ANÁLISIS DE RIESGOS PARA APLICACIONES P2P

AUTOR:

SHIRLEY PAOLA HERRERA HERNÁNDEZ

UNIVERSIDAD INDUSTRIAL DE SANTANDER

FACULTAD DE INGENIERIAS FÍSICO-MECÁNICAS

ESCUELA DE INGENIERÍAS ELÉCTRICA, ELECTRÓNICA Y TELECOMUNICACIONES

ESPECIALIZACIÓN EN TELECOMUNICACIONES

BUCARAMANGA

2007

ANÁLISIS DE RIESGOS PARA APLICACIONES P2P

AUTOR:

SHIRLEY PAOLA HERRERA HERNÁNDEZ

PROYECTO DE GRADO

DIRECTOR:

Mag. FABIAN MOLINA MOLINA

UNIVERSIDAD INDUSTRIAL DE SANTANDER

FACULTAD DE INGENIERIAS FÍSICO-MECÁNICAS

ESCUELA DE INGENIERÍAS ELÉCTRICA, ELECTRÓNICA Y TELECOMUNICACIONES

ESPECIALIZACIÓN EN TELECOMUNICACIONES

BUCARAMANGA

2007

TITULO: ANÁLISIS DE RIESGOS PARA APLICACIONES P2P*

AUTOR: HERRERA HERNANDEZ, Shirley Paola**

PALABRAS CLAVES:

Seguridad de la información

Aplicaciones P2P
Análisis de riesgos
Gestión de riesgos
Mensajería Instantánea
Soluciones tecnológicas
Comunicación
Red de datos

CONTENIDO:

Hoy en día muchas organizaciones a nivel mundial están empezando a contemplar el uso de aplicaciones P2P; no obstante, la falta de orientación y conocimiento en las evaluaciones y en el análisis de riesgos respectivo, hace necesario profundizar este estudio desde un punto de vista más formal. Razón por la cual en esta monografía se abordará dicho análisis a partir de la visión conceptual de la seguridad informática y con el formalismo sugerido por algunos estándares internacionales para el proceso de gestión, análisis y mitigación de riesgos, con el propósito de definir las ventajas y desventajas que implementar P2P conlleva para la organización. Bajo estas circunstancias, se visualizan aspectos técnicos, económicos, administrativos y por supuesto legales que generen pautas para evaluar la viabilidad del uso de este tipo de aplicaciones y así garantizar la integridad, disponibilidad y confiabilidad de la comunicación en la red de datos.

El objetivo principal de este trabajo es servir como punto de referencia y apoyar la toma de decisiones en cuanto al uso de aplicaciones P2P dentro de un ambiente corporativo, con base en la definición de una metodología de gestión de riesgos que pueda ser desarrollada por cualquier tipo de organización.

Conjuntamente se hace referencia a algunas soluciones tecnológicas que pueden ser adoptadas por la organización con el propósito de mitigar los riesgos consecuencia del uso de aplicaciones sobre redes P2P.

---

* Trabajo de Grado
** Escuela de ingenierías eléctrica, electrónica y de telecomunicaciones
Especialización en telecomunicaciones
Director. Magíster Fabián Molina Molina

TITLE: RISK ANALISYS FOR P2P APPLICATIONS*

AUTHOR: HERRERA HERNANDEZ, Shirley Paola**

KEY WORDS:

Information security
P2P applications
Risk analisys
Risk management
Instant messenger
Technological solutions
Communications
Data network

CONTENTS:

Nowadays, a lot of worldwide companies are beginning to consider the usage of P2P applications; however, the lack of teaching and knowledge of the evaluations and risk analysis makes necessary to study in depth from a more formal point of view. Therefore, in this project such analysis will be tackled from the conceptual view of network systems security and the suggested formalism by some international standards for the networks management, analysis, and risk reduction process, in order to define advantages and disadvantages for the organization when P2P applications are utilized. Under these circumstances, legal, administrative, economical, technical aspects that generate guidelines to evaluate use feasibility of this kind of applications are shown, in order to guarantee integrity, availability, and reliability of data network communication.

The main objective of this project is to serve as reference point and support to P2P applications usage decisions in a corporative environment, according to a methodology definition of risk management which could be developed by any kind of organization.

Jointly, some technological solutions are discussed that might be adopted by the organization with the purpose of reduce the risks caused by use of P2P applications on data networks.

_____

* Thesis

** Electrical, Electronical and Telecommunications engineering school
Telecommunications Specialization
Director: Master Fabian Molina Molina

DEDICATORIA

Para Tulito y Cris, soy lo que he llegado a ser,
Sólo y gracias a ustedes.

AGRADECIMIENTOS

A Dios por supuesto, por permitirme una vez más culminar otra etapa.

Agradezco a mi director de monografía, Fabián Molina por su apoyo y confianza, a mi evaluador Samuel Pinzón por mostrarme mis errores y hacer de éste un mejor trabajo, a Oscar G. por enseñarme que hasta lo imposible es posible y de forma muy especial a Jorge Medina, por su paciencia, su conocimiento, su orientación, sencillamente por ser el mejor asesor. GRACIAS.

A Cesar Duarte, Tatiana Navas y en general a la Coordinación de la Especialización en Telecomunicaciones por su total disponibilidad y colaboración.

A mi familia y amigos porque es inevitable contar con ustedes.

Shirley Herrera

TABLA DE CONTENIDO

ANEXOS

INDICE DE FIGURAS

INDICE DE TABLAS

INTRODUCCIÓN

La comunicación a través de las redes de datos se ha diversificado en los últimos tiempos gracias a los diferentes tipos de protocolos o arquitecturas que se utilizan, dando lugar a modelos de enlace como el *PEER TO PEER* (en español *par a par*) ó más conocido como **P2P[1];** sin embargo, la traducción par a par no supone que solo pueda haber transferencia de archivos entre dos equipos, implica que las maquinas pueden actuar como cliente o servidor al mismo tiempo, con lo cual se podría decir que P2P es una comunicación de "*igual a igual*".

Hoy en día muchas organizaciones a nivel mundial están empezando a contemplar el uso de aplicaciones P2P; sin embargo, 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 de aplicaciones desde una conceptualización en el área de la seguridad de la información para garantizar la integridad, disponibilidad y confiabilidad de la comunicación en la red de datos.

El objetivo principal de este trabajo es servir como punto de referencia y apoyar la toma de decisiones en cuanto al uso de aplicaciones P2P dentro de un ambiente corporativo, con base en la definición de una metodología de gestión de riesgos que pueda ser desarrollada por cualquier tipo de organización.

Conjuntamente se hace referencia a algunas soluciones tecnológicas que pueden ser adoptadas por la organización con el propósito de mitigar los riesgos consecuencia del uso de aplicaciones sobre redes P2P.

[1] De aquí en adelante se utilizará el término P2P para hacer referencia a aplicaciones P2P.

1. FUNDAMENTOS TEÓRICOS PARA EL DESARROLLO DEL TRABAJO

En este capítulo se exponen los fundamentos teóricos necesarios para el desarrollo de este trabajo, se involucran temas como la conexión de nodos, la definición, características, funcionalidad y aplicaciones del enlace P2P, así mismo se consideran aspectos relevantes de la teoría de gestión de riesgos, entre otros.

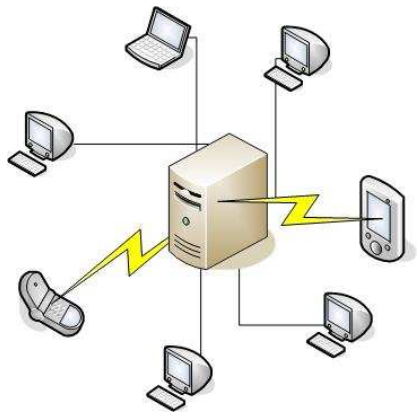
1.1 CONEXIÓN DE NODOS

Las redes de datos se pueden clasificar según su topología, la localización geográfica, la tecnología, el tipo de conexión de nodos entre otros y es en este último punto donde interviene el término **P2P**, que básicamente determina una forma de efectuar el proceso de transmisión de datos dentro de una red de computadores. Según el tipo de conexión de nodos, las redes de datos se clasifican en:

1.1.1 Conexión punto a multipunto

Se realiza en base a una sola estación que se comunica con múltiples usuarios, es la conexión típica en redes de radio o telefonía móvil.

Figura 1. CONEXIÓN PUNTO A MULTIPUNTO



Fuente: Aporte del autor

1.1.2 Acceso compartido

También llamada conexión por difusión, este tipo de enlace se realiza a través de un solo canal, por lo cual existen problemas con el control de acceso al medio, por lo general se trabaja en redes LAN[1] ó redes de televisión.

1.1.3 Conexión punto a punto

La comunicación se realiza entre dos computadores haciendo uso de un enlace dedicado, es utilizado por proveedores de acceso conmutado a Internet vía telefónica ó cuando el acceso a Internet es acceso con enlaces dedicados. Esta es la base del enlace P2P que se detalla a continuación[2].

