ANÁLISIS DE RIESGO SOBRE EL USO DE LOS *SOCIAL MEDIA* EN AMBIENTES CORPORATIVOS PARA LA DIVULGACIÓN INSTITUCIONAL Y EL ACERCAMIENTO COMERCIAL.

JORGE ALBERTO MEDINA VILLALOBOS

UNIVERSIDAD INDUSTRIAL DE SANTANDER
ESCUELA DE INGENIERÍAS ELÉCTRICA, ELECTRÓNICA Y TELECOMUNICACIONES
ESPECIALIZACIÓN EN TELECOMUNICACIONES
BUCARAMANGA
2011

ANÁLISIS DE RIESGO SOBRE EL USO DE LOS *SOCIAL MEDIA* EN AMBIENTES CORPORATIVOS PARA LA DIVULGACIÓN INSTITUCIONAL Y EL ACERCAMIENTO COMERCIAL.

JORGE ALBERTO MEDINA VILLALOBOS

Trabajo de grado para optar el título de Especialista en Telecomunicaciones.

Directora:

SHIRLEY PAOLA HERRERA HERNANDEZ

Ingeniera Electrónica, Especialista en Telecomunicaciones

UNIVERSIDAD INDUSTRIAL DE SANTANDER
ESCUELA DE INGENIERÍAS ELÉCTRICA, ELECTRÓNICA Y TELECOMUNICACIONES
ESPECIALIZACIÓN EN TELECOMUNICACIONES
BUCARAMANGA
2011

CONTENIDO

INDICE DE FIGURAS

INDICE DE TABLAS

I. INTRODUCCIÓN

Hoy en día, el uso de los Social Media ha empezado a impactar el reconocimiento de las marcas y a generar ingresos a las organizaciones que deciden utilizarlos, de hecho, algunos estudios realizados sobre el uso de estas nuevos canales de comunicación social en las empresas del Fortune Global 100, registran que el 54% posee una página de fans en Facebook, el 65% tiene una cuenta activa en Twitter, el 50% tiene un canal en YouTube y un 33% hace uso de blogs corporativos[1].

Sin duda alguna, esta tendencia ha alcanzado nuestras fronteras y es necesario definir las ventajas y desventajas que esto conlleva para la organización. Bajo estas circunstancias, resulta relevante visualizar aspectos técnicos, económicos, administrativos y por supuesto legales que generen pautas para evaluar la viabilidad del uso de este tipo soluciones desde una conceptualización en el área de la seguridad de la información (SI) para garantizar la integridad y confiabilidad de la información.

El objetivo principal de este trabajo es servir como punto de referencia para cualquier organización y apoyar la toma de decisiones en cuanto al uso de los Social Media dentro de un ambiente corporativo, con base en una metodología de gestión de riesgos estandarizada que pueda ser desarrollada por cualquier tipo de organización.

[1] ENGAGEMENTdb, The World's Most Valuable Brands. Who's Most Engaged? Ranking the Top 100 Global Brands, www.engagementdb.com/downloads/ENGAGEMENTdb_Report_2009.pdf

II. MARCO TEORICO

1. SOCIAL MEDIA

1.1 Introducción a los *Social Media*

En la actualidad, suelen presentarse algunas confusiones en las esferas ejecutivas de las organizaciones e incluso en las esferas académicas acerca de qué exactamente podría ser incluido bajo el termino *Social Media* y sobre cómo éste difiere de algunos términos relativos que se han usado de forma casi que intercambiable: la Web 2.0 y los Contenidos Creados por el Usuario, UCC[2]. Antes de dar una definición general del término Social Media, procederemos a definir estos dos términos:

i. Web 2.0

En 2004, el termino Web 2.0 fue usado por primera vez para describir la nueva forma en que los desarrolladores de software y los usuarios finales empezaron a utilizar la World Wide Web. Esta nueva era dejó atrás la época en que los contenidos eran creados y publicados por un individuo o una organización, iniciando una época marcada por la colaboración y la coautoría de contenidos.

A pesar que el concepto de Web 2.0 no implica ningún tipo de actualización tecnológica para la WWW, sí existe una serie de funcionalidades básicas que son necesarias para su funcionamiento. La aparición de tecnologías como el Adobe Flash para la inclusión de interactividad, los RSS (Really Simple Syndication) para la notificación frecuente de actualización de contenidos y el uso de AJAX (Asynchronous Java Script), una técnica para la recuperación de datos de forma asíncrono desde los servidores web sin necesidad de interferir con la visualización y el comportamiento de toda la página.

[2] OECD, User-Created Content Participative Web and User-Created Content: Web 2.0, Wikis and Social Networking

ii. Contenido Creado por el Usuario, UCC.

El termino UCC, tomó fuerza en 2005 cuando se utilizó ampliamente para describir las diferentes formas de contenidos que eran creados por usuarios finales y publicados en diferentes portales de contenido. De acuerdo con la Organización para la Cooperación Económica y el Desarrollo 3 (OECD), se requieren tres condiciones para que una publicación web sea considerada como UCC:

- La publicación debe ser realizada en una página web de acceso público o en una página de una red social asequible a un grupo selecto de usuarios.
- La publicación debe mostrar un cierto nivel de esfuerzo creativo.
- La publicación debe ser creada fuera las rutinas comerciales.

La primera condición permite excluir el contenido intercambiado a través de correos electrónicos y mensajería instantánea; la segunda, la simple replicación de contenidos preexistentes; finalmente la tercera condición, permite excluir el contenido que ha sido creado dentro de contexto comercial.

1.2 Definición

Los Social Media son un grupo de aplicaciones basadas en Internet que se han construido en los fundamentos ideológicos y tecnológicos de la Web 2.0, y que permiten la publicación de Contenidos Creados por el Usuario, UCC.

Las tecnologías conocidas como Social Media, son aquellas que permiten la creación y diseminación de contenido a través de la Internet en las redes sociales. A diferencia de los medios de comunicación tradicionales, los Social Media se identifican por el alto grado de interacción e interactividad disponible para el consumidor, creando plataformas de comunicación

[3] OECD, Organization for Economic Cooperation and Development - www.oecd.org

altamente efectivas en donde cualquier usuario puede crear libremente contenido y compartirlo en tiempo real con una audiencia global.

1.3 Clasificación de los Social Media

Para diferenciar los *Social Media*, se ha hecho uso de un esquema de clasificación que se basa en un conjunto de teorías de investigación de medios y procesos sociales, los dos elementos claves de los *Social Media*.

i. Teorías de Investigación de Medios:

- La ***Teoría de la Presencia Social*** establece que los medios de comunicación difieren entre sí, por su grado de presencia social, la cual es definida como el nivel de contacto acústico, visual y físico que se puede alcanzar entre dos pares que intervienen en una comunicación. La presencia social está influenciada por: la intimidad entre los pares (Comunicación Interpersonal vs. Comunicación Mediada) y la inmediatez del medio (Sincrónico vs. Asincrónicos). La presencia social es menor para las comunicaciones mediadas que para las interpersonales, y para los medios asincrónicos que para los sincrónicos; finalmente, a mayor presencia social, más grande será la influencia social que tendrán entre sí, los actores que intervienen en la comunicación.
- La ***Teoría de la Riqueza de Contenidos*** (Media Richness Theory) está basada en la asunción de que la meta de cualquier comunicación es la desambiguación y la reducción de la incertidumbre. Establece que los medios difieren entre sí dependiendo del grado de riqueza de contenidos que poseen, es decir, en la cantidad de información que pueden transmitir en un intervalo de tiempo dado; por lo tanto, unos medios son más efectivos que otros desambiguando reduciendo la incertidumbre.

ii. Los Procesos Sociales

- Los procesos de Auto-Presentación y Auto-Divulgación, establecen que en cualquier tipo de interacción social, la gente siente el deseo de controlar las impresiones que los demás se harán sobre ellos. Por un lado, esta actitud es explicada por la necesidad de influenciar a los demás para obtener recompensas; por otro lado, está el deseo de crear una imagen que sea consistente con la su propia imagen interior. El concepto de la ***Auto-Presentación***, explica la razón por la cual una persona desea crear una página web personal en el ciberespacio. El concepto de la ***Auto-Divulgación***, es el proceso mental consciente o inconsciente por el cual, esa persona decide revelar información personal consistente con la imagen personal que se desea presentar en el ciberespacio. Estos conceptos pueden ser utilizados en el proceso de clasificación de los Social Media, en la medida en que se asume que estos pueden ordenarse según el grado de auto-divulgación que es requerido y el grado de auto-presentación que el medio permite.

La combinación de ambas dimensiones, es decir, las teorías y los procesos, nos lleva a la clasificación de los Social Media que se presenta a continuación en la tabla 1.

Tabla 1. Clasificación de los Social Media.

