manera efectiva contra amenazas que afecten a su reputación web.

[4] http://en.wikipedia.org/wiki/Anonymous_%28group%29

Mediante el análisis de riesgo se busca identificar cuáles son las vulnerabilidades de un sistema y las amenazas asociadas a cada vulnerabilidad:

Riesgo = vulnerabilidad + amenaza que la explota

De esta forma se identifican no solo los puntos débiles del sistema sino que también se identifican los métodos de protección más adecuados para cada vulnerabilidad al conocer los ataques que puede sufrir.

Otro aspecto importante a destacar en el análisis de riesgos es que cada riesgo es valorado. De esta manera se puede conocer los riesgos que mayor importancia tienen y poner más medios para subsanarlo en un periodo de tiempo menor. La valoración de cada riesgo depende de la probabilidad de que ocurra y del impacto que acarrearía en caso de darse (**Figura 7**):

Valoración del riesgo = probabilidad x impacto

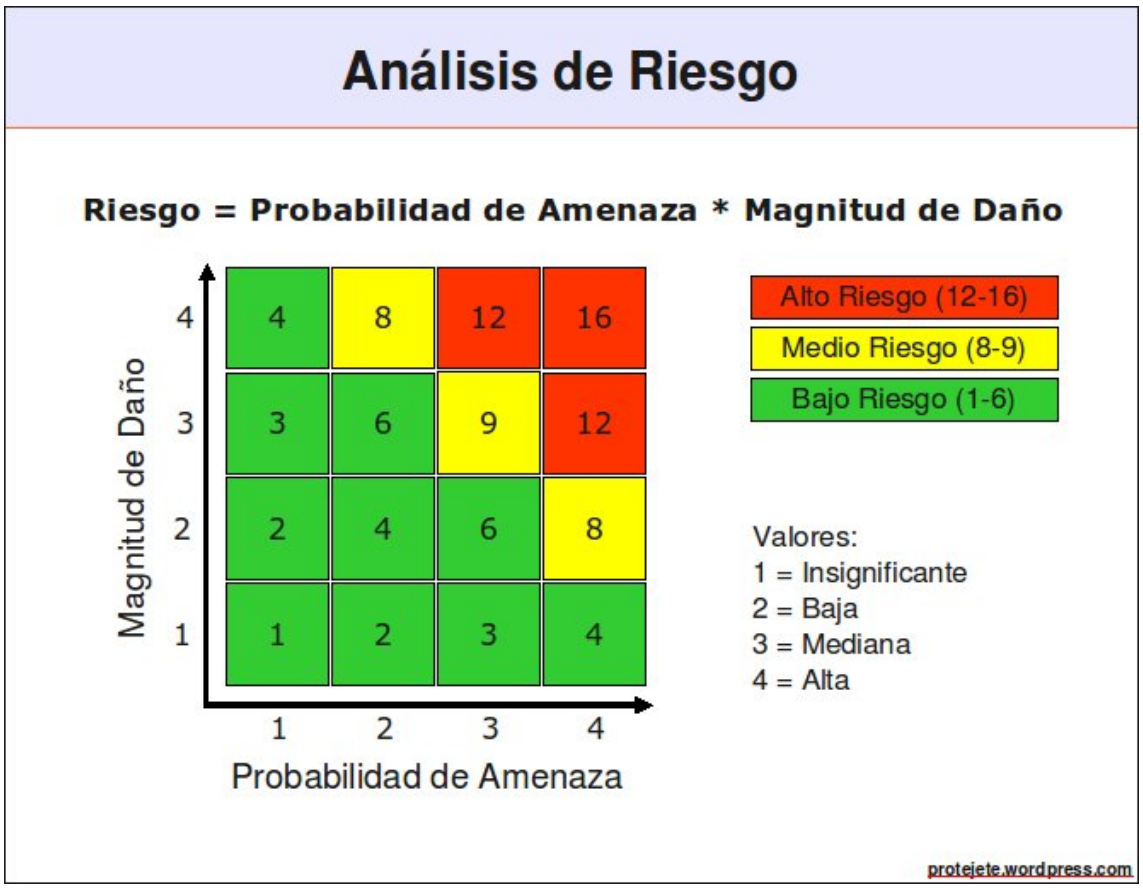

Figura 7- Valoración de un riesgo

De esta manera se evita dar demasiada importancia a grandes riesgo que es muy difícil que ocurran o a riesgos que a pesar de ser frecuentes apenas tengan impacto en la entidad.