[1] Local Area Network, hace referencia a la clasificación de redes debido a su localización geográfica.
[2] Si el lector desea mayor información al respecto favor revisar las referencias [Gualdrón, 2005] y [Tanembaum, 2003]

2. METODOLOGÍA DE ANÁLISIS DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

Dentro de la teoría de gestión de riesgos, que involucra determinar y minimizar los posibles impactos presentes en un evento de seguridad, se encuentra el análisis de riesgos. Este se lleva a cabo para determinar en conjunto con el tratamiento del riesgo la relación costo-beneficio y de esta forma decidir la viabilidad de un proyecto. La gestión de riesgos puede orientar la destinación de recursos y presupuesto en cuanto a seguridad se refiere[1].

Para realizar este análisis es necesario llevar a cabo los siguientes pasos:

- Identificación de bienes o activos
- Valoración de bienes o activos
- Identificación de las vulnerabilidades, amenazas, los riesgos asociados y la probabilidad de ocurrencia del riesgo.
- Determinar el impacto del riesgo mediante un análisis cuantitativo o cualitativo
- Calcular el nivel de riesgo

Finalmente después de realizar todo el estudio se obtendrán criterios suficientemente útiles para determinar la factibilidad de un proyecto. Así mismo se podrán identificar las fallas y establecer las posibles soluciones.

Este capitulo tiene por objeto proponer una metodología de análisis de riesgos de seguridad de la información, que cumpla con los ítems descritos anteriormente.

[1] Mayor información revisar la referencia [MEDINA, 2006]

2.1 METODOLOGÍA PARA LA REALIZACIÓN DE LA GESTIÓN DE RIESGOS

La descripción de la metodología que se realiza en páginas siguientes adopta las normas y guías establecidas para realizar una correcta gestión de riesgos, por ende se lleva a cabo una descripción general de este proceso de gestión, sin perjuicio de omitir una serie de pasos que no resultan determinantes para este trabajo; sin embargo, si se desea implementar todo un programa de gestión del riesgo es necesario seguir a profundidad los pasos que se listan a continuación, por lo cual se recomienda al lector interesado en este tema retomar la norma ISO 27001.

- Paso 1. Respaldo de la alta dirección
- Paso 2. Desarrollar una política pertinente para la organización
- Comunicación de políticas
- Gestión de riesgos a nivel organizacional
- Gestión de riesgos a nivel programa, equipo ó área
- Monitoreo y revisión de todos los mecanismos implementados.

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.

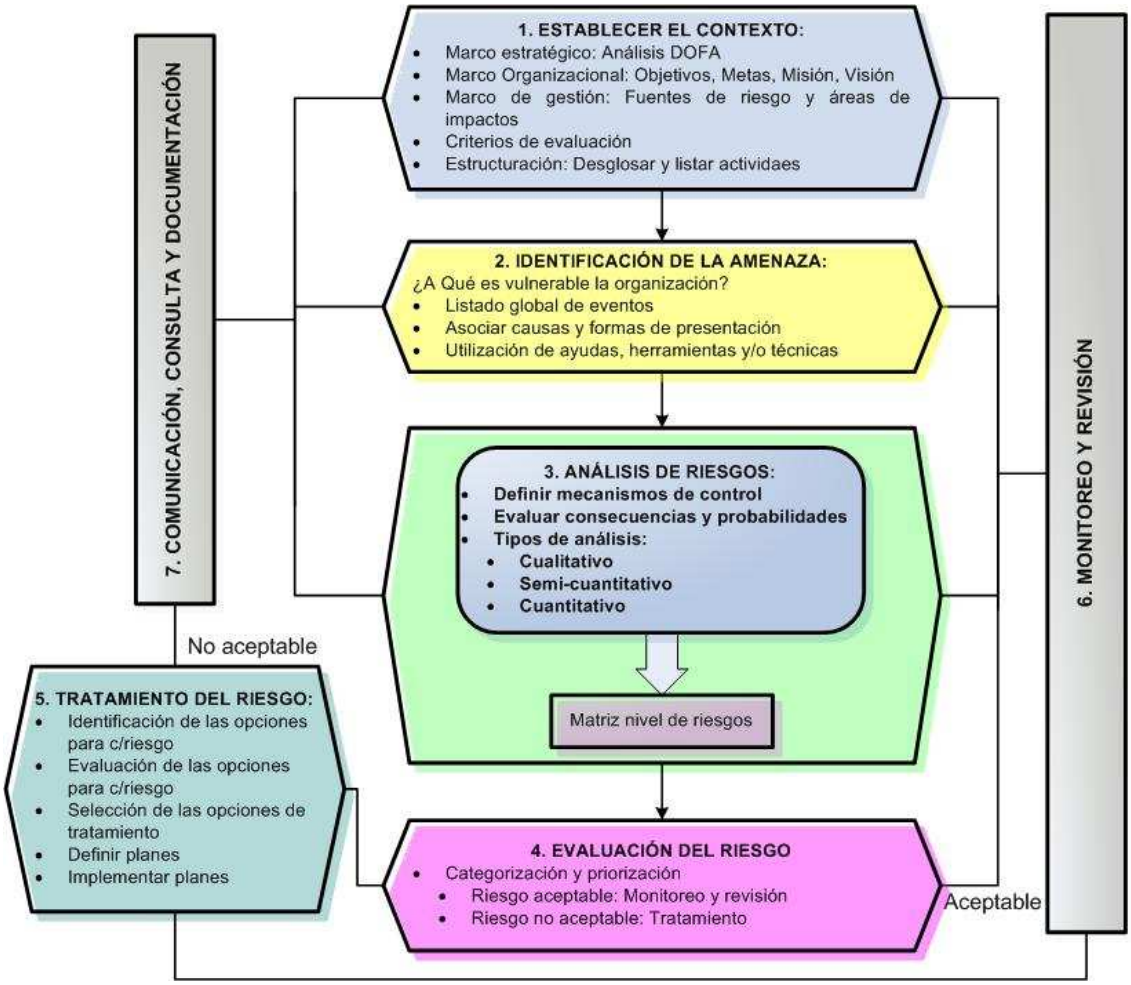
La seguridad de la información no es ajena a este concepto, por el contrario en un sin número de aplicaciones es necesario realizar e implementar la gestión del riesgo a fin de contener y mitigar los riesgos que puedan poner en peligro el funcionamiento o el correcto desempeño de una organización ya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

En estas secciones se detalla la estructura metodológica propuesta para ser implementada en el interior de una organización, se tomó como base algunas

metodologías ya establecidas, éstas pueden ser tanto de carácter comercial como de uso libre por ejemplo: OCTAVE, MAGERIT, entre otras. Asimismo se darán las pautas para el análisis de riesgos realizado a aplicaciones P2P descrito en el capítulo 3 de este documento.

La figura 5 presenta el diagrama de bloques que resume esta metodología:

Figura 2. DIAGRAMA DE BLOQUES DE LA METODOLOGÍA DESCRITA



Fuente: Aporte del autor

2.2 PASOS A SEGUIR EN LA GESTIÓN DE RIESGOS

2.2.1 Paso 1. Establecer el contexto

Este paso enmarca los parámetros básicos para realizar la gestión de riesgos de forma que se define el entorno de todo el proceso de gestión, así como posteriores estudios mas detallados.

Para definir el contexto de un proceso de gestión es necesario alinearlo con el marco estratégico de la organización para así obtener la base del marco estratégico, organizacional y de gestión del proceso.

- **Marco ó contexto estratégico**: El análisis estratégico hace referencia a la relación que existe entre la organización y su entorno; éste estudio debe contar con el apoyo de la alta dirección para así poder desarrollar estudios mas detallados si es el caso; es importante resaltar que la gestión de riesgos necesita estar estrechamente relacionada con la misión, visión y objetivos de la organización.

  Para establecer un marco estratégico se deben realizar las siguientes tareas:

  - Análisis DOFA[1], teniendo en cuenta aspectos financieros, de operación, de imagen, sociales y culturales de las actividades que realiza la organización.
  - Identificación de las partes internas y externas interesadas o relacionadas con la organización.
  - Esclarecer y listar los elementos que pudieran apoyar o entorpecer la capacidad para enfrentar un riesgo.

- **Marco o contexto organizacional**: Para realizar un correcto proceso de gestión de riesgos es necesario comprender la organización, así como sus objetivos, proyectos, estrategias y necesidades debido a que las políticas y metas apoyan la definición de los criterios para determinar si un riesgo es aceptable o no, aditivo sus opciones de tratamiento.

[1] DOFA: Análisis administrativo que determina las Debilidades, Oportunidades, Fortalezas y Amenazas de una organización.

Tareas a desarrollar:

- Claridad sobre los objetivos, metas y estrategias de la organización.
- Conocer y entender las políticas, actividades y/o proyectos que realice la entidad.

- **Marco o contexto de gestión**: Este contexto complementa los anteriores, sumando el establecimiento de la actividad o departamento de la organización que va a ser analizada, por lo cual en este punto se debe:
  - Establecer el proyecto o actividad al igual que sus objetivos, metas específicas y alcances en tiempo y lugar.
  - Identificar y listar las áreas de impacto o fuentes genéricas de riesgos relacionadas con la actividad o el departamento de la organización.
  - Definir el alcance y las actividades de la gestión de riesgos a realizar.
  - Las funciones y responsabilidades de las partes que participan en el proceso de gestión.
  - Identificar procesos en proyectos de gestión similares pero de otras áreas u organizaciones. (Esto sirve como base para determinar los puntos anteriores)

Ahora bien una vez establecido el marco estratégico, organizacional y de gestión es necesario desarrollar los criterios de evaluación y la estructuración de actividades significativas.