		Presencia Social / Riqueza de Contenidos		
		Baja	Media	Alta
Auto-Presentación	Alta	Blogs - Micro blogs	Redes Sociales	Sociedades Virtuales
Auto-Divulgación	Baja	Proyectos de Colaboración	Comunidades de Contenidos	Juegos Virtuales

1.3.1 Proyectos de Colaboración

Los proyectos de colaboración habilitan la creación conjunta y simultanea de contenido por usuarios concurrentes, en ese sentido, se convierten en la manifestación más democrática de los UCC. EL fundamento principal de los proyectos de colaboración es que el esfuerzo conjunto de múltiples actores conlleva a mejores resultados que los cualquier actor pudiese obtener individualmente. Desde la perspectiva corporativa, los proyectos de colaboración tienden a convertirse en una fuente o repositorio de información. El mejor ejemplo de este grupo son los proyectos de enciclopedias en-línea.

1.3.2 Blogs

Son formas especiales de páginas web que publican de forma cronológica. Son el equivalente a las páginas web personales cuyo contenido puede variar desde información muy personal, hasta información relevante en temas específicos. Desde el punto de vista corporativo, las empresas han utilizado los blogs como un medio de interacción con sus usuarios, sin embargo, no pueden dejar a un lado los efectos colaterales que estas interacciones puedan ocasionar.

1.3.3 Comunidades de Contenidos

Están orientadas a que los usuarios compartan contenidos sin que sea necesario que los usuarios creen perfiles personales, es decir, no es necesaria la auto-divulgación. Desde el punto de vista corporativo, las comunidades de contenido representan un riesgo para la fuga de información o la responsabilidad legal por infringir material protegido por la propiedad intelectual o por derechos de autor.

1.3.4 Redes Sociales

Las redes sociales son páginas que contienen aplicaciones que habilitan a los usuarios a interrelacionarse mediante la creación de perfiles en dónde su información personal es requerida para que los usuarios puedan reconocerse entre sí, formando reuniones virtuales de colegas, amigos e incluso, dando lugar a nuevas relaciones. A nivel corporativo, algunas organizaciones están haciendo uso de las redes sociales con propósitos de marketing.

1.3.5 Mundos Virtuales (sociedades y juegos virtuales)

Los mudos virtuales son plataformas que replican un ambiente tridimensional en el cual los usuarios aparecen en forma de *avatars* personalizados que interactúan entre sí como si lo hicieran en la vida real. Los mundos virtuales son la máxima manifestación de los Social Media, al proveer el más alto nivel de presencia social y riqueza de contenidos. Existen dos tipos de mundos virtuales: los juegos virtuales y las sociedades virtuales. En los mundos de juegos, los jugadores deben comportarse de acuerdo a reglas estrictas dentro del contexto MMORPG (*Massive Multiplayer On-line Role Play Game*). A diferencia de los juegos virtuales, en las Sociedades Virtuales no existen reglas más allá de las reglas físicas como la gravedad, lo cual abre un rango ilimitado de posibilidades de interacción, llevando a los usuarios a exhibir comportamientos similares a los vistos en el mundo real.

1.4 Los Social Media en el Ámbito Corporativo

Los *Social Media* se han convertido en una poderosa herramienta para las empresas a lo largo del globo las cuales, los están usando en diferentes áreas funcionales de negocio y disfrutan hoy en día de numerosos beneficios como el aumento en el reconocimiento de marca, aumentos en ventas,

aumento de presencia en la red, e incluso, aumentos en los índices de satisfacción del cliente.

Las organizaciones más comprometidas, han descubierto que es posible monitorear el mercado, a sus competidores y a sus clientes vía *Social Media*, lo cual les permite ser los primeros en reaccionar estratégicamente a los requerimientos o variaciones del mercado.

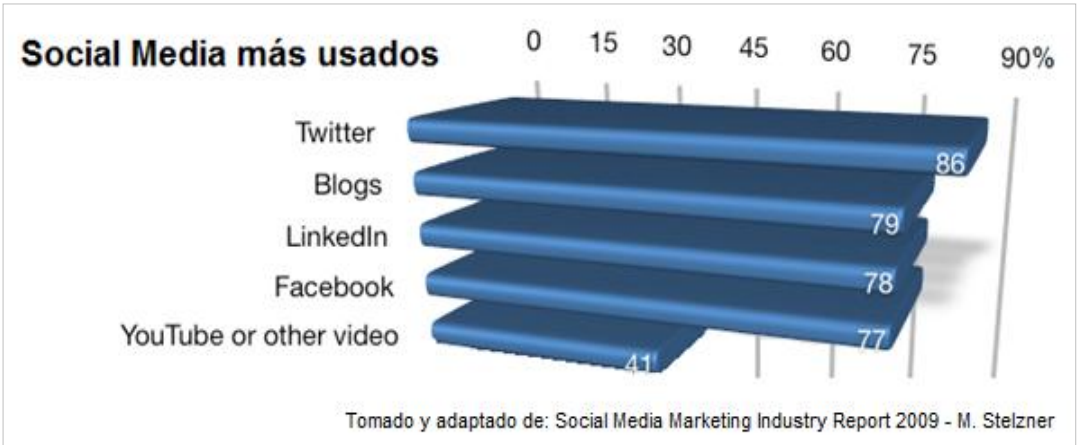

Figura 1. Social Media más usados por las empresas.

En el *Social Media Marketing Industry Report* de 2009, Michael Stelzner condensa, entre otras cosas, los resultados de una encuesta realizada acerca de los Social Media más utilizados (Figura 1) y de los beneficios obtenidos por las organizaciones que están haciendo uso de estos medios (Firgura 2).

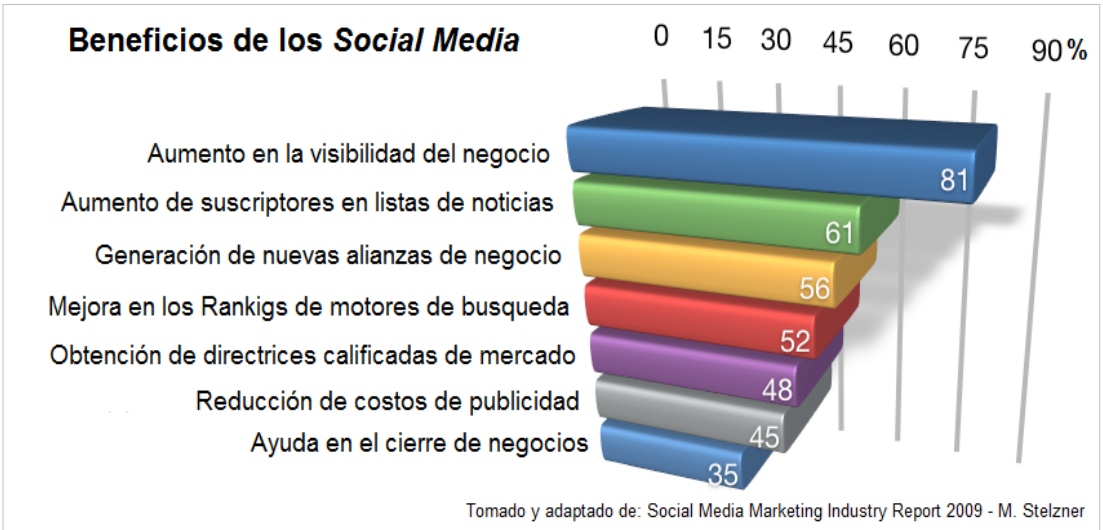

Figura 2. Beneficios obtenidos por empresas que usan Social Media

Debido a la facilidad de uso y medición, y sobre todo la habilidad para llegar grandes multitudes de forma casi instantánea, los Social Media, se están convirtiendo en una fuerza poderosa para que los negociantes logren atraer y comprometer a sus clientes, empleados y sobre todo a sus inversionistas. Estas características atractivas sumadas a que los Social Media no requieren nuevas infraestructuras tecnológicas, permiten que sean introducidas a la organización por cualquiera de los integrantes del equipo de ventas o publicidad, y sin involucrar las áreas de TI, un gerente de proyecto y mucho menos, un análisis de riesgo para la organización.

Dado que el uso de los Social Media conlleva en sí mismo un riesgo inherente que podría impactar negativamente a la organización en diferentes aspectos, se hace de vital importancia la definición de un plan estratégico para su adopción, que permita considerar los compromisos entre riesgos y beneficios.

1.5 Modelos para la Implementación Corporativa de Los Social Media[4]

Cómo con todas las nuevas tecnologías y los nuevos programas, las organizaciones tienen a su disposición diferentes alternativas para adoptarlas. Dependiendo de la experiencia de la organización con los Social Media, esta podrá optar por una de las tres alternativas, cada una de ellas tiene sus fortalezas y debilidades.

1.5.1 Modelo distribuido

Cada unidad de negocio o grupo de trabajo puede crear su propio programa de Social Media sin la necesidad de una autorización centralizada. Este tipo de acercamiento inicia generalmente en grupos apasionados que desean parecer originales ante sus clientes, no obstante, la falta de centralización produce que los diferentes grupos puedan verse incoherentes y asíncronos ante un mismo cliente, e incluso, que diferentes grupos compartan información particular de cada uno de ellos pero que en conjunto, toda la información compartida por los diferentes grupos, pueda llegar divulgar por inferencia, información sensible o confidencial.