Una de las metodologías de riesgos más populares es MAGERIT[5]

[5]http://administracionelectronica.gob.es/?_nfpb=true&_pageLabel=PAE_PG_CTT_General&langPae=es

- **Implantación de una política de seguridad:** Se entiende por políticas de seguridad al conjunto de directrices de seguridad enfocadas a establecer la actuación de una entidad ante problemas de seguridad. En la política se establecen los procedimientos para evitar que se produzcan problemas de seguridad informática.

  La política se toma para una entidad en concreto y se adapta a las necesidades y la organización de esta.

  Para que una política sea efectiva es necesario probar su funcionamiento para comprobar que lo establecido en ella es realmente efectivo. También se deben realizar revisiones después de algún incidente de seguridad para comprobar si la política ha funcionado como era deseable ante un problema real.

- **Plan de acción ante problemas de seguridad:** A mayores de la política de seguridad es necesario establecer un plan sobre cómo actuar ante un fallo provocado por un problema de seguridad informática cuando este ya se ha producido.

  En este plan se fijan las medidas a tomar a posteriori así como los encargados de llevar a cabo el plan. Al igual que ocurre con la política de seguridad es necesario testear el plan de acción para asegurar su validez.

  En el plan se fijan de manera clara actuaciones para llevar a cabo inmediatamente después de producirse el problema. Se persigue minimizar el impacto del fallo, solucionarlo con la mayor brevedad y si fuese posible identificar la fuente para evitar nuevos fallos.

- **Plan de Continuidad de Negocio:** El plan de continuidad de negocio establece también las medidas a tomar tras un problema de seguridad que afecte a la actividad de negocio de la empresa. La principal diferencia del plan de continuidad negocio, respecto a otras medidas, es que los problemas a los que pretende dar respuesta tienen tal magnitud que podrían hacer quebrar a toda la entidad.

  El plan de continuidad de negocio cubre todo el *workflow* de actividades desde que se detecta el problema hasta que este es subsanado. El principal objetivo que se persigue con el plan de continuidad de negocio es asegurar que las actividades de la entidad no se vean afectadas y en caso de que se van afectadas, volver a retomarlas en el menor espacio de tiempo posible.

6 Evolución de la Reputación Web desde el punto de vista de la S.I.

La evolución de la reputación Web se debe plantear sobre la evolución de la Web 2.0, teniendo en cuenta el camino que esta puede tomar en un futuro. Así mismo los aspectos de Seguridad Informática relacionados con la reputación web también irán de la mano de la Web 2.0 y la posible evolución de esta.

En este contexto futuro planteado existen una serie de puntos a tener en cuenta para entender el camino que va a tomar la gestión de la reputación Web (y dentro de esta gestión, los aspectos de Seguridad Informático relacionados):

- **Las Herramientas de monitorización se sofistican:** En la actualidad existen muchas herramientas de monitorización útiles para gestionar la reputación Web, como por ejemplo Google Alerts[6] o Yahoo Alerts[7]. Mediante estas herramientas se pueden crear disparadores que enviarán avisos cada vez que se publique un determinado contenido, especificado por el usuario.

  Recientemente están apareciendo otro tipo de herramientas con un funcionamiento similar a las anteriores, pero específicamente diseñadas para monitorizar redes sociales. Una de estas herramientas es SocialScan[8]

  Este tipo de herramientas evolucionará hacia herramientas específicamente enfocadas a monitorizar la reputación Web. En la actualidad ya existen una serie de herramientas de este tipo. Se puede citar Twinfluence[9]. Con este tipo de herramientas se potenciará aún más la visibilidad de las opiniones de los usuarios, haciendo más importante si cabe la gestión de la reputación Web. Se deberán cuidar con más detalle cada uno de los aspectos envueltos en la reputación web, especialmente el de la seguridad informática

- **El impacto será cada vez mayor:** Como se ha expuesto en el punto anterior las opiniones de los usuarios tendrán cada vez más visibilidad. Esto conllevará un mayor impacto de las opiniones al tener un potencial público objetivo mayor.

- **Incremento de la importancia de la clasificación (Tagging):** Será necesario profundizar en el campo de la clasificación de la información para identificar aquella que realmente sea interesante para la gestión de la reputación web.