- **Criterios de evaluación**: En este punto del proceso se deben definir los criterios para evaluar si un riesgo puede ser aceptable o no, y de esta forma determinar que tipo de tratamiento se debe llevar a cabo. La definición de esta evaluación se basa en los criterios a continuación listados; sin embargo, éstos a su vez se ven influenciados por la política interna de la organización, sus objetivos, metas e interés de las partes involucradas:
  - Operacionales
  - Técnicos
  - Financieros
  - Legales

- Sociales o humanitarios
- Percepciones internas y externas

Cabe mencionar que aunque en este punto se determinan los criterios de evaluación, éstos pueden verse modificados a medida que se completan todos los pasos en el proceso de gestión de riesgos, debido a que es factible encontrar riegos particulares y por ello adecuar diferentes técnicas de análisis; no obstante, la definición de estos criterios en este punto es de vital importancia para no perder el objeto de la gestión.

- **Actividades estratégicas**: Se define como la división de las actividades o proyectos en un listado de elementos con el fin de no pasar por alto riesgos importantes, al desglosar las actividades se busca generar un espacio que permita identificar y realizar un correcto análisis, como siempre el desglose va ligado a la actividad de la organización y por supuesto a la naturaleza del riesgo.

2.2.2 Paso 2. Identificación de la amenaza ¿a qué es vulnerable la organización?

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 facilitar esta tarea se aconseja resolver los siguientes interrogantes:

- **¿Que vulnerabilidades se encuentran en la organización?** Pero específicamente que vulnerabilidades tiene la organización relacionadas con la actividad o el departamento a analizar, para esto el grupo encargado del estudio se debe basar en el marco estratégico, organizacional y de gestión que ya se ha evaluado.
- **¿Cómo y por qué puede suceder?** Existen amenazas que pueden ser explotadas ocasionando que el riesgo sea inevitable; sin embargo, existen también otras amenazas que aunque es posible determinarlas no

representan un peligro para la organización, razón por la cual es fundamental determinar en este punto cuales son las amenazas reales que pueden converger en un riesgo.

Para documentar este ítem se aconseja listar a cada vulnerabilidad ya establecida, las amenazas que puedan ser explotadas, y así mismo determinar en el siguiente interrogante los riesgos asociados a estas amenazas.

- **¿Que Ayudas, herramientas y/o técnicas deben ser utilizadas?** Existen diferentes técnicas o métodos para identificar las causas y el mismo riesgo, pero éstas dependen de la naturaleza de las actividades que se están revisando, así como de los tipos de riesgo. Algunas técnicas son:
    - Listas de verificación.
    - Juicios basados en otras experiencias o registros
    - Diagramas de flujo
    - Lluvia de ideas
    - Análisis de sistemas o de escenarios
    - Existen unas mas avanzadas como técnicas de ingeniería de sistemas o minería de datos[1].

2.2.3 Paso 3. Análisis del Riesgo

Este paso es el centro del proceso de gestión de riesgos, el análisis del riesgo pone en consideración las fuentes de riesgo, sus consecuencias y las posibilidades de que estas ocurran, con el objeto de determinar la aceptabilidad de un riesgo y el tratamiento que se debe implementar.

Es posible realizar un pre-análisis para excluir del estudio detallado los riesgos de bajo impacto o de características similares; sin embargo, debe haber un listado registrado con estos riegos para así documentar un análisis del riego completo.

[1] Mayor información revisar la referencia [Orallo, Quintana & Ramírez, 2005]

Para realizar este análisis, se parte de los listados y los resultados que se han obtenido en los numerales anteriores, se analizan diferentes combinaciones de cálculos de consecuencias y mecanismos de control existentes partiendo de los 3 tipos de análisis que se describen mas adelante.

- **Mecanismos de control**: Se refiere a la administración, los sistemas técnicos y procedimientos que buscan controlar el riesgo; se evalúan sus fortalezas y debilidades. Para este paso es posible apoyarse en las técnicas y herramientas descritas en el paso 2 y/o métodos que involucran inspecciones y técnicas de auto-evaluación.
- **Consecuencias y probabilidad**: Debe evaluarse el impacto de las consecuencias asociadas a un evento y combinarlas con la probabilidad de ocurrencia para determinar el nivel de riesgo, esto mediante análisis y cálculos estadísticos, también es posible basarse en datos del pasado para ello y con el propósito de no realizar sesgos subjetivos se recomienda tener en cuenta las siguientes fuentes de información:
    - Registro de otros estudios
    - Experiencia pertinente
    - Prácticas y experiencias industriales
    - Literatura publicada y reconocida (Internet)
    - Investigaciones de mercado
    - Modelos económicos
    - Minería de datos
    - Juicios de expertos

    Como ejemplo de técnicas para realizar estos análisis se tiene:

    - Realizar entrevistas a expertos en el área de interés
    - Organizar grupos de expertos interdisciplinarios
    - Evaluaciones individuales realizadas a los integrantes del área de gestión evaluada.
    - Uso de árboles de error y árboles de eventos.

- **Tipos de análisis**: Existen 3 tipos de análisis del riesgo, que se diferencian por su grado de exactitud y esto va a depender de la información y disponibilidad de los datos; no obstante, todos tienen el mismo principio determinar la matriz de nivel de riesgos.

  Se tiene entonces el análisis cualitativo, semi-cuantitativo y cuantitativo, en la práctica se realiza primero un análisis cualitativo ó pre-análisis que arroja un nivel de riesgo general y luego se focaliza realizando un análisis cuantitativo en el área de interés.

  - Análisis cualitativo: 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.

  Las tablas 1 y 2 son un ejemplo de los indicadores descriptivos que normalmente son empleados:

Tabla 1. Descriptores para consecuencias o impactos

NIVEL	DESCRIPTOR	DETALLE (se hace referencia a consecuencias médicas y financieras)
1	Bajo	Ningún daño, pérdidas financieras insignificantes.
2	Medio	Primeros auxilios, Perdidas financieras medianas
3	Medio – Altos	Tratamiento médico, perdidas en la capacidad de producción, perdidas financieras importantes
4	Alto	Daños graves, muerte, perdida financiera más que considerable.

Tabla 2. Descriptores cualitativos para probabilidad

NIVEL	DESCRIPTOR	DETALLE
a	Improbable	Puede ocurrir solo en situaciones excepcionales
b	Posible	Es posible que ocurra en algunas ocasiones
C	Probable	Podría ocurrir en la mayoría de las circunstancias
d	Casi cierto	Se espera que ocurra en la mayoría de circunstancias

La tabla 3 radica su importancia en la determinación exacta del nivel de riesgo, ésta matriz es una relación entre la descripción del impacto y su probabilidad de ocurrencia y es utilizada para encasillar cada riesgo asociado, encontrado en el paso 2.

Tabla 3. Matriz de nivel

PROBABILIDAD	IMPACTOS			
	Bajo	Medio	Medio-Alto	Alto
a) Improbable	L	L	L	L
b) Posible	L	M	M	H
c) Probable	L	M	E	E
d) Casi cierto	L	H	E	E

L = Nivel inferior (*Low*), gestionar riesgo mediante rutina

M = Nivel Moderado (*Midle*), especifica la responsabilidad de la dirección.

H = Nivel Alto (*High*) necesita la atención del director

E = Nivel Extremo (*Extrem*), Requiere acción inmediata

Nota: *como se mencionó anteriormente estas tablas pueden modificarse de acuerdo a las necesidades y requerimientos de la organización y la naturaleza de los riesgos, es posible variar el orden, el número o el detalle de cada nivel descriptivo. Se recomienda trabajar con niveles pares debido a que algunos estudios indican que al trabajar con niveles impares las personas tienden a optar por la media*.

- Análisis semi-cuantitativo: Se basa en el estudio cualitativo, pero a diferencia de éste, se asigna un valor numérico a los niveles descriptivos detallados en las tablas 3 y 4. Éste análisis tiene por objeto generar una priorización más detallada que la que surge del análisis cualitativo; no obstante, no llega a sugerir un valor numérico tan real como el que se busca en el análisis cuantitativo.

  Hay que resaltar que este tipo de análisis necesita un correcto estudio para su implementación, ya que es posible que la selección de los números relacionados no muestre el verdadero nivel del riesgo, en especial cuando los impactos y la probabilidad son extremos, por ende no se realiza un acertado análisis del riesgo, poniendo en peligro todo el proceso.

  En este punto es necesario hacer referencia a dos conceptos que componen la “posibilidad de ocurrencia” éstos se relacionan mediante la multiplicación de sus valores.

  a). **Frecuencia de exposición**: Grado de existencia de una fuente de riesgo.

  b). **Probabilidad:** Grado de materialización y sus consecuencias de una fuente de riesgo.

- Análisis cuantitativo: Este tipo de análisis es el más completo y por tanto el más complejo, asigna valores numéricos para determinar las consecuencias, probabilidades y nivel de riesgo, por lo cual la calidad de este análisis depende de la exactitud numérica y la veracidad de las fuentes de los datos empleados.