1.5.2 Modelo Centralizado

Ocasionalmente, como consecuencia de las falencias del modelo distribuido, las compañías se mueven hacia un modelo centralizado en el cual, sólo una unidad de negocio controla los Social Media, generalmente, esta centralización se hace en el área de mercadeo y publicidad. Inicialmente, el modelo centralizado proporciona un único mensaje coherente al cliente, sin embargo, al cabo de poco tiempo los Social Media se convierten en un canal más de mercadeo y empiezan a desperdiciarse las oportunidades que un canal de comunicación de dos vías puede ofrecer, principalmente, se pierde la oportunidad de recibir realimentación directa de los mercados.

[4] Owyang, Jeremiah. Forrester. How to organize your company for social computing. 2009

1.5.3 Modelo Federado

El modelo federado está formado por un grupo interdisciplinario que representa a todos los accionistas de la organización. Este grupo centraliza la gerencia de los Social Media facilitando así la comunicación entre las áreas y permitiendo que los recursos sean compartidos por aquellos que desean tener canales originales de comunicación con sus clientes. Este modelo permite evitar el envió de múltiples mensajes o la incoherencia entre ellos, pero al mismo tiempo, permite que los individuos expertos se acerquen a los clientes y ofrezcan soluciones personalizadas. Sin embargo, a pesar de los beneficios, este modelo requiere del apoyo de la alta gerencia y de unos acuerdos culturales a lo largo de la organización, incluso en ocasiones, de un presupuesto dedicado.

2. SEGURIDAD DE LA INFORMACIÓN

Hoy en día es fácil reconocer que la información, sin importar su forma (impresa, digital u oral), es un activo primordial para las organizaciones y que como los demás activos importantes del negocio, representa valor o un bien que requiere ser protegido adecuadamente.

2.1 Principios fundamentales de la Seguridad de la Información

A continuación se presentan y describen los principios fundamentales de la seguridad de la información:

i. Confidencialidad (Confidentiality)

Evita la divulgación intencional o accidental del contenido de un mensaje o cualquier otro tipo de información, es decir, sólo las personas o procesos autorizados pueden acceder a la información.

ii. Integridad (Integrity)

El concepto de integridad garantiza que la información es exacta y completa, esto incluye los siguientes tópicos:

- Personas o procesos no autorizados no pueden modificar los datos.
- Personas o procesos autorizados no realizan modifican no autorizadas a los datos.
- Los datos son consistentes interna y externamente.

iii. Disponibilidad (Availability)

Asegura que los usuarios autorizados podrán tener un acceso confiable y oportuno a la información o a los recursos computacionales en el momento que ellos lo requieran.

2.2 Conceptos Auxiliares

A continuación se presentan y describen algunos de los conceptos de apoyo que permiten implementar controles y realizar seguimiento a los principios fundamentales:

i. Identificación (Identification)

Es el medio por el cual un usuario proclama su identidad ante un sistema. La identificación es usada comúnmente en Control de Acceso pues, es necesaria para la autenticación y la autorización.

ii. Autenticación (Authentication)

Cuando se puede garantizar la identidad de un usuario y se comprueba que el usuario es quien dice ser.

iii. Autorización (Authorization)

Son los derechos y permisos concedidos a un individuo o un proceso al que se le ha permitido acceder a un recurso computacional.

iv. Observancia (Accountability)

Es la capacidad del sistema para registrar las acciones y el comportamiento de un individuo dentro del sistema, y su capacidad para determinar la identidad del usuario.

v. No Repudio (Don't Disavowal)

Es cuando la información involucrada en un evento corresponde a quien participa. Las personas que intervienen un evento no pueden evadir o negar su intervención.

3. METODOLOGÍA PARA EL ANÁLISIS DE RIESGOS

Este capítulo tiene por objeto describir la metodología de análisis de riesgo que se utilizará como base para identificar las implicaciones de la adopción de los Social Media en un entorno corporativo.

La norma ISO/IEC 27005;2008 proporciona los lineamientos para modelar los procesos de Gestión de Riesgos de Seguridad de la Información dentro de una organización; sin embargo, esta norma no promueve una metodología específica para la gestión de riesgos por lo tanto, dependerá de la organización buscar y definir el mejor acercamiento dependiendo del sector de negocio. Esta norma hace parte de la familia ISO 27000, la cual presenta los lineamientos y recomendaciones para la definición e implementación de1 Sistema de Gestión de la Seguridad de la Información, SGSI.

La gestión de riesgos se reconoce como una actividad que aplica métodos lógicos y sistemáticos para establecer el contexto, identificación, análisis, evaluación, tratamiento, monitoreo y comunicación de los riesgos asociados a cualquier tipo de actividad ó proceso, por lo cual hoy en día se considera que este proceso es vital y debe ejecutarse en cualquier organización que busque identificar oportunidades y prevenir o minimizar pérdidas.

La seguridad de la información no es ajena a este concepto, por el contrario en un sin número de aplicaciones es necesario realizar e implementar la gestión del riesgo a fin de contener y mitigar las amenazas que puedan poner en peligro el funcionamiento o el correcto desempeño de una organización ya sea estatal o privada.

En la siguiente gráfica se plantea un resumen gráfico del proceso conceptual de análisis de riesgo que se plantea en la norma ISO 27005, y que podría ser implementada en el interior de una organización para llevar a cabo una correcta gestión de riesgos.

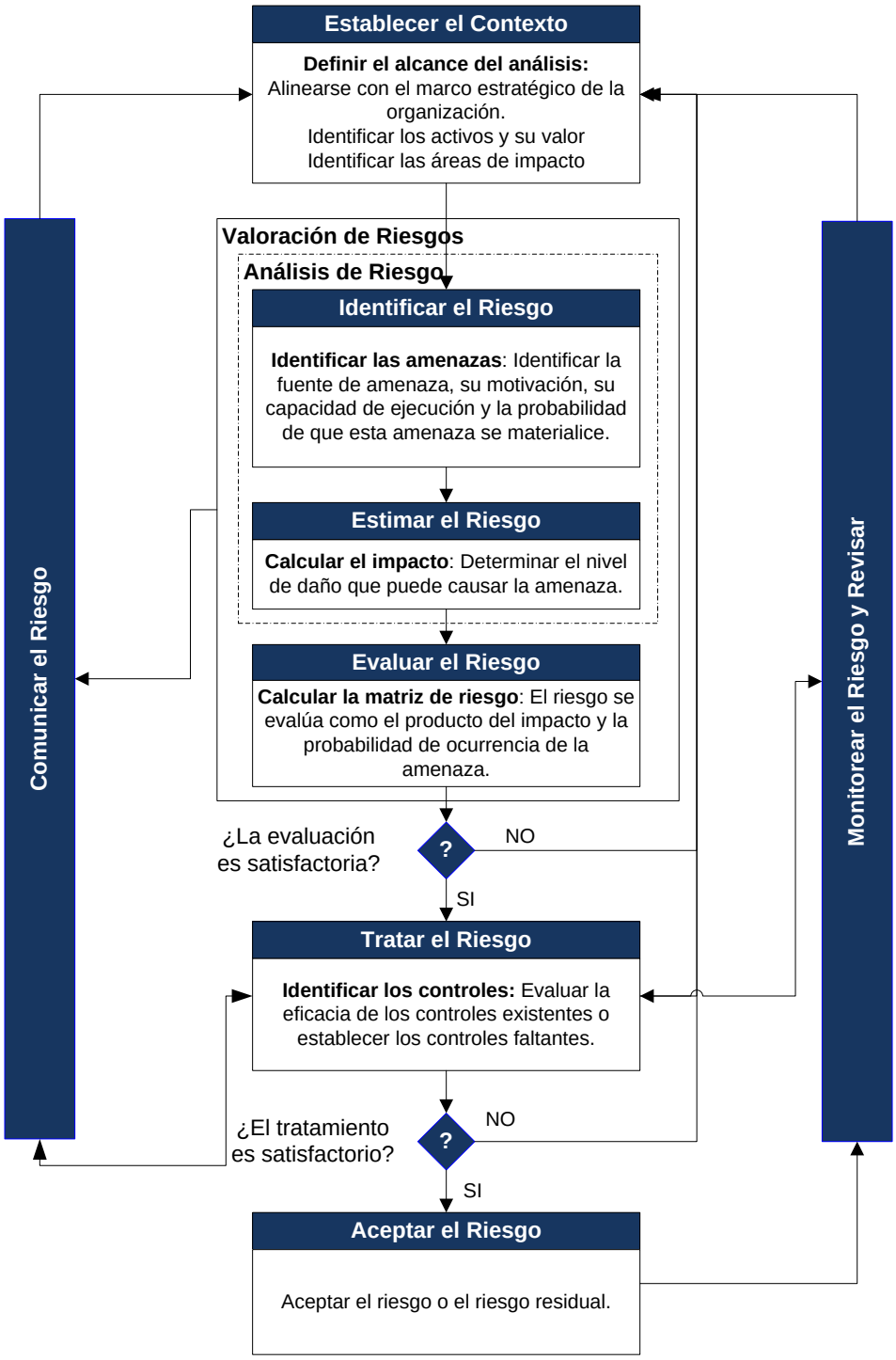

Figura 3. Diagrama de bloques de la metodología descrita

III. CASO DE ESTUDIO

A continuación, se realizarán el análisis de riesgo sobre el uso de los Social Media en un ambiente corporativo, en particular, se realizará una evaluación particular de las implicaciones de la adopción de estas nuevas tecnologías en el Banco Central de Colombia.