- **Mayor importancia de las redes sociales (aspectos de seguridad):** Las redes sociales serán el principal campo de batalla en la gestión de la reputación online. Cada vez es mayor el número de entidades que cuentan con perfiles en distintas redes sociales para promocionar sus actividades. Esto les permite llegar directamente al público objetivo a

[6] http://www.google.es/alerts
[7] http://alerts.yahoo.com/
[8] http://www.socialscan.com/
[9] http://twinfluence.com/

través de estas herramientas. Así mismo los propios usuarios hacen también uso de las redes sociales para compartir sus opiniones y consultar las de otros usuarios.

Este auge de las redes sociales trae consigo una necesidad de plantear un nuevo campo en el ámbito de la seguridad informática, la seguridad en las redes sociales [7]. Será necesario proteger los perfiles profesionales en las redes sociales, ya que en caso de sufrir un ataque pueden convertirse en todo lo contrario a lo que se busca y ser un perjuicio para la reputación web.

En este sentido una herramienta importante para incrementar la seguridad en las redes sociales es

- **Incremento del número de ataques:** Desde los últimos años el número de ataques informáticos ha crecido exponencialmente[10]. Esto ha hecho que la seguridad informática tenga cada vez más importancia en todos los aspectos de una organización (por supuesto también en el de la reputación web).

  Esta situación no tiene visos de remitir en el tiempo, es más, todo indica que los ataques van a continuar incrementándose, ya que cada vez son mayores los alicientes para los atacantes (mayor número de usuarios, más datos personales en la web, incremento del volumen de negocio de internet) por lo tanto las técnicas de seguridad informática deben de evolucionar para poder seguir el ritmo de los atacantes. Esta evolución debe tener en cuenta el incremento de ataques y llevar consigo un aumento del presupuesto para representar una protección efectiva

- **Ataques enfocados a mermar la reputación Web:** Tradicionalmente los ataques informáticos tenían como objetivo provocar un daño a los sistemas de una entidad o particular para sacar un provecho de ello; sin embargo, el auge de la importancia de la reputación web ha hecho que se empiecen a producir ataques directamente enfocados a mermar la reputación web de una empresa.

  Uno de los ataques de este tipo más recientes es el sufrido por la cadena de noticias americanas FOX. Aprovechando la fecha del 4 de Julio (Conmemoración de la Independencia de Estados Unidos) unos atacantes accedieron a su Twitter e introdujeron una falsa noticia sobre la muerte de Barack Obama, presidente de EEUU:

  http://www.elmundo.es/elmundo/2011/07/04/comunicacion/1309773303.html

[10] http://www.geekology.com.ar/noticias-varias/symantec-preve-un-aumento-de-ataques-informaticos-en-2011/

Otro caso de este tipo es el reciente ataque contra la cuenta de Twitter de Paypal Reino Unido. Un hacker accedió a la cuenta y la utilizó para promocionar la página paypalsucks.com en la que se relatan malas experiencias de clientes de Paypal.

http://noticias.lainformacion.com/arte-cultura-y-espectaculos/internet/atacada-la-cuenta-de-twitter-de-paypal-en-reino-unido_W4YJz2RMRwhyOk9aozFCe3/

En un futuro este tipo de ataques se verán incrementados y usarán tecnologías más avanzadas. Los responsables de seguridad informática deben tener esto en cuenta y adaptar sus sistemas para protegerse y recuperarse de este tipo de ataques.

- **Ataques a la reputación Web de los usuarios:** La importancia que están adquiriendo los particulares en internet (especialmente en el campo de la reputación web) hará que se empiecen a producir ataques directamente contra la reputación Web de los usuarios en lugar de contra las propias entidades.

  Este tipo de ataques persigue mermar la credibilidad de un usuario, o grupo de usuarios, intentando de esta manera restar importancia a las opiniones de estos.

  Las entidades deben intentar poner medios para proteger a sus propios usuarios de este tipo de ataques ya que a menudo estos serán sus mejores defensores. En un futuro esto puede ser un método de incrementar la reputación web de una empresa al ser vista como protectora de sus usuarios.

  Independientemente, las entidades dedicadas a la seguridad informática deberán tener esto en cuenta y desarrollar métodos que permitan a los usuarios monitorizar su propia reputación y protegerse de ataques contra ella.

7 Conclusiones

En este trabajo se ha planteado un estudio sobre la reputación web desde el punto de vista de la seguridad informática.