  Utiliza diferentes métodos para determinar cuantitativamente los niveles de las áreas estudiadas, las consecuencias, por ejemplo se

estiman de acuerdo a criterios monetarios, técnicos, humanos y se basa en datos históricos o extrapolación de estudios experimentales; en ocasiones se hace necesario utilizar más de un valor numérico para expresar las consecuencias, la posibilidad se expresa en términos de frecuencia de exposición, probabilidad o una combinación de ambas, por último el nivel de riesgo es una matriz resultado de la relación numérica combinatoria de las consecuencias, posibilidad y probabilidad, pero que están asociados desde luego al tipo de riesgo y al contexto de la organización.

Algunos ejemplos cuantitativos de la gestión de riesgos son:

a). **Pérdida financiera o ganancia**: Se multiplican las pérdidas financieras (o ganancias) de un periodo por la frecuencia anual del periodo, esto arroja como resultado el valor esperado por año.

b). **Fatalidad:** Puede ser calculado por el número de muertes por año ó el porcentaje de población expuesta.

c). **Desastres naturales**: En la práctica se acostumbra a utilizar productos software simuladores de desastres naturales, árboles de error, entre otros, acompañados de estudios y probabilidades de datos históricos.

- **Sensibilidad**: La realización de un estudio de sensibilidad se hace necesario cuando se utiliza el análisis cuantitativo, debido a que los resultados generados de este análisis pueden ser imprecisos, resulta entonces pertinente estudiar los cambios en los datos y las hipótesis de forma que se multiplique el valor cuantitativo del estudio anterior por la sensibilidad.

2.2.4 Paso 4. Evaluación del Riesgo

Una vez se obtiene la matriz del nivel de riesgo generada por la implementación de alguno de los tipos de análisis del numeral anterior, se realiza una comparación entre estos niveles y los criterios de riesgos que ya se han establecido (Criterios de evaluación, numeral 2.2.1)

Es necesario realizar esta comparación con la misma base tanto de la matriz como de los criterios; es decir, si la matriz es cualitativa, los criterios de riegos deben ser cualitativos, si se realizo un análisis cuantitativo, obteniéndose por ello una matriz cuantitativa, los criterios de comparación deben estar expresados en valores numéricos, esto con el fin de ser consistentes en todo el proceso de gestión.

Este paso tiene como objetivo obtener un listado de priorización de riesgos con el propósito que la dirección pueda tener la discrecionalidad para determinar que acciones deben llevarse a cabo; sin embargo, estas decisiones deben basarse en los objetivos, metas y actividades de la organización, las consecuencias de asumir el riesgo sin abandonar el contexto del mismo, finalmente debe incluirse la tolerabilidad de las partes interesadas y participes del área en cuestión.

Cuando se determina que un riesgo se encuentra en categorías como “bajo riesgo” o “aceptable” estos pueden tratarse con un mínimo de esfuerzo, pero siempre bajo supervisión y monitoreo para garantizar la permanencia en estas categorías.

El siguiente numeral (2.3.5) sugiere que hacer cuando la evaluación del riesgo arroje que éste no es “aceptable”.

2.2.5 Paso 5. Tratamiento del Riesgo

Este numeral hace referencia a las actividades que deben seguirse cuando se ha determinado que un riesgo no es “aceptable” y por ende debe ser tratado, se evalúan las opciones de tratamiento, los planes y la implementación de éste.

- **Opciones y evaluación para el tratamiento de un riesgo**: A continuación se enlistan las diferentes opciones que se tiene para tratar un riesgo:
    - Evitar el riesgo no ejecutando la actividad que puede generar el riesgo (siempre que sea posible) esta aversión al riesgo puede hacer que se generen otros riesgos mas importantes, además:

a.) Hacer una mala implementación del tratamiento pues se incurre en mayores costos sin importar la información que se tenga ya del riesgo.

b). Dejar decisiones en terceros que no poseen la competencia del caso.

c). Aplazar decisiones que no deben evitarse.

d). Tomar opciones con riesgos aparentemente menos potenciales sin importar los beneficios.

- Reducir la probabilidad de ocurrencia. La tabla 4 presenta algunos ejemplos que deben tenerse en cuenta y que ayudan a la dirección a reducir, mitigar ó controlar la posibilidad de ocurrencia.

Tabla 4. Acciones que disminuyen la probabilidad de ocurrencia

ACCIONES PARA CONTROLAR O MITIGAR LA PROBABILIDAD
Acciones de mejoramiento, resultado de auditorias y programas de verificación de cumplimiento
Condiciones contractuales
Revisión formal de requerimientos, especificaciones, diseño, ingeniería y operaciones
Inspección y procesos de control
Inversión y gestión de portafolios
Mantenimiento preventivo
Aseguramiento de calidad, gestión y normalización
I+DT+I (Investigación, Desarrollo Tecnológico e Innovación)
Formación estructurada
Supervisión y monitoreo
Ensayos, disposiciones organizacionales y técnicas de control

- Reducción de consecuencias. La tabla 5 muestra una serie de actividades que permiten reducir, mitigar y controlar las consecuencias asociadas a un riego.

Tabla 5. Acciones para disminuir consecuencias asociadas a un riesgo.

ACCIONES PARA CONTROLAR Y/O MITIGAR LOS IMPACTOS
Planes de contingencia
Arreglos y condiciones contractuales
Diseño de características
Planes de recuperación de desastres
Barreras estructurales y de ingeniería
Reducción de exposición a fuentes de riesgos
Planeación de control de fraudes
Planeación de portafolios de servicios
Políticas y control de precios y costos
Separación y/o reubicación de actividades y/o recursos
Relaciones publicas (pagos discrecionales)

- Transferir el riesgo: Esta opción involucra otras entidades u organizaciones que comparten parcial o totalmente la responsabilidad de asumir un riesgo; se implementan mecanismos como contratos o acuerdos de seguros, o alianzas estratégicas.

  El problema que conlleva esta decisión es que aunque se comparta el riesgo éste no disminuye para la sociedad, además se corre el "riesgo" que el tercero responsable no puede manejar correctamente la situación, convirtiéndose esta decisión en otro riesgo o problema.

- Retener el riesgo: A pesar de transferir o tratar los riesgos, es posible que queden algunos ya sea por fracaso en la identificación, por defecto o como resultado de tratamientos hechos; a estos riesgos se

les denomina “riesgo residual”; sin embargo, **lo más importante asegurar y verificar que el riesgo residual este por debajo del riesgo aceptable.**

Una vez estudiadas las formas de tratamientos que se tienen para mitigar los riesgos o impactos producidos por una amenaza explotada, es necesario evaluar estás opciones de tratamiento junto con criterios como: cultura organizacional, tiempo de implementación arquitectura, relación costo/beneficio, entre otros, además de los mencionados en el numeral 2.2.1, sin perjuicio de utilizarse una o la combinación de varias soluciones.

La decisión para optar una solución u otra está relacionada estrechamente de nuevo con las necesidades, objetivos, actividades y metas de la organización, con lo cual del estudio que se ha realizado a través de los pasos anteriores se ha podido determinar la prioridad del riesgo para tomar decisiones en las que se involucran grandes rubros presupuestales al ser implementadas, en estos términos es decisión de la dirección teniendo presenta la relación costo/beneficio qué resulta mas ventajoso y por supuesto esto va a depender expresamente del tipo de organización estudiada; sin embargo, en términos generales se puede decir que lo más recomendado en este punto del proceso de gestión es combinar las opciones de tratamiento para mitigar un riesgo, entre las cuales una de la combinaciones mas eficaces es unir la reducción de vulnerabilidades o probabilidades de ocurrencia de una amenaza, la reducción del impacto ante un evento no deseado, la transferencia y la retención del riesgo residual. En otras palabras es trabajar conjuntamente el uso efectivo de contratos y programas de mitigación de riesgos.

- **Planes de tratamiento**: Una vez se ha determinado qué acciones y controles se van a seguir para mitigar los riesgos es necesario documentar cómo se van a implementar estas soluciones.

  El plan de tratamiento busca entonces:

  - Identificar responsables
  - Realizar cronogramas
  - Establecer presupuestos

- Evaluar resultados esperados y medidas de desempeño: esta evaluación debe contrarrestar las opciones contra los criterios de desempeño, entendiéndose las responsabilidades individuales objetivos y monitoreo de actividades críticas.
- Realizar procesos de revisión por implementar.