1. CONTEXTO CORPORATIVO.

1.1 Introducción

El Banco de la República de Colombia actúa desde el año 1923 como banco central, sin embargo, es desde 1.991 con la nueva Constitución Política de Colombia que se establecen las nuevas funciones del Banco[5].

La Constitución de 1991 estableció que el objetivo principal de la política del Banco de la República es la preservación de la estabilidad de los precios, es decir, la reducción de la inflación. Para lograrlo, la Junta Directiva fija una meta anual y maneja los instrumentos de política monetaria, cambiaria y crediticia que tiene a su cargo. A través de estos instrumentos, el Banco busca crear un ambiente de estabilidad que promueva el crecimiento económico y que ofrezca seguridad a los trabajadores y empresarios.

Las políticas monetaria, cambiaria y crediticia están interrelacionadas y por ello no siempre es posible separarlas totalmente. Una medida de carácter monetario puede afectar tanto la tasa de cambio como las tasas de interés. Por esta razón, las tres políticas deben estar perfectamente coordinadas, para que el objetivo de controlar y reducir la inflación pueda ser cumplido.

A continuación se presentan las funciones del Banco de la República:

[5] Constitución Política de Colombia de 1.991, capítulo 6 y la ley 31 de 1.992

1.1.1 Emisión de moneda legal:

El atributo de la emisión, propio de la soberanía monetaria de la Nación es exclusivo e indelegable del Banco de la República y se ha materializado, con la autorización del Congreso, por medio de varios contratos.

1.1.2 Funciones de crédito del Banco de la República:

La Ley 31 de banca central prevé condiciones precisas: prohíbe de manera categórica al Emisor otorgar créditos y garantías a particulares o entidades privadas. Se exceptúan los créditos de apoyo transitorio de liquidez a los establecimientos de crédito en cumplimiento del papel de prestamista de última instancia.

En cuanto al crédito del Banco de la República al Gobierno, si bien el nuevo régimen no lo prohíbe, sí establece condiciones muy rigurosas para su concesión. En efecto, se establece que este tipo de crédito debe limitarse a casos de extrema necesidad, y se requiere la aprobación unánime de todos los miembros de la Junta Directiva. No obstante, es importante señalar que la Constitución dejó abierta la posibilidad de que el Banco pueda continuar adquiriendo en el mercado secundario títulos de deuda emitidos por el Gobierno. De esta forma no es el Banco el que financia directamente al Gobierno, sino los particulares que han comprado estos títulos.

1.1.3 Banquero de bancos

Como todo banco central, el Banco de la República desempeña la función de banquero de bancos. De una parte, es depositario de los dineros que le consignan en cumplimiento del requisito de reserva bancaria que sirve para regular la capacidad de crédito del sistema bancario. Esta reserva, mantenida con máximas condiciones de seguridad, sirve de respaldo a la liquidez del sistema. De otra parte, como ya se señaló el Banco de la República actúa como prestamista de última instancia de los

establecimientos de crédito, en casos de iliquidez transitoria originada en retiros masivos de depósitos.

El Banco de la República ha hecho aportes de gran importancia al desarrollo del sistema de pagos y de la infraestructura del sector financiero en nuestro país y al logro del mandato legal de velar por el normal funcionamiento de los pagos internos y externos. El más relevante de ellos para los objetivos de contribuir a la eficiencia del aparato productivo, la estabilidad del sistema financiero y la canalización de las señales de la política monetaria en los mercados de dinero es el servicio de transferencia de dinero y registro de operaciones entre intermediarios financieros, del mercado de valores y otros, por medios electrónicos y en tiempo real a través de su sistema de pagos de alto valor denominado CUD (“sistema de cuentas de depósito”).

Adicionalmente, el Banco administra la "cámara de compensación interbancaria de cheques", la cámara de compensación interbancaria de pagos electrónicos de bajo valor (CENIT), el Depósito Central de Valores – DCV, en el cual se custodian y administran los títulos desmaterializados de deuda pública, y el sistema electrónico de negociaciones (SEN) de títulos de deuda pública.

1.1.4 Funciones cambiarias

La Ley 31 también le atribuye al Banco de la República la función de diseñar y determinar el manejo de la política de la tasa de cambio, es decir, de definir el conjunto de normas relacionadas con aquélla de común acuerdo con el Ministro de Hacienda y Crédito Público. Desde 1999 hasta la actualidad la tasa de cambio está sujeta a un régimen flexible, en el cual el Banco de la República permite que el precio del dólar sea determinado por el mercado, aunque tiene la facultad de intervenir cuando se vea amenazada su estabilidad. Sin embargo, en un mercado cambiario libre

como el actual, el Banco de la República no busca modificar la tendencia que el mercado le imprime a la tasa de cambio.

De la misma manera, la Junta Directiva dispone la intervención del Banco de la República en el mercado cambiario como comprador o vendedor de divisas, o la emisión y colocación de títulos representativos de las mismas.

1.1.5 Administración de las reservas internacionales

Al Banco de la República le corresponde administrar las reservas internacionales del país incluyendo el manejo, inversión, depósito de custodia y disposición de los activos de reserva. La inversión ha de efectuarse principalmente con base en criterios de seguridad y liquidez, a fin de facilitar los pagos del país en el exterior.

El Banco ante todo, busca la seguridad y estabilidad en sus inversiones y procura que la reserva tenga liquidez para asegurar oportunos pagos a otros países.

Las reservas internacionales son medios de pago de aceptación internacional generados, entre otros conceptos, por: i) la diferencia entre los ingresos provenientes de las exportaciones o ventas al exterior y los gastos que se hacen para las importaciones o para las compras realizadas en el resto del mundo; ii) la diferencia entre lo que ingresa por préstamos externos e inversión extranjera y lo que se paga en capital, intereses y retención de utilidades; y iii) la diferencia entre los giros que envían los colombianos residentes en el exterior y los que se les envían a ellos. Las reservas tienen por objeto atender las necesidades del Gobierno y los particulares para hacer pagos al exterior.

Las reservas están compuestas por monedas libremente convertibles, es decir, que pueden cambiarse legalmente por otras que poseen amplia

aceptación internacional, por oro, y por derechos especiales de giro (DEG).

1.1.6 Banquero, agente fiscal y fideicomisario del Gobierno

El Banco de la República cumple con estas funciones al recibir en depósito fondos de la Nación y de las entidades públicas bajo las condiciones que establezca la Junta Directiva. Además, a solicitud del Gobierno puede actuar como agente fiscal en la contratación de créditos externos e internos y en operaciones que sean compatibles con las finalidades del Banco.

1.1.7 Promotor del desarrollo científico, cultural y social

El nivel profesional y la estructura operativa del Banco le han permitido apoyar simultáneamente el desarrollo científico, cultural y social del país, a través de la creación de fundaciones destinadas a seleccionar, estimular y financiar investigaciones en las áreas de las ciencias, la tecnología, las humanidades, la antropología, la arqueología, la educación y la salud. Además, ha participado en el rescate y preservación del patrimonio cultural y en la creación de estímulos a su desarrollo mediante la administración y creación de bibliotecas y museos especializados en todo el país. El Museo del Oro y la Biblioteca Luis Ángel Arango, hacen parte del Banco de la República y tienen amplio reconocimiento nacional e internacional por la labor que desarrollan.

2. IDENTIFICACIÓN Y VALORACIÓN DE ACTIVOS

2.1 Activos primarios

Se identifican como activos primarios la información y los procesos o actividades de negocio de la organización.

2.1.1 La información

Según las políticas de seguridad de la información del Banco de la República, la información debe estar clasificada de acuerdo a su valor y sensibilidad. Teniendo como base los requerimientos de confidencialidad e integridad de la información, se establece la siguiente matriz de sensibilidad:

Tabla 2. Matriz de sensibilidad

MATRIZ DE SENSIBILIDAD		INTEGRIDAD		
		Baja	Media	Alta
CONFIDENCIALIDAD	Baja	Pública	Sensible	Sensible
	Media	Privada	Privada	Privada
	Alta	Confidencial	Confidencial	Confidencial

Tabla 3. Clasificación de la Información

CLASIFICACIÓN	DESCRIPCIÓN	EJEMPLO
PUBLICA	Información pública de carácter cultural cuya divulgación efectiva favorece y hace parte de las actividades del negocio.	Información de exposiciones culturales del Museo del Oro, La Casa de la Moneda, La Casa Botero, la red de bibliotecas.
SENSIBLE	Información que es pública por decreto de ley, no obstante, la divulgación errada de esta información podría causar impactos negativos a la imagen corporativa o incluso, afectar algunos sectores económicos del país.	Informes de la Junta Directiva sobre política económica y decisiones de balanza cambiaria.
PRIVADA	Información de uso privado del Banco. Su divulgación podría afectar tanto a empleados como a la misma organización. Su alteración o falta de disponibilidad puede afectar las actividades del negocio e incluso del sector financiera.	Información crediticia de los empleados. Información de estudios económicos. Información cultural protegida por derechos de autor.