En primer lugar se ha esbozado el contexto actual de Internet, en el cual se mueve la reputación Web. Este contexto está marcado por la irrupción de la Web 2.0 como nuevo paradigma de entender las comunicaciones online. Todos los estudios (referencias) están de acuerdo en que se trata de un fenómeno que únicamente acaba de empezar y que su crecimiento en los próximos años va a ser aún mayor.

En este escenario son los usuarios quienes mayoritariamente generan los contenidos de la web. Es por tanto necesario tener al usuario como piedra angular de cualquier actuación. En este sentido la gestión de la reputación web tiene como principal misión gestionar las opiniones de los usuarios, tratando que estas sean positivas en su mayor parte y de esta manera influir en la opinión de otros usuarios.

Sin embargo, gestionar la reputación web no es fácil. Como se ha expuesto durante el estudio, hay numerosos factores relacionados que deben tenerse en cuenta para forjar una reputación web sólida y confiable. Uno de los factores que tiene más importancia es el de la seguridad informática, ya que los problemas derivados de fallos en la gestión de la seguridad informática a menudo tienen un gran impacto en la reputación web de una entidad.

No obstante, hay que tener en cuenta que la correcta gestión de la seguridad informática no es una tarea trivial. De la mano del auge de la Web 2.0 se ha producido un notable incremento de los ataques informáticos, empelando cada vez técnicas más sofisticadas. También han surgido ataques enfocados directamente a atacar a la reputación web de entidades y de particulares. Es por ello que a pesar del coste que conlleva la gestión de la seguridad informática es necesario implantar los métodos adecuados para hacer frente a este tipo de ataques.

Por último se ha planteado la coyuntura en un futuro próximo, en la cual se moverá la reputación web. En ella se plantea un escenario aún más complicado con un mayor número de usuarios y un mayor impacto de los factores asociados. Los aspectos de seguridad informática asociados serán también más complejos y costosos empujados por la continua expansión de la web. Se debe por tanto invertir más a este respecto de cara a ofrecer una protección eficaz contra el volumen de ataques esperado.

Así mismo, espoleadas por la aparición de estos nuevos tipos de comunicación, aparecerán nuevos tipos de ataques informáticos contra entidades y usuarios. El punto principal de ataque serán las identidades virtuales de empresas y particulares en las redes sociales, haciendo necesario que las técnicas de protección se adapten a estas nuevas reglas de juego.

Podemos por tanto concluir que la gestión de la seguridad informática asociada a la reputación web es cada vez más costosa y compleja debido a la evolución de los sistemas tradicionales de comunicación; sin embargo, es un coste que

es necesario tener en mente y asumir ya que de lo contrario el perjuicio, tanto de imagen como de volumen de negocio, que se pudiese tener por no hacerlo sería mucho mayor.

8 Referencias

[1. *What is Web 2.0: Design Patterns and Business Models for the Next Generation of Software.* **O'Reilly, Tim.** 1, s.l. : Communications & Strategies, 2007.
2. **Bloch, Ethan.** Have We Reached a World of Infinite Information? 2011.
3. *A Classification schem for analysing Web 2.0 Tourism Websites.* **Bingley, Scott, y otros.** 4, s.l. : Journal of Electronic Commerce Research, 2010, Vol. 11.
4. **Mathes, Adam.** Folksonomies - Cooperative Classification and Communication Through Shared Metadata. *http://www.adammathes.com/academic/computer-mediated-communication/folksonomies.html.* [Online] Enero 30, 2004.
5. *Getting the Most Out of Social Annotations for Web Page Classification.* **Zubiaga, Arkaitz, Martinez, Raquel y Fresno, Víctor.** s.l. : Proceedings of the 9th ACM symposium on Document engineering - DocEng '09, 2009.
6. *A preconditioning approach to the pagerank computation problem* . **Tudisco, Francesco y Di Fiore, Carmine.** s.l. : Linear Algebra and its Applications, 2011.
7. **INTECO y AEPD.** *Estudio sobre la privacidad de los datos personales y la seguridad de la información en las redes sociales online.* 2009.
8. **The Apache Software Foundation.** Apache Lucene. [En línea] 31 de Marzo de 2011. [Citado el: 25 de Abril de 2011.] http://lucene.apache.org/.
9. **Michael McCandless, Erik Hatcher, and Otis Gospodnetić.** *Lucene in Action, Second Edition.* s.l. : Manning Publications, 2010.
10. **Karypis, George.** *Cluto A clustering toolkit.* s.l. : University of Minnesota, Department of Computer Science, 2003.