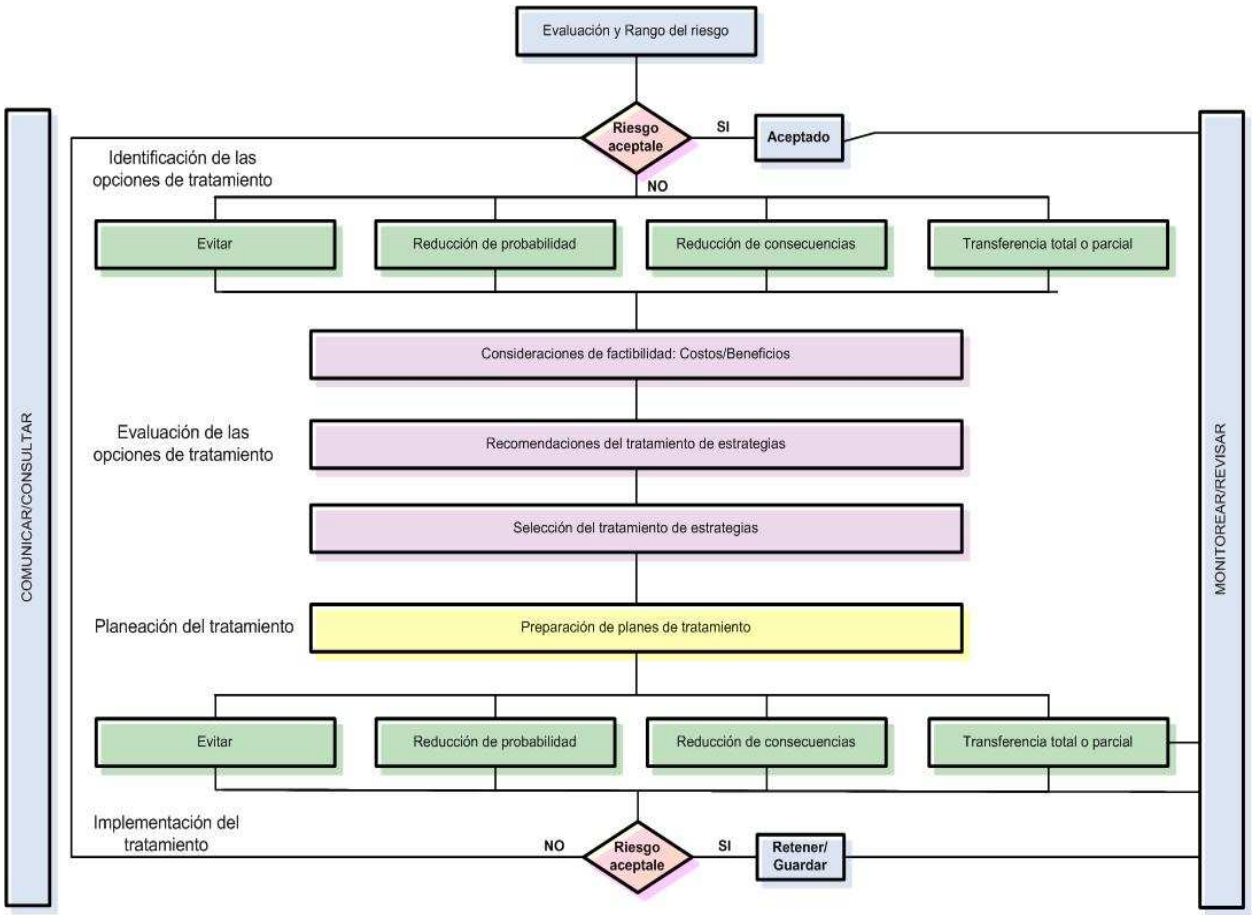
Figura 3. EJEMPLO FICHA PLAN DE TRATAMIENTO

Elemento Riesgo:	**Ref:**
Resumen – Respuesta recomendada e impacto	
Plan de acción: 1. Acciones propuestas 2. Recursos requeridos 3. Responsabilidades 4. Cronograma 5. Reporte y monitoreo requerido **Responsable**:_____ **Fecha**:_____ **Preparado por**:_____ **Fecha**:_____	

- **Implementación de planes de tratamiento**: Es crucial en la implantación de un plan de tratamiento establecer estrategias que especifiquen los métodos, las responsabilidades y funciones individuales, así como la monitorización con respecto a los criterios específicos. Esta tarea debe estar en mano de las personas capaces de enfrentar y mitigar los riesgos y de ser posible debe determinarse desde el principio quien será el

responsable de cada área de interés. Con respecto al riesgo residual resulta conveniente decidir si se va a retener o se va a implementar algún plan específico para mitigarlo; sin embargo, si esta por debajo del riesgo aceptable sólo es necesario su supervisión.

Figura 4. CUADRO RESUMEN TRATAMIENTO DEL RIESGO.



Fuente: Aporte del autor

2.2.6 Paso 6. Monitoreo y revisión

No es suficiente determinar y priorizar los riesgos e implementar soluciones que lleven a mitigarlos, es necesario realizar un acompañamiento con tareas de monitorización y revisión de los planes establecidos, las estrategias y el sistema de gestión con el objeto de garantizar el éxito, la pertinencia y la efectividad del tratamiento, aditivo asegurar que la condiciones cambiantes del sistema no alteren las prioridades establecidas, cabe mencionar que pocos riesgos son estáticos.

Se aconseja entonces repetir el ciclo de gestión del riesgo, así como su revisión y monitoreo, dependiendo de los criterios organizacionales, es fundamental llevar ésta tarea a cabo para obtener eficacia y asegurar el corrector desempeño de la organización.

2.2.7 Paso 7. Comunicación y Consulta

Aunque se describe al final de los pasos a realizar este punto debe acompañar todo el proceso de gestión, es fundamental para la optimización de resultados, establecer canales de comunicación entre todas las partes involucradas tanto externas como internas en el sistema de gestión, dado que este es un proceso conjunto entre las personas que toman las decisiones como quienes las ejecutan, debe propenderse por la comunicación bilateral, es posible que muchas de la decisiones que se tomen estén influenciadas por la aceptabilidad y las percepciones sobre riesgos, consecuencias y beneficios, provenientes de las partes implicadas con la gestión de riesgos. Se aconseja entonces identificar, documentar y entender estas percepciones.

2.3 DOCUMENTACIÓN

De igual forma como la comunicación la documentación es una etapa que está relacionada estrechamente con todo el proceso de gestión. El objetivo es documentar culturas organizacionales, métodos, fuentes de datos, resultados y todo el proceso en si desarrollado.

Se hace necesario adelantar esta documentación por las siguientes razones:

- Garantizar que el proceso seguido está siendo implementado de forma apropiada.
- Ofrecer un método sistemático para la identificación y análisis del riesgo.
- Llevar un registro de los riesgos para desarrollar una base de datos del conocimiento de la organización.
- Dar a las personas responsables un plan de gestión pertinente para su aprobación e implementación.

- Definir responsabilidades y responsables.
- Generar espacios de auditoria que garanticen la eficacia del proceso.
- Compartir y comunicar el proceso.

De forma global se mencionan algunos tópicos que deben estar presentes en la etapa de documentación:

- Objetivos
- Fuentes de información
- Suposiciones y decisiones
- Políticas
- Conformidad y declaraciones de debida diligencia. (responsabilidad en el cumplimiento de políticas y procedimientos)
- Registro de riesgos, para casa riesgo se debe llevar un registro de:
    - Fuente
    - Naturaleza
    - Controles existentes
    - Clasificación
    - Vulnerabilidad
- Cronogramas del tratamiento del riesgos y planes de acción
- Documentos para monitoreo, revisión y auditoria

3. EJEMPLOS PRÁCTICOS DE ANALISIS DE RIESGOS PARA APLICACIONES P2P

Este capítulo aborda la ejemplificación de la metodología de gestión de riegos descrita en el capítulo 2. Se realizará la implementación del método sugerido para evaluar los riesgos asociados al uso de una aplicación P2P dentro de un escenario determinado, con el propósito de analizar, evaluar, y presentar posibles opciones para mitigar los riesgos hallados durante el proceso de gestión. No obstante, es importante recalcar que éste escenario será un ejemplo ficticio, razón por la cual, no se profundizara en detalles como la visión, misión y demás descriptores de una organización.

El análisis de riesgos es único y directamente dependiente de cada organización, y derivará del escenario escogido.

3.1 GESTIÓN DE RIESGOS: MENSAJERÍA INSTANTÁNEA (MI[1])

3.1.1 Paso 1. Establecer el contexto

- **Marco Estratégico**: La gestión de riesgos aplicada a la mensajería instantánea (ésta aplicación puede incluir compartir archivos, transferencia de archivos, voz y video, entre otros), se realiza para una institución del sector público. La actividad que lleva a cabo la institución es la gestión y el apoyo para el desarrollo de la ciencia, la tecnología y la investigación desde perspectivas académicas, productivas y empresariales a nivel regional, nacional e internacional.
    - Análisis DOFA: a groso modo se identifican algunas características del análisis DOFA que pueden representar este tipo de instituciones:
      Dificultades: Difusión de las ayudas y/o gestión que puede realizar la institución en especial para el sector productivo tipo PYME[2]. Recurso humano insuficiente en todas las áreas para cumplir a cabalidad objetivos y metas de la institución.

[1] En adelante se hará uso de la abreviatura MI para indicar Mensajería Instantánea
[2] PYME: acrónimo de Pequeña Y Mediana Empresa

Oportunidades: Favorecer la investigación, el desarrollo de la ciencia y la tecnología a través de mecanismo de apoyo financiero, apoyo de estudios en el exterior, publicaciones, gestión de proyectos en desarrollo, entre otros.

Fortalezas: Relación estrecha con investigadores de universidades, centros de investigación y centros de desarrollo tecnológico. Convenios realizados con otras instituciones del estado, organismos nacionales e internacionales con el objeto de apalancar recursos para financiación.

Amenazas: Mala imagen y/o desacreditación de la gestión realizada. Finalización sin oportunidad de continuidad de convenios en pro de la búsqueda de recursos para financiación.

- Partes internas relacionadas: Todo el recurso humano de planta y de contratación de la entidad.

  Partes externas relacionadas: Estado, Universidades nacionales e internacionales, empresas sector productivo, manufacturero y de servicios tipo PYME y grande empresa, centros de desarrollo tecnológico, cualquier entidad interesada en el desarrollo de investigación, innovación, ciencia y tecnología.
- Elementos de apoyo y obstáculos para enfrentar un riesgo.