CONFIDENCIAL	Información que debe guardarse bajo reserva por disposiciones de ley. Su divulgación no autorizada puede afectar la política económica del país y su imagen nacional e internacional.	Información de reserva bancaria.

2.1.2 Los procesos y actividades de negocio

Según las funciones del banco, se identifican los siguientes procesos y actividades de negocio que podrían verse favorecidos o afectados por el uso de los Social Media:

Tabla 4. Principales procesos de negocio

PROCESO O ACTIVIDAD	DESCRIPCIÓN
Bajar la Inflación	Tomar decisiones de política económica para controlar la inflación
Emisión y distribución de efectivo	Emitir la moneda legal y distribuirla a lo largo del territorio nacional.
Administrar las reservas internacionales	Administrar las reservas internacionales del país incluyendo el manejo, inversión, depósito de custodia y disposición de los activos de reserva
Determinar la política cambiaria.	Tomar decisiones de política económica para controlar la tasa cambiaria.

2.2 Activos secundarios

Se identifican como activos secundarios el hardware, el software, la red, el personal, la infraestructura (edificios) y la estructura organizacional.

2.2.1 El Hardware

Se entiende como Hardware la plataforma computacional (computadores de escritorio, portátiles, servidores y periféricos) que soportan la operación

de la organización. La afectación total o parcial del hardware podría afectar la prestación de servicios internos y/o externos.

2.2.2 El Software

Constituye todos los programas (sistemas operativos, aplicaciones, bases de datos, etc.) y sistemas de información que contribuyen a la operación y procesamiento de datos. La afección total o parcial del software podría afectar la prestación de servicios internos y/o externos.

2.2.3 La Red

Son todos los dispositivos y medios de telecomunicaciones que permiten la interconexión de todo el hardware y los sistemas de información. La afectación total o parcial del hardware podría afectar la prestación de servicios internos y/o externos.

2.2.4 El Personal

Todas las personas o grupos de personas que se involucran con los sistemas de información, no obstante, el análisis estará limitado a los siguientes equipos de trabajo:

Tabla 5. Principales unidades organizacionales

GRUPO	DESCRIPCIÓN
Junta Directiva	Junta Directiva y Gerencia General
Estudios Económicos	Grupos de programación de inflación, información económica y la unidad de investigaciones.
Reservas Internacionales	Estudios financieros, operaciones de desarrollo de mercados y reservas internacionales.
Operación Bancaria	Contaduría, fiduciaria y valores, cambios internacionales, pagos electrónicos e internacionales.
Informática	Gestión informática, tecnología informática, seguridad informática y continuidad informática.
Tesorería - Imprenta	Imprenta de billetes, fábrica de moneda y

	tesorería.
Administrativa	Recursos humanos, servicios médicos, compras y documentación editorial
Control Interno	Control interno y análisis de operaciones.
Cultural	Red de bibliotecas y artes, museos y fundaciones.
Comunicación Institucional	Comunicación institucional y relaciones públicas
Jurídico	Asesores jurídicos, control disciplinario interno.

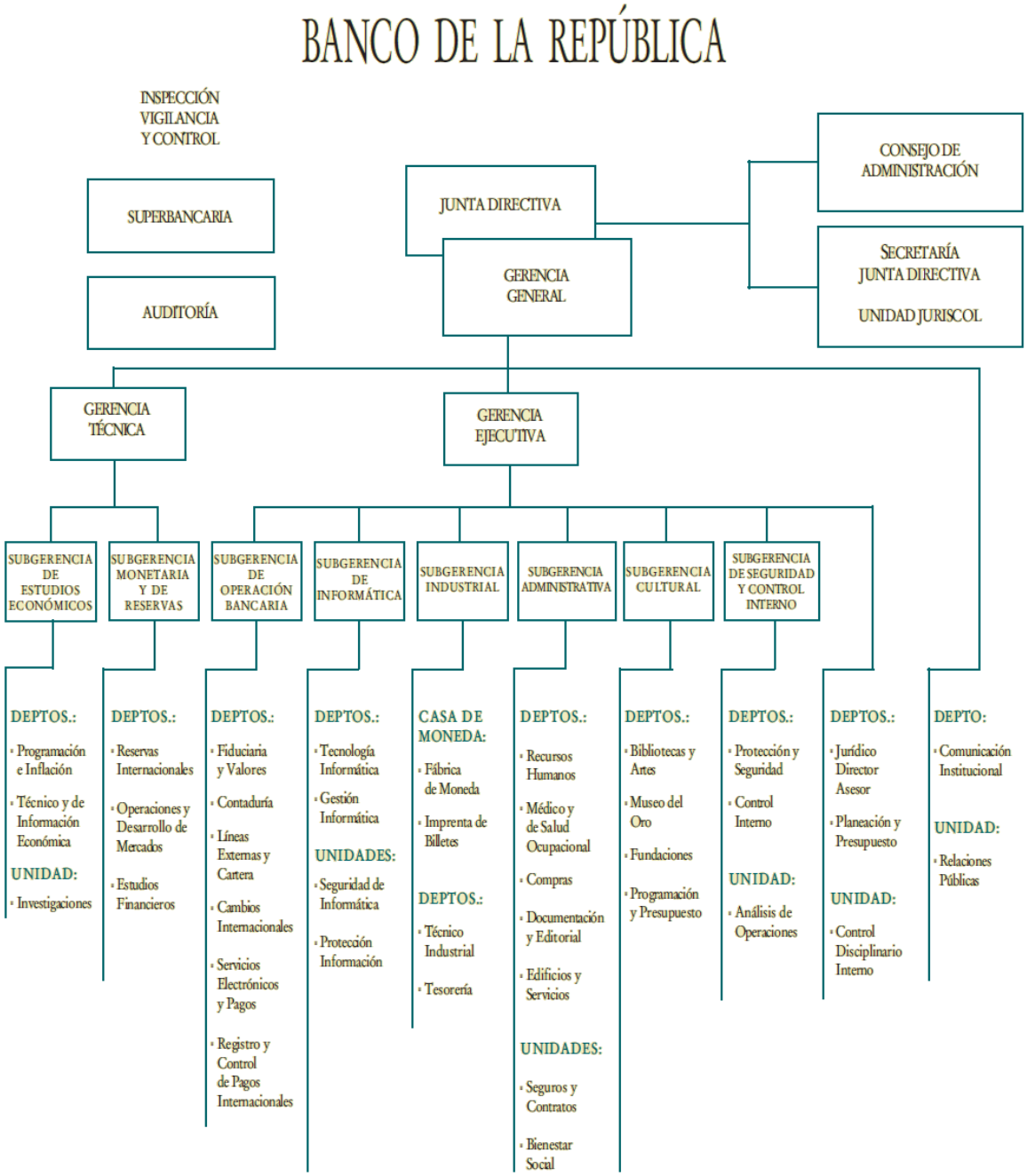

Figura 4. Organigrama del Banco de la República (2009-2010)

3. ANÁLISIS DE IMPACTO

3.1 Impactos directos

Se identifican como impactos directos los que afectan la operación del negocio y por ende el cumplimiento de los objetivos, también son impactos directos los que representan costos financieros directos producto del incidente.

3.2 Impactos indirectos

Se identifican como impactos indirectos los que suelen derivarse a futuro por los incidentes que se presentaron, por ejemplo: la responsabilidad legal, mala imagen y pérdidas financieras por costo de oportunidad.

Tabla 6. Áreas de impacto y nivel de impacto

ÁREAS DE IMPACTO	NIVEL DE IMPACTO		
	BAJO	MEDIO	ALTO
Cumplimiento de Objetivos	No afecta el cumplimiento de los objetivos	Retrasos o cumplimiento parcial de los objetivos.	Incumplimiento general de los objetivos.
Financiero & Activos	No se presentan pérdidas financieras. No se afectan los activos informáticos.	Pérdidas financieras leves o parciales. Se involucran algunos activos informáticos que afectan parcialmente la operación.	Pérdidas financieras serias y/o a terceros. Se involucran muchos activos informáticos que afectan la operación del negocio y/o el negocio de terceros.
Intangibles e Imagen	No se afecta la imagen.	Se afecta la imagen a nivel sectorial.	Se afecta la imagen a nivel nacional o internacional.
Responsabilidad Legal	No hay responsabilidad	Hay responsabilidad	Hay responsabilidad

	legal.	legal por incumplimiento de normativas sectoriales.	legal por incumplimiento de normativas nacionales.

4. IDENTIFICACIÓN DE AMENAZAS Y VULNERABILIDADES

Este proceso de identificación de riesgos debe hacerse de forma amplia, sistemática y estructurado, debe incluir tanto los riesgos que estén bajo el control de la organización como los que no, este paso es crucial en el proceso de gestión, debido a que los riesgos potenciales que no se listen en este punto serán excluidos de todo el análisis. Para este análisis, se consideraran las amenazas provenientes de las siguientes fuentes: personas, tecnologías y procesos o procedimientos.

Para la determinación de la criticidad de la amenaza, se tendrá en cuenta la motivación, la frecuencia ocurrencia y los controles que mitigan la amenaza, por lo tanto, se definirá la probabilidad de que una amenaza se materialice como:

Tabla 7. Descriptor cualitativo para la probabilidad de que una amenaza se materialice.

DESCRIPTOR	DESCRIPCIÓN
Improbable	Sólo podría ocurrir en situaciones excepcionales
Probable	Ha ocurrido en algunas ocasiones y podría repetirse
Certero	Ha ocurrido en múltiples ocasiones y es casi seguro que volverá a ocurrir.

Para este análisis, se enfocará el esfuerzo a determinar el efecto que podrían tener las personas y su comportamiento, las nuevas tecnologías, los procesos y procedimientos que generan las amenazas que atentan contra los principios básicos de la seguridad de la información, es decir, la confidencialidad, la integridad y la disponibilidad.

4.1 Amenazas originadas por el comportamiento humano

4.1.1 Delincuentes informáticos:

Tanto las motivaciones de los atacantes informáticos como su capacidad de ejecutar la amenaza varían dependiendo del perfil del hacker[6]. La UNICRI (*United Nations Interregional Crime and Justice Research Institute*), recientemente realizó un proyecto de cobertura mundial para determinar el perfil criminal de los atacantes informáticos.

Tabla 8. Perfil de los atacantes informáticos según la UNICRI.

CLASIFICACIÓN	AMENAZA	OBJETIVOS	MOTIVACIÓN
Wannabe	Ninguno	Usuarios finales	Moda
Script-Kiddie	Bajo	Fallas específicas	Fama
Cracker	Medio Alto	Compañías, negocios	Fama
Ethical Hacker	Medio	Fabricantes de tecnología	Conocimiento
Paranoic Hacker	Medio Alto	Por necesidad	Conocimiento
Ciber-Warrior	Alto	Pequeñas empresas o usuarios finales	Dinero
Industrial Spy	Alto	Grandes empresas.	Dinero
Government Agent	Alto	Gobierno	Espionaje

- **Suplantación o robo de identidad:** Un atacante malintencionado podría estar interesado en robar o suplantar la identidad corporativa a fin de afectar su imagen o simplemente utilizar estos nuevos canales de comunicación para realizar cualquier tipo de engaño. Ejemplo: estudios de seguridad reportan que un alto porcentaje de

[6] R.Chiesa, S. Ducci, S. Ciappi, Profiling Hackers – The science of criminal profiling as applied to the world of hacking. CRC Press.

usuarios está en riesgo de ser víctima de robo de identidad en Facebook.[7] [8]

- **Alteración intencional de la información publicada:** Un tercero mal intencionado, podría publicar comentarios desinformativos o vínculos a otros sitios web no oficiales e incluso maliciosos.
- **Publicación intencional de información no autorizada:** En la actualidad se han reportado múltiples vulnerabilidades en los portales de los Social Media que permiten a terceros malintencionados la publicación de mensajes no autorizados y mensajes publicitarios (spam), causando malestar a los clientes del servicio y afectando la imagen corporativa de las organizaciones afectadas.
- **Eliminación accidental de la información publicada.** Un tercero mal intencionado podría eliminar la información publicada impidiendo la divulgación de la misma.

4.1.2 Empleados

Es necesario tener en cuenta, que los usuarios que no se encuentran a gusto con la organización, podrían en determinado momento, faltar a su ética y realizar acciones perjudiciales para su organización en forma de retaliación por su malestar. Los administradores del Social Media, o cualquiera de los empleados que tenga acceso al Social Media para publicar comentarios o subir material audiovisual podrían publicar información que afecte a la organización o a otros empleados, generando responsabilidades legales. Ejemplo: Violaciones a derechos de autor o difamaciones.

- **Ingenuidad del empleado:** Una gran parte de los usuarios finales son reacios a seguir las recomendaciones de buen uso de las

[7] http://www.sophos.com/pressoffice/news/articles/2007/08/facebook.html
[8] http://www.idtheftdailynews.com/entity/profile/facebook/

nuevas tecnologías (ejemplo: políticas de contraseñas, políticas de PC seguro, etc.), ocasionando la inefectividad de los controles; adicionalmente, la ingenuidad de los usuarios finales, respecto a la inseguridad informática y a las estafas en línea, los hace susceptibles a ataques de ingeniería social.

- **Mala higiene informática:** El usuario final considera en muchas ocasiones que su PC de la casa es un PC seguro, sin embargo, no se preocupa por mantenerlo como tal, es decir, olvida o no se interesa por tener una buena suite de antivirus, firewall, y detector de intrusos; olvida actualizar su sistema operativo y aplicaciones; descarga e instala software desconocido; descarga y abre documentos y archivos multimedia de procedencia desconocida, generando ambientes de baja seguridad o poca higiene informática.
- **Divulgación accidental o intencional de información confidencial (reserva bancaria) a través del Social Media**: Todos y cada uno de los Social Media tienen un documento de políticas de uso, que por lo general, establecen que el administrador de la página debe ser un representante autorizado por la organización y que toda la información que éste allí cargue, quedará publicada bajo la configuración de privacidad abierta para "todos". Ejemplo: Documento de Normas de las Páginas de Facebook[9],
- **Divulgación accidental o intencional de información protegida por las leyes de propiedad intelectual y derechos de autor**: Los Social Media, en general, establecen que los usuarios y organizaciones que hacen uso de sus servicios para publicar material, conceden una licencia no exclusiva, transferible, con posibilidad de ser sub-otorgada, sin *royalties* y aplicable globalmente, para utilizar cualquier contenido que sea publicado. Ejemplo: Documento de Declaración de Derechos y

[9] Normas de las páginas de Facebook: http://www.facebook.com/terms_pages.php

Responsabilidades [10] de Facebook, en el numeral segundo, en relación al contenido protegido por las leyes de Derechos de Autor y Propiedad Intelectual.

- **Divulgación accidental o intencional de información sensible o personal por parte de los empleados del Banco que hagan uso del Social Media**: Los empleados del Banco, podrían realizar publicaciones intencionales o accidentales en los Social Media del Banco de la República, que ocasionen la divulgación de información de carácter sensible para el Banco y/o de carácter personal para los demás empleados.
- **Alteración accidental o intencional de información publicada por parte del administrador o los administradores del Social Media:** El(los) administrador(es) del Social Media, autorizados por el Banco para tal fin, podrían modificar el contenido a su discreción desde y fuera de la red del Banco.
- **Eliminación accidental o intencional de la información o de la cuenta de servicio del Social Media:** El administrador está en capacidad de eliminar información del Social Media e incluso, cancelar la cuenta y el servicio del Social Media.

4.1.3 Usuario final, cliente

- **Publicación de contenido ofensivo por parte de los visitantes de la página:** Estadísticas de los últimos años reportan que cerca del 80% de los blogs o bitácoras, contienen lenguaje ofensivo, el cual puede ir desde lenguaje para adultos hasta imágenes pornográficas.[11]
- **Quejas y reclamos públicos:** Afectación de la imagen de la organización ante la posibilidad de que los visitantes de los Social

[10] Declaración de Derechos y Responsabilidades: http://www.facebook.com/terms.php#/terms/spanish.php
[11] http://www.scansafe.com/__data/assets/pdf_file/3717/gtr_mar2007_v4.pdf

Media, realicen comentarios acerca de las publicaciones realizadas en este medio, incluso, ante la posibilidad de que se presenten quejas o reclamos públicos.

4.2 Amenazas asociados a las nuevas tecnologías

4.2.1 Malware o código malicioso:

Infortunadamente, no todas las nuevas tecnologías buscan algo positivo, con frecuencia aparecen en la red programas cuya finalidad es la de afectar los servicios, alterar la información o simplemente robarla. Se encuentran catalogadas como malware todas las aplicaciones de tipo adware (pop-ups, baners), trackware (barras de herramientas sensibles al contexto) y el spyware (envía a terceros información acerca de los hábitos de navegación e información confidencial del usuario), adicionalmente, se incluyen también todos los programas tipo virus, gusanos y troyanos. Ejemplo: Koobface[12], fue el primer malware que se transmitió a través de las redes sociales MySpace y Facebook y Twitter entre otras.

4.2.2 Errores en el software (bugs y vulnerabilidades):

Como la mayoría de estas aplicaciones son desarrolladas bajo licencias públicas (GNU), es fácil encontrar errores en el código fuente que pueden ser explotados por un atacante, para ejecutar código arbitrario en un sistema remoto. Prueba de ello son las múltiples notificaciones generadas mensualmente por organizaciones como el CERT, *Computer Emergency Response Team*[13]. Ejemplo: En el último año se han reportado cerca de una decena de bus en portales de blogs y redes sociales que permiten circunvenir los controles de privacidad de los usuarios.

[12] J. Baltazar, J. Castroya, R. Florez. The real face of Koobface: The largest Web 2.0 Botnet Explained. TrendMicro Threat Research.

[13] CERT: Centro de expertos para la seguridad en Internet, opera en Estados Unidos, Carnegie Mellon University.