Tabla 6. Elementos de apoyo y obstáculos

Elementos de Apoyo	**Obstáculos**
Recurso humano encargado competente	Falta de información en todos los estamentos de la entidad
Respuesta inmediata para mitigar el problema	Poca disponibilidad de recursos para implementar técnicas de seguridad informática
Buenas relaciones con partes externas a la entidad.	Sentido de pertenencia escaso
	Ignorancia de los amenazas
	Rápida difusión de amenazas

	tecnológicas asociadas a la infraestructura de red
	Falta de comunicación con la alta dirección
	Priorización de necesidades y recursos (los aportes para nueva tecnología no son una prioridad)
	Equipos y sistemas que no poseen tecnología de punta.

- **Marco Organizacional**: En este paso se han estudiado a profundidad los objetivos, metas y prioridades de la institución, de igual forma su misión, visión, políticas y estrategias para le ejecución de sus actividades.
- **Marco de Gestión**: El proyecto o actividad que se va a realizar es la utilización de Mensajería Instantánea a través de redes P2P.
  - Fuentes de riesgo y áreas de impacto asociadas a esta actividad**:** El siguiente cuadro (Tabla 7) en lista las áreas de impactos y las fuentes de riesgo detectadas en el estudio para este caso.

Tabla 7. Fuentes de riesgo y áreas de impacto

FUENTES DE RIEGOS	ÁREAS DE IMPACTO
Utilización no adecuada de los recursos informáticos que puede generar pagos legales y/o responsabilidades comerciales.	Activos informáticos (hardware, software y datos) y recursos humano
Comportamiento humano	Ingresos y derechos
Nuevas tecnologías	Costos
Administración de las Actividades de gestión y control sin el correcto seguimiento.	Comportamiento Organizacional

	Programación y realización de actividades
	Intangibles (Imagen, reputación, buen nombre)
	Desempeño

Con el propósito de relacionar las fuentes de riesgo con las áreas que pueden ser impactadas por la utilización de la MI se presenta la tabla 8

Tabla 8. Relación fuentes de riesgos y áreas de impacto

FUENTES DE RIESGOS	**ÁREAS DE IMPACTO**						
	Activos y RH	**Ingresos**	**Costos**	**Comportamiento organizacional**	**Programación de actividades**	**Intangibles**	**Desempeño**
Utilización no adecuada de los recursos informáticos que puede generar pagos legales y/o responsabilidades comerciales.	X	X	X			X	
Comportamiento humano	X	X	X	X	X	X	X
Nuevas tecnologías	X		X	X	X	X	X
Administración de las Actividades de gestión y control sin el correcto seguimiento.	X	X	X	X	X	X	X

- Alcance de la gestión de riesgos para MI utilizando redes P2P: El objetivo de este análisis es determinar los riesgos en que puede incurrir la entidad si utiliza redes P2P para ésta aplicación. Además se tiene presente que las necesidades de comunicación con sectores aislados en tiempo real, incrementan de acuerdo a las necesidades de la entidad, por esta razón es fundamental evaluar, a la par, los mecanismos para mitigar los riegos encontrados.
- Los responsables directos del proceso de gestión de esta aplicación será el grupo de informática, específicamente; sin embargo, en caso de existir, será el personal dedicado a velar por la seguridad de la información pues, sobre ellos recaen entre otras las siguientes funciones: definir políticas sobre el uso adecuado de los recursos, implementar los mecanismos de la seguridad de la información y llevar a cabo el seguimiento de la aplicación y del cumplimiento de las políticas.
- Otros estudios: para este análisis por su carácter de ejemplificación se omitirá el estudio de otros análisis similares.

- **Criterios de evaluación**: Debido a las características, objetivos y actividades de la entidad los criterios relacionados con las áreas de impacto que se tendrán en cuenta para realizar la evaluación del riesgo son:
  - Financieros/Área de Ingresos y Costos
  - Técnicos/Área de Activos y Desempeño
  - Operacionales/Área de Recurso Humano, Programación de actividades, Comportamiento organizacional y Desempeño)
  - Legales/Área de Costos e Intangibles
  - Percepciones internas y externas /Área de Intangibles y Desempeño
- **Actividades Estratégicas**: De acuerdo a la actividad desarrollada por la entidad, a continuación se lista una serie de elementos desglosados que la conforman:
  - Gestionar y realizar seguimiento a los proyectos financiados por la entidad.

- Gestionar y realizar seguimiento de las propuestas que pueden ser elegibles para apoyo financiero.
- Internacionalización de la entidad con actividades de apoyo y financiación para investigaciones académicas e industriales, así como para participación en eventos fuera del país.
- Registro, evaluación y reconocimiento de grupos de investigación, centros de desarrollo tecnológico, publicaciones y jóvenes investigadores.
- Buscar espacios que permitan la concertación de convenios con el estado, organismos privados nacionales y/o internacionales con el propósito de apalancar recursos de financiación.
- Apoyar y asesorar el esclarecimiento de las líneas de financiación y las modalidades de apoyo en las diferentes áreas.
- Difusión de las diferentes modalidades de financiación existentes para proyectos de investigación.

El siguiente cuadro es el resumen del análisis sobre las actividades estratégicas de la organización en relación con las áreas de impacto que pueden ser afectadas si se utiliza redes P2P (Tabla 9):

Tabla 9. Listado de Actividades estratégicas/Áreas de impacto

Actividades estratégicas	**Área de Impacto**
Gestionar y realizar seguimiento a los proyectos financiados por la entidad.	**Áreas de impacto: Desempeño, Comportamiento Organizacional y Programación de actividades** Desarrollo de actividades diferentes a las programadas y que no corresponden a tareas de la entidad No cumplimiento de actividades, horarios y cronogramas debido a imprevistos como: afectación de equipos, video conferencias, transferencia de voz y video, entre otros. **Ingresos, Costos e Intangibles** Fuga de información reservada que ponga en riesgo la confiabilidad y

	transparencia del proceso de gestión de proyectos. Afectación de la buena imagen de la entidad si se presentan demandas causadas por algún problema de confidencialidad relacionado con derechos de autor y patentes, originados ya sea por entes externos o internos. **Activos, Costos, Programación de actividades y Desempeño** Afectación del buen funcionamiento de los equipos debido a la infección de virus y similares.
Gestionar y realizar seguimiento de las propuestas que pueden ser elegibles para apoyo financiero.	**Desempeño, Comportamiento Organizacional y Programación de actividades** Desarrollo de actividades diferentes a las programadas y que no corresponden a tareas de la entidad No cumplimiento de actividades, horarios y cronogramas debido a imprevistos como afectación de equipos, video conferencias, transferencia de voz y video, entre otros. **Ingresos, RH, Costos e Intangibles** Fuga de información privada de los proponentes que ponga en riesgo la confiabilidad en la entidad y sea causante de demandas por derechos de autor y demás. **Activos, Costos, Programación de actividades y Desempeño** Afectación del buen funcionamiento de los equipos debido a la infección de virus y similares.
Internacionalización de la entidad con actividades de apoyo y financiación para investigaciones académicas e industriales, así como para participación en eventos fuera del país.	**Ingresos, Costos e Intangibles** Afectación del buen nombre a nivel internacional (y/o nacional) si no está a disposición la tecnología adecuada para la realización de video conferencias o el uso compartido de archivos.

	Fuga de información de los proyectos y propuestas que ponga en riesgo la confiabilidad y transparencia del proceso. Afectación de la buena imagen de la entidad si se presentan demandas causadas por algún problema de confidencialidad por parte de funcionarios o pares evaluadores. **Desempeño, Comportamiento Organizacional y Programación de actividades** No cumplimiento de actividades, horarios y cronogramas debido a imprevistos como afectación de equipos, video conferencias, transferencia de voz y video, entre otros. **Activos, Costos, Programación de actividades y Desempeño** Afectación del buen funcionamiento de los equipos debido a la infección de virus y similares.
Registro, evaluación y reconocimiento de grupos de investigación, centros de desarrollo tecnológico, publicaciones y jóvenes investigadores.	**Desempeño, Comportamiento Organizacional y Programación de actividades** Desarrollo de actividades diferentes a las programadas y que no corresponden a tareas de la entidad No cumplimiento de actividades, horarios y cronogramas debido a imprevistos como afectación de equipos, video conferencias, transferencia de voz y video, entre otros. **Ingresos, Costos e Intangibles** Fuga de información perteneciente a grupos y centros de investigación que ponga en riesgo la privacidad, confiabilidad y transparencia de los procesos. **Activos, Costos, Programación de actividades y Desempeño** Afectación del buen funcionamiento de los equipos debido a la infección