4.2.3 Social Media

- **No disponibilidad del servicio de divulgación (Social Media):** En el último año, se han reportado algunos ataques de negación de servicio que han atentado contra la disponibilidad de los servicios de redes sociales[14].
- **Clausura o suspensión del servicio por violación a las normativas del Social Media:** Los Social Media se reservan el derecho a excluir de la red social, y a cancelar los servicios que esta presta, a cualquier individuo u organización que incumpla con los derechos y deberes proclamados su normativa.
- **No divulgación del contenido públicado:** Muchos de los Social Media, en sus documentos normativos o de acuerdos de nivel de servicio (SLA), se eximen de responsabilidad en el proceso de distribución del material o la información compartida por el administrador del Social Media. Ejemplo: Normas de las Páginas de Facebook[15].

4.3 Amenazas asociadas a los procesos y procedimientos de administración de los Social Media.

4.3.1 Administración del Social Media

En la actualidad, el único mecanismo de autenticación usado en Social Media es la combinación usuario-contraseña y el canal de acceso es la Internet, por lo tanto, el administrador del Social Media podría conectarse desde cualquier lugar del mundo, incluso, desde PCs de uso público.

- **Gestión de contraseñas:** Los mecanismos de autenticación utilizados por los Social Media no son lo suficientemente fuertes.

[14] http://news.cnet.com/8301-27080_3-10305200-245.html
[15] Normas de las páginas de Facebook: http://www.facebook.com/terms_pages.php

- **No divulgación de procedimientos de autorización de publicación:** La falta de divulgación del esquema de gobierno de los Social Media dentro de la organización puede ocasionar que se presenten movimientos no autorizados en canales de Social Media no autorizados.

4.3.2 Monitoreo del Social Media

En la actualidad no existen mecanismos automatizados que permitan monitorear el contenido publicado en el Social Media, esto podría ocasionar que incidentes que atenten contra la imagen de la organización no sean detectados a tiempo.

- **Ausencia de monitoreo de uso de imagen corporativa:** No hay mecanismos automatizados que permitan navegar la red en búsqueda de usos nos autorizados de la imagen corporativa.
- **Ausencia de monitoreo de comentarios y/o contenidos:** No hay mecanismos ni procedimientos que permitan monitorear en tiempo real los contenidos publicados ni los comentarios realizados.

4.3.3 Revisiones contractuales o de licenciamiento de uso.

- **Acuerdos de Nivel de Servicio del Social Media:** Todos y cada uno de los diferentes Social Media tienen documentos en los que presentan sus acuerdos de nivel de servicio. La mayoría de ellos se exonera de los daños que pueda causar la ausencia de servicio y se reservan el derecho a publicar la información subida por el usuario.
- **Condiciones de uso del Social Media:** Los Social Media poseen documentos en donde se expresan las condiciones de uso y los usos aceptables de los servicios por ellos prestados.
- **Acuerdos de privacidad:** En términos de privacidad, los Social Media cambian con cierta frecuencia sus acuerdos de privacidad,

por lo tanto, la organización debe monitorear estos cambios y analizar sus implicaciones.

- **Autorización de publicación:** Los Social Media obtienen mediante la aceptación de los acuerdos servicio, una autorización para publicar la información subida por los usuarios, esto les concede de una u otra forma, algunos derechos patrimoniales de puesta a disposición del material audiovisual de sus usuarios.

5. IDENTIFICACIÓN DE CONTROLES

Es necesario determinar los controles existentes o necesarios para mitigar el riesgo, ya sea porque se reduzca la probabilidad de ocurrencia o porque impide o complica el actuar del agente de amenaza.

5.1 Controles de Gobierno

- **Establecer Políticas de Seguridad:** Es necesario establecer políticas de seguridad de la información que dicten los lineamientos corporativos relativos al uso de los Social Media. El Departamento de Seguridad de la Información será el encargado de escribir, mantener y velar por el cumplimiento de esta política.
- **Establecer esquemas de gobierno:** Es necesario definir y establecer la estructura organizacional, los procesos y los procedimientos que gestionaran el uso de los Social Media. Se recomienda el uso de un esquema federado y liderado por la Oficina de Comunicación Institucional.

5.2 Controles tecnológicos

- **DLP (Data Lost|Leak Prevention):** Estos controles permiten evitar la fuga de información confidencial o sensible de una organización, sin embargo, la efectividad de este tipo de controles depende de

que la organización realice una buena clasificación de la información.

- **Software Antimalware:** La instalación y uso de software antimalware (antivirus, antispyware, etc.) en los PCs utilizados por los administradores de los Social Media, disminuyen la probabilidad de que las contraseñas sean robados por terceros malintencionados.

5.3 Controles a nivel de procedimientos

- **Cambio de contraseñas y contraseñas fuertes:** Se recomienda a los administradores de los Social Media el cambio de las contraseñas con una frecuencia de 30 días y el uso de contraseñas fuertes.
- **Administración desde la organización:** A pesar de que los administradores podrían conectarse a los Social Media desde cualquier lugar, se recomienda que sólo lo hagan desde los PCs de la organización, ya que estos están protegidos por diferentes medidas de seguridad.
- **Autorización de publicación:** Se recomienda que exista una unidad organizacional encargada de aprobar la información que será publicada en los Social Media. La unidad organizacional encargada de dar el visto bueno a las publicaciones, deberá solicitar como criterio de aprobación, los derechos de puesta a disposición del material audiovisual.
- **Monitoreo de los Social Media:** Se recomienda la revisión periódica, al menos dos veces al día, de los canales de comunicación interactiva en búsqueda de comentarios negativos o perjudiciales para la imagen de la organización. Adicionalmente, es necesario monitorear la red en busca de posibles suplantaciones o usos no autorizados de la marca.

- **Sensibilización:** Periódicamente es necesario enviar notificaciones preventivas a los usuarios o clientes acerca de los peligros que existen en la red y de las precauciones que deberían tomar para protegerse. Se debe realizar una capacitación intensiva a los administradores de los Social Media.

5.4 Controles legales

- **Revisión de los acuerdos de servicio:** La organización, con la colaboración del Departamento Jurídico, deberán revisar los acuerdos de servicio de cada uno de los Social Media que vayan a ser utilizados para la interacción con sus clientes.
- **Revisión de los derechos de autor y/o patrimoniales:** La organización, con el apoyo del Departamento Jurídico, deberán revisar las implicaciones legales de la cesión de derechos que implica la aceptación de los acuerdos de servicio del Social Media.
- **Aviso legal:** Es necesario adjuntar un aviso legal (Disclaymer) en todas y cada una de las publicaciones que se realicen en los Social Media.

6. CALCULO DE LA MATRIZ DE RIESGO

Este análisis hace uso de formas descriptivas para determinar la magnitud de las consecuencias potenciales asociadas a un riesgo y la probabilidad de que éstas ocurran. El valor cualitativo puede ser modificado de acuerdo a las necesidades de la organización y al riego particular evaluado.

Se realiza como una actividad inicial para identificar que riesgos necesitan estudio detallado, cuando el nivel de riesgo no es tal como para invertir tiempo y esfuerzos en un estudio escrupuloso ó cuando no se cuenta con datos numéricos.

La tabla 9 radica su importancia en la determinación exacta del nivel de riesgo, ésta matriz es una relación entre la magnitud de impacto y la probabilidad de ocurrencia de la amenaza.

Tabla 9. Matriz de nivel de riesgo.

PROBABILIDAD	IMPACTO		
	Bajo	Medio	Alto
Improbable	**Bajo**	**Bajo**	**Medio**
Probable	**Bajo**	**Medio**	**Alto**
Certero	**Medio**	**Alto**	**Alto**

En cualquier caso, estos descriptores podrían ser modificados para obtener niveles más amplios de clasificación del riesgo, los impactos y las probabilidades. No obstante, para este caso de estudio se partirá del uso del los descriptores básicos.

Tabla 10. Análisis de riesgo cualitativo para el uso corporativo de los Socia Media

Análisis de riesgo cualitativo para el uso corporativo de los Socia Media			Cumplimiento de Objetivos		Financiero		Intangibles Imagen		Responsabilidad Legal	
Fuente	Amenaza	Probabilidad	Impacto	Risk	Impacto	Risk	Impacto	Risk	Impacto	Risk
Asociadas al comportamiento humano	Delincuentes informáticos		ALTO		ALTO		ALTO		ALTO	
	Suplantación o robo de identidad	Probable	Alto	Alto	Alto	Alto	Alto	Alto	Alto	Alto
	Alteración intencional de la información publicada	Probable	Medio	Medio	Alto	Alto	Alto	Alto	Alto	Alto
	Publicación intencional de información no autorizada.	Probable	Medio	Medio	Alto	Alto	Alto	Alto	Alto	Alto
	Eliminación intencional de información publicada.	Probable	Medio	Medio	Bajo	Bajo	Bajo	Bajo	Bajo	Bajo
	Empleados		ALTO		ALTO		ALTO		ALTO	
	Divulgación accidental o intencional de información confidencial (reserva bancaria)	Probable	Alto	Alto	Alto	Alto	Alto	Alto	Alto	Alto
	Divulgación accidental o intencional de información protegida con Copyright.	Probable	Medio	Medio	Medio	Medio	Alto	Alto	Media	Medio
	Divulgación accidental o intencional de información sensible o personal	Probable	Medio	Medio	Bajo	Bajo	Bajo	Bajo	Alto	Medio
	Alteración accidental o intencional de la información publicada	Probable	Medio	Medio	Alto	Alto	Alto	Alto	Alto	Alto
	Publicación accidental o intencional de información no autorizada.	Probable	Medio	Medio	Alto	Alto	Alto	Alto	Alto	Alto
	Eliminación accidental o intencional de información publicada.	Probable	Medio	Medio	Bajo	Bajo	Bajo	Bajo	Bajo	Bajo
	Mala higiene informática	Probable	Alto	Alto	Alto	Alto	Alto	Alto	Alto	Alto
	Atacante interno	Probable	Alto	Alto	Alto	Alto	Alto	Alto	Alto	Alto
	Usuarios finales o clientes		ALTO		MEDIO		ALTO		ALTO	
	Publicación de contenido ofensivo	Certero	Bajo	Medio	Bajo	Medio	Alto	Alto	Media	Alto
	Quejas y reclamos públicos	Probable	Medio	Alto	Medio	Medio	Alto	Alto	Media	Alto

Análisis de riesgo cualitativo para el uso corporativo de los Socia Media			Cumplimiento de Objetivos		Financiero		Intangibles Imagen		Responsabilidad Legal	
Fuente	Amenaza	Probabilidad	Impacto	Risk	Impacto	Risk	Impacto	Risk	Impacto	Risk
Asociadas a la tecnología	Código malicioso		BAJO		MEDIO		MEDIO		MEDIO	
	Virus informáticos	Probable	Bajo	Bajo	Medio	Medio	Bajo	Bajo	Medio	Medio
	Malware (Adware, Spyware, etc.)	Probable	Bajo	Bajo	Medio	Medio	Medio	Medio	Medio	Medio
	Vulnerabilidades y exposiciones comunes		BAJO		BAJO		MEDIO		BAJO	
	Errores de configuración	Probable	Bajo	Bajo	Bajo	Bajo	Medio	Medio	Bajo	Bajo
	Errores de programación	Probable	Bajo	Bajo	Bajo	Bajo	Medio	Medio	Bajo	Bajo
	Servicio del Social Media		BAJO		BAJO		MEDIO		BAJO	
	No disponibilidad del servicio por DoS.	Probable	Bajo	Bajo	Bajo	Bajo	Medio	Bajo	Bajo	Bajo
	Clausura o suspensión del servicio por incumplimiento de las normativas.	Improbable	Bajo	Bajo	Bajo	Bajo	Alto	Medio	Medio	Bajo
	No divulgación del contenido publicado	Improbable	Medio	Bajo	Bajo	Bajo	Medio	Bajo	Bajo	Bajo
Asociadas a los procesos y procedimientos	Administración del Social Media		ALTO		ALTO		ALTO		ALTO	
	Ausencia de gestión de contraseñas	Certero	Medio	Alto	Medio	Alto	Alto	Alto	Alto	Alto
	No divulgación de procedimientos para la autorización de publicación	Probable	Medio	Medio	Bajo	Bajo	Medio	Medio	Bajo	Bajo
	Monitoreo del Social Media		MEDIO		MEDIO		ALTO		ALTO	
	Ausencia de monitoreo al uso de la imagen corporativa	Certero	Bajo	Medio	Bajo	Medio	Alto	Alto	Medio	Alto
	Ausencia de monitoreo a los comentarios y/o contenidos	Probable	Alto	Alto	Bajo	Bajo	Alto	Alto	Medio	Medio
	Revisión contractual o de licenciamiento de uso		ALTO		ALTO		ALTO		ALTO	
	No revisión de los acuerdos de nivel de servicio	Certero	Medio	Alto	Bajo	Medio	Bajo	Medio	Medio	Alto
	No revisión de las condiciones de uso del Social Media	Certero	Medio	Alto	Medio	Alto	Bajo	Medio	Medio	Alto
	No revisión de los acuerdos de privacidad	Certero	Medio	Alto	Medio	Alto	Medio	Alto	Alto	Alto
	No revisión de la cesión de derechos y autorización de puesta a disposición.	Certero	Alto	Alto	Alto	Alto	Alto	Alto	Alto	Alto

IV. CONCLUSIONES

El uso de los Social Media se está convirtiendo en una fuerza motivadora del cambio para empresas e individuos. En la medida en que esta nueva tecnología de comunicación ofrece grandes oportunidades de interacción Business to Client (B2C) y Business to Business (B2B), también representa riesgos significativos que deben ser determinados y gestionados.

Los riesgos asociados a los Social Media, deben ser analizados desde una perspectiva que permita considerar no sólo los riesgos de su adopción sino también los riesgos del costo de oportunidad que se podrían presentar al ignorar las oportunidades potenciales que podrían generarse con la adopción de estas nuevas tecnologías de comunicación.

La metodología de análisis de riesgos presentada en este documento cumple con los requisitos mínimos establecidos por la norma ISO 27005 para la Gestión de Riesgos de Seguridad de la Información, por lo cual, puede ser empleada por una organización que desee alinearse con este estándar.

El caso de estudio contemplado en este análisis representa un buen ejemplo dada su heterogeneidad de funciones, permitiendo así que diferentes organizaciones puedan reflejarse con facilidad en el desarrollo de este documento y extrapolarse a sus funciones y objetivos particulares.

Los resultados del caso de estudio reflejan los altos riesgos en que podría incurrir una organización que utilice los Social Media para la publicación y divulgación de información de carácter sensible, dado los altos impactos que se causarían ante la materialización de amenazas contra la integridad de la información, dejando en claro la necesidad de implementar seguridades jurídicas sobre la información publicada cuando su divulgación sea absolutamente necesaria.

Los Social Media representan canales económicos y de gran penetración, excelentes para la publicación y divulgación de información de carácter público, como lo es la información de carácter cultural o educativo.

Queda plasmada la necesidad de regulación interna o gobierno corporativo sobre los Social Media como canales institucionales o de mercadeo para la organización, siendo el esquema federado el de mayores beneficios para cualquier organización.

El efecto de la sensibilización como contramedida a la ingenuidad de los empleados resulta ser, un control absolutamente necesario para las organizaciones que deseen optar por la adopción de los Social Media como un canal de comunicación institucional.

Existe hoy en día un nicho de negocio que se divisa en temas de monitoreo, control de contenidos, y autenticación fuerte para las organizaciones que deseen hacer uso de los Social Media y que desean proteger sus marcas e imagen corporativa.

V. BIBLIOGRAFÍA

- **Asur, Sitaram. Huberman, Bernardo.** Predicting the future with Social Media. Social Computing Lab at HP Labs. 2010.
- **Baltazar, Jonell. Cstoya Joey. Flores, Ryan.** The real face of Koobface: The Largest Web 2.0 Botnet Explained. Trend Micro Research. 2009.
- **Cappex.com.** Establish a Benchmark for Social Media use in College Admission. 2010.
- **Dutta, Soumitra. Mia, Irene.** Global Information Technology Report 2009-2010. World Economic Forum. 2010.
- **Hansche, Susan**. Official $(ISC)^2$ Guide to the CISSP-ISSEP CBK. Auerbach Publications. 2006
- **ISO/IEC 27005 International Standar.** Information Technologý, Security Techniques, Information Security Risk Management. 2008.
- **Jackson Lewis.** Social Media and the Workplace: Managing the Risks. 2009.
- **Johnson, B.** Social Media Intensity Services. IDG Connect. 2009.
- **Johnson, B.** Social Media Optimization Services. IDG Connect. 2009.
- **Joshi, Anupam. Finin, Tim. Java, Akshay. Kale, Anubhav. Kolari, Pranam.** Web 2.0 Mining: Analyzing Social Media. University of Maryland, Baltimore. 2007.
- **Kaplan, Andreas. Haenlein, Michael.** Users of the world, unite! The challenges and opportunities of Social Media. Kelley School of Business at Indiana University. 2009.
- **Owyang, Jeremiah.** How to organize your company for Social Computing. Forrester. 2009.
- **Redecker, Christine. Ala-Mutka, Kirsti. Punie, Yves.** Learning 2.0 – The impact of Social Media on Learning in Europe. JRC Technical Notes. 2010.

- **Rico, Salomon. Bradley, Ben. Kiefer, Michael.** Social Media: Business benefits and security, governace and assurance perspectives. ISACA. 2010.
- **Rust, Roland. Kannan, P.Na Peng.** The Customer Economics of Internet Privacy. University of Maryland. 2002.
- **Stewart, James Michel. Chapple, Mike.** CISSP Certified Information System Security Professional Study Guide. Sybex. 2008.
- **Tieto.** Social Media and networking drive changes in financial services. What do Internet users expect of social lending and banking services?. Tieto 2010.
- **Various Authors.** Participative Web and User Created Content – Web 2.0, Wikis and Social Networking. OECD – Organization for Economic Co-Operation and Development. 2007.
- **Various Authors.** Piracy of Digital Content. OECD – Organization for Economic Co-Operation and Development. 2009.
- **Various Authors.** The role of digital identity management in the Internet Economy: A primer for policy makers. OECD – Organization for Economic Co-Operation and Development. 2008.
- **Won Gyum No,** An Empirical Investigation of Internet privacy: Customer behavior, Companies' Privacy Policy Disclosure, and a Gap. University of Waterloo. Ontario, Canada. 2007.