	de virus y similares.
Buscar espacios que permitan la concertación de convenios con el estado, organismos privados nacionales y/o internacionales con el propósito de apalancar recursos de financiación.	**Desempeño, Comportamiento Organizacional y Programación de actividades** No cumplimiento de actividades, horarios y cronogramas debido a imprevistos como afectación de equipos, video conferencias, transferencia de voz y video, entre otros. **Ingresos, Costos e Intangibles** Fuga de información reservada que debe ser conocimiento solo de las partes interesadas mientras dura el proceso de concertación. Afectación del buen nombre a nivel internacional (y/o nacional) si está a disposición la tecnología adecuada para la realización de video conferencias o el uso compartido de archivos. **Activos, Costos, Programación de actividades y Desempeño** Afectación del buen funcionamiento de los equipos debido a la infección de virus y similares.
Apoyar y asesorar el esclarecimiento de las líneas de financiación y las modalidades de apoyo en las diferentes áreas.	**Costos e Intangibles** Fuga de información confidencial para las organizaciones como propuestas o proyectos de innovación y desarrollo tecnológico. Afectación de la buena imagen de la entidad si se presentan demandas causadas por algún problema de confidencialidad, derechos de autor y privacidad. Afectación del buen nombre a nivel internacional (y/o nacional) si está a disposición la tecnología adecuada para la realización de video conferencias o el uso compartido de archivos. **Desempeño, Comportamiento Organizacional y Programación de**

	actividades Desarrollo de actividades diferentes a las programadas y que no corresponden a tareas de la entidad No cumplimiento de actividades, horarios y cronogramas debido a imprevistos como afectación de equipos, video conferencias, transferencia de voz y video, entre otros. **Activos, Costos, Programación de actividades y Desempeño** Afectación del buen funcionamiento de los equipos debido a la infección de virus y similares.
Difusión de las diferentes modalidades de financiación existentes para proyectos de investigación.	**Desempeño, Comportamiento Organizacional y Programación de actividades** Desarrollo de actividades diferentes a las programadas y que no corresponden a tareas de la entidad No cumplimiento de actividades, horarios y cronogramas debido a imprevistos como afectación de equipos, video conferencias, transferencia de voz y video, entre otros. **Activos, Costos, Programación de actividades y Desempeño** Afectación del buen funcionamiento de los equipos debido a la infección de virus y similares. **Costos e Intangibles** Afectación del buen nombre a nivel internacional (y/o nacional) si está a disposición la tecnología adecuada para la realización de video conferencias o el uso compartido de archivos.

3.1.2 Paso 2. Identificación del riesgo

Siguiendo la guía de gestión de riesgos, se responderán los siguientes interrogantes con el objeto de encontrar las vulnerabilidades, las posibles amenazas y el listado de riegos que implica la utilización de MI a través de redes P2P:

- **¿Que vulnerabilidades se encuentran en la organización?** La vulnerabilidad mas relevante que se obtiene de este estudio es precisamente el uso de Mensajería Instantánea mediante redes P2P, de no utilizarse este medio de comunicación no habría el porqué de esta ejemplificación, debe entenderse además que las vulnerabilidades son propias y de originan al interior de la organización. Otras vulnerabilidades que pueden presentarse tienen que ver con la infraestructura y los equipos de red por ejemplo; sin embargo, este punto ya se aborda en el concepto técnico de la MI.
- **¿Cómo y por qué puede suceder?** Las amenazas asociadas a la vulnerabilidad descrita en la sección anterior, que pueden ser explotadas y convertirse en un riesgo son:

Tabla 10. Relación vulnerabilidades y amenazas

Vulnerabilidades	**Amenazas**
Uso de MI mediante redes P2P	**Asociadas a la intranet** 1. Fallas en los protocolos que se encargan de la conexión entre los diferentes terminales. 2. Tecnología atrasada que no permite cumplir a cabalidad el objetivo de la aplicación y/o una rápida contingencia del evento riesgoso. 3. Disponibilidad deficiente de recursos técnicos para atender la demanda generada. **Asociadas a Incidencias Legales** 1. Violaciones legales en cuanto a confidencialidad y privacidad de documentos causados por personal

	asociado a la entidad ó a la organización. **Asociadas a los problemas tecnológicos sobre la seguridad de la información** 1. Ataques con códigos maliciosos. 2. Problemas en los mecanismos de seguridad de la información a nivel de hardware y/o software. 3. Fallas en los equipos de comunicación debidas a incrementos en los canales de comunicación, tasas de transferencia descontroladas, entre otros. 4. CH encaminado al no cumplimiento de las funciones y obligaciones establecidas.

- **Ayudas, herramientas y/o técnicas**: Mediante la utilización de algunas técnicas y herramientas de análisis se determinaron los riesgos relacionados con las amenazas encontradas por la implementación de aplicaciones sobre redes P2P. La tabla 10 se tomó como base y se obtuvo el siguiente cuadro (Tabla 11)

Tabla 11. Cuadro resumen amenazas y riesgos asociados al uso de MI.

AMENAZAS	RIESGOS	
Asociadas a la intranet	Problemas de confidencialidad	
	Falta de autenticidad en los datos compartidos	
	Baja disponibilidad	
	Autenticación, usuarios no autorizados	
	Trazabilidad nula	
Asociadas a Incidencias Legales	Responsabilidades corporativas no reconocidas	
	Violación de derechos de autor y patentes	
	Multas y pagos judiciales	
Asociadas a los problemas tecnológicos sobre la seguridad de la información	Código Malicioso	**Virus:** • Ataques DDoS • Desinstalación de Antivirus y Firewall • Troyanos/keylogger

		• Corrupción o borrado de archivos
		Malware(adware/spyware)
		Errores en el SW
		Fuga de Información sensible
	Riesgos asociados a la disponibilidad de recursos.	Incremento en el uso de canales de comunicación
		Perturbaciones en los patrones normales de uso
		Tasas de Tx superiores al umbral ó invertidas
	Riesgos asociados a factores humanos	Recursos y conocimiento del usuario final

3.1.3 Paso 3. Análisis del Riesgo

- **Mecanismos de control**: Se refiere a la administración, los sistemas técnicos y procedimientos que buscan controlar el riego, se evalúa sus fortalezas y debilidades. Para este paso es posible apoyarse en las técnicas y herramientas descritas en el paso 2 y/o métodos que involucran inspecciones y técnicas de auto-evaluación. Para realizar este punto es necesario tener un mayor conocimiento de los mecanismos que utiliza la entidad, razón por la cual, supondremos que la organización no dispone de ningún control en el momento y que este análisis será utilizado en una etapa posterior del ciclo del SGSI para tomar decisiones sobre la adquisición de los mecanismos de seguridad de la información apropiados para mitigar los riesgos hallados durante esta evaluación.
- **Consecuencias y probabilidad**: Debe evaluarse la magnitud de las consecuencias asociadas a un evento y combinarlas con la probabilidad de ocurrencia para determinar el nivel de riesgo, esto mediante análisis y cálculos estadísticos, también es posible basarse en datos del pasado para ello y con el propósito de no realizar sesgos subjetivos se recomienda tener en cuenta las siguientes fuentes de información:
    - Registro de otros estudios
    - Experiencia pertinente

- Prácticas y experiencias industriales
- Literatura publicada y reconocida (Internet)
- Investigaciones de mercado
- Modelos económicos
- Minería de datos
- Juicios de expertos

Como ejemplo de técnicas para realizar estos análisis se tiene:

- Realizar entrevistas a expertos en el área de interés
- Organizar grupos de expertos interdisciplinarios
- Evaluaciones individuales realizadas a los integrantes del área de gestión evaluada.
- Uso de árboles de error y árboles de eventos.

Para efectos prácticos del presente documento no se desarrolla este punto; sin embargo, esto no implica que no se deba realizar la asociación entre las consecuencias de un evento y su probabilidad de ocurrencia con el fin de obtener el nivel de riesgo, (parte fundamental en el estudio) éste tema se ahondará en la siguiente sección: “Tipos de análisis”.

- **Tipos de análisis**: Existen 3 tipos de análisis del riesgo, que se diferencian por su grado de exactitud y esto va a depender de la información y disponibilidad de los datos.

  En primera instancia y por la exactitud de los datos presentes, se realizará el análisis cualitativo como ejemplo.

  - Análisis cualitativo: 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.

    Se tomó como base las tablas 1 y 2 vistas en el capitulo 2 para describir la matriz de nivel de riesgos.

    Para el caso de estudio, no se modifican las descripciones ni los niveles sugeridos.

Tabla 12. Matriz de nivel

PROBABILIDAD	IMPACTOS			
	Bajo	Medio	Medio-Alto	Alto
a) Improbable	L	L	L	L
b) Posible	L	M	M	H
c) Probable	L	M	E	E
d) Casi cierto	L	H	E	E

L = Nivel inferior (*Low*), gestionar riesgo mediante rutina

M = Nivel Moderado (*Midle*), especifica la responsabilidad de la dirección.

H = Nivel Alto (*High*) necesita la atención del director

E = Nivel Extremo (*Extrem*), Requiere acción inmediata

De acuerdo a la tabla 15, la siguiente es la conclusión del análisis de riesgos aplicada a los riesgos asociados a redes P2P encontrados para esta aplicación, tabla 13:

Tabla 13. Matriz nivel de riesgos

RIESGOS	PROBABILIDAD	IMPACTOS	NIVEL DE RIESGOS
Recursos y conocimiento del usuario final	Casi cierto	Alto	E
Responsabilidades corporativas no reconocidas	Probable	Medio-Alto	E
Multas y pagos judiciales	Probable	Medio-Alto	E
Autenticación, usuarios no autorizados	Probable	Medio-Alto	E
Falta de autenticidad en los datos compartidos	Probable	Medio-Alto	E
Problemas de confidencialidad	Posible	Alto	H
Fuga de información sensible	Posible	Alto	H
Tasas de Tx descontroladas ó invertidas	Casi cierto	Medio	H
Fallas en los sistema de seguridad informática	Posible	Alto	H

Troyanos/Keylogger	Posible	Alto	H
Corrupción o borrado de archivos	Posible	Alto	H
Incremento uso de canales	Probable	Medio	M
Perturbaciones en los patrones normales de uso	Probable	Medio	M
Desintalación de Antivirus y firewall	Posible	Medio-Alto	M
Baja disponibilidad	Probable	Medio	M
Fallas en los protocolos de conexión	Posible	Medio-Alto	M
Trazabilidad nula	Improbable	Medio	L
Ataques DDoS	Posible	Bajo	L
Malware	Posible	Bajo	L

De ésta primera matriz es posible descartar algunos riesgos que no representan peligro como tal para la entidad en cuestión y por lo tanto pueden descartarse.

Con el propósito de priorizar los riesgos, debido a que muchos de ellos tienen el mismo nivel cualitativo de importancia, se profundiza en el análisis semi-cuantitativo, de acuerdo a la información que se tiene.

- Análisis semi-cuantitativo: Para determinar numéricamente los niveles resultantes de la matriz (tabla 13) se hace referencia a los siguientes términos que componen la “posibilidad de ocurrencia”:

  a). **Frecuencia de exposición**: Grado de existencia de una fuente de riesgo.

  b). **Probabilidad:** Grado de materialización y sus consecuencias de una fuente de riesgo.

  Para asociar a los niveles de matriz un valor entre 0 y 1; se parte del promedio y la desviación estándar relacionados con el producto de la frecuencia de exposición y la probabilidad referidas, el resultado se observa en la tabla 14 y la matriz de nivel numérica se encuentra en la tabla 15

Tabla 14. Matriz de niveles asociado a una valor numérico

PROBABILIDAD	IMPACTOS			
	Bajo	Medio	Medio-Alto	Alto
a) Improbable	L (0,01)	L (0,04)	L (0,07)	L (0,1)
b) Posible	L (0,04)	M (0,16)	M (0,28)	H (0,4)
c) Probable	L (0,07)	M (0,28)	E (0,49)	E (0,7)
d) Casi cierto	L (0,10)	H (0,40)	E (0,70)	E (1,0)

Tabla 15. Matriz nivel de riesgos análisis semi-cuantitativo

RIESGOS	PROBABILIDAD	IMPACTOS	NIVEL DE RIESGOS
Recursos y conocimiento del usuario final	Casi cierto	Alto	E (1)
Responsabilidades corporativas no reconocidas	Probable	Medio-Alto	E (0,49)
Multas y pagos judiciales	Probable	Medio-Alto	E (0,49)
Autenticación, usuarios no autorizados	Probable	Medio-Alto	E (0,49)
Falta de autenticidad en los datos compartidos	Probable	Medio-Alto	E (0,49)
Problemas de confidencialidad	Posible	Alto	H (0,4)
Fuga de información sensible	Posible	Alto	H (0,4)
Tasas de Tx descontroladas ó invertidas	Casi cierto	Medio	H (0,4)
Fallas en los sistema de seguridad informática	Posible	Alto	H (0,4)
Troyanos/Keylogger	Posible	Alto	H (0,4)
Corrupción o borrado de archivos	Posible	Alto	H (0,4)
Incremento uso de canales	Probable	Medio	M (0,28)
Perturbaciones en los patrones normales de uso	Probable	Medio	M (0,28)
Desintalación de Antivirus y firewall	Posible	Medio-Alto	M (0,28)
Baja disponibilidad	Probable	Medio	M (0,28)
Fallas en los protocolos de conexión	Posible	Medio-Alto	M (0,28)

Trazabilidad nula	Improbable	Medio	L (0,04)
Ataques DDoS	Posible	Bajo	L (0,04)
Malware	Posible	Bajo	L (0,04)

- Análisis cuantitativo: Este análisis aunque más preciso que los anteriores depende en gran medida de datos exactos tomados de la entidad y por ende para ésta ejemplificación no se lleva a cabo.

3.1.4 Paso 4. Evaluación del Riesgo

Una vez obtenida la tabla de priorización (tabla 15) el paso 4 tiene el propósito de ofrecerle a la alta dirección la discrecionalidad para determinar que acciones deben llevarse a cabo; sin embargo, estas decisiones deben basarse en los objetivos, metas y actividades de la organización.

Como se observa en la tabla 15 tres riesgos resultaron categorizados como “bajo riesgo” por lo cual la organización puede tratarlos con el mínimo esfuerzo; no obstante, es tarea del grupo responsable del análisis de gestión, monitorizar y supervisar su permanencia en está categoría.

El numeral (3.1.5) sugiere que hacer con los 16 riesgos restantes, que pertenecen a los grupos “medio riesgo”, “alto riesgo” y “riego extremo”.

3.1.5 Paso 5. Tratamiento del Riesgo

De acuerdo a las opciones de tratamiento del riesgo que se presentaron en el capítulo 2, a continuación se resumen que acciones en general podrían llevarse a cabo para mitigar cada riesgo y de esta forma evaluar cual es la mejor opción ó si es necesario combinar las posibilidades:

1. Evitar el riesgo (No permitir la realización de actividades asociadas)
2. Reducir la posibilidad de ocurrencia
3. Reducir las consecuencias
4. Transferir el riesgo
5. Retener el riesgo

- **Evaluación de las opciones**: La tabla 19 define las posibilidades para tratar un riesgo, base para determinar cuales realmente se llevaran a cabo. En general resulta más conveniente combinar: la reducción de la posibilidad de un riesgo, la reducción de las consecuencias de un riego, las transferencias y la retención del riesgo residual. En otras palabras es trabajar conjuntamente el uso efectivo de contratos, financiación de riesgos y programas de reducción de riesgos; no obstante, se hace claridad que estos procedimientos están estrechamente ligados con las necesidades, las políticas, la misión, visión y objetivos de la entidad y por consiguiente estás recomendaciones son sólo pautas para un estudio mas detallado, ya sea que se aborde el tipo organización del ejemplo o en general cualquier entidad corporativa.

Tabla 16. Acciones de tratamiento evaluadas y definidas

RIESGOS	**OPCIONES DE TRATAMIENTO**				
	1	**2**	**3**	**4**	**5**
Recursos y conocimiento del usuario final		X	X		X
Responsabilidades corporativas no reconocidas		X	X	X	
Multas y pagos judiciales		X	X	X	
Autenticación, usuarios no autorizados		X	X	X	
Falta de autenticidad en los datos compartidos		X	X		X
Problemas de confidencialidad		X	X		X
Fuga de información sensible		X	X		X
Tasas de Tx descontroladas ó invertidas		X	X	X	
Fallas en los sistema de seguridad informática		X	X	X	X
Troyanos/Keylogger		X	X		X
Corrupción o borrado de archivos		X	X		X
Incremento uso de canales		X	X		X
Perturbaciones en los patrones normales de uso		X	X		X
Desintalación de Antivirus y firewall		X	X		X
Baja disponibilidad		X	X		X

Fallas en los protocolos de conexión			X	X	X

La tabla 16 es una generalidad resumida de las acciones a tomar, los siguientes párrafos describen las acciones y controles para cada riesgo involucrado en aplicaciones P2P:

- A pesar de trabajar con tres o mas combinaciones de tratamiento del riesgo, las acciones que se llevan a cabo varían para cada uno; sin embargo, existen asociadas para todos las amenazas las siguientes actividades:

  1. Auditoria, supervisión, monitoreo y mecanismos de control y verificación del cumplimiento de las políticas de SI
  2. Instalación de software de gestión de redes que permita la designación de perfiles, usuarios y contraseñas.
  3. Capacitar a los funcionarios de todos los estamentos, sobre las amenazas y perjuicios que puede traer tanto para la entidad como para si, el uso de ciertas aplicaciones ó servicios de red, de igual forma fomentar la adecuada utilización de los servicios, mejorando malos hábitos ya adquiridos.
  4. Crear programas desde la gerencia de recurso humano que generen sentido de pertenencia y responsabilidad por parte de los funcionarios

- Ahora bien para facilitar la percepción de las actividades que pueden implicar varios riesgos, éstos fueron agrupados en 4 categorías y utilizan como plan de tratamiento la combinación de 3 ó 4 opciones: la reducción de la vulnerabilidad y la probabilidad de ocurrencia de un riesgo, la reducción de las consecuencias, las transferencias y la retención del riesgo residual, los siguientes son los grupos resultantes:

  Control en la asignación de usuarios, permisos y contraseñas: Dentro de ésta categorías se encuentran los siguientes riesgos:

- Problemas de Confidencialidad
- Recursos y conocimiento del usuario final
- Autenticación, usuarios no autorizados

Específicamente las actividades que se deben llevar a cabo son las siguientes:

Acciones para disminuir la posibilidad de ocurrencia:

1. Condiciones contractuales
2. Aseguramiento de calidad, gestión y normalización
3. Políticas de utilización de red
4. Adjudicación por perfil del cargo de equipos y hardware para comunicaciones

Así mismo estás son las acciones que deben seguirse para disminuir las consecuencias:

1. Arreglos y condiciones contractuales
2. Planes de recuperación de desastres informáticos como copias periódicas de seguridad de toda la información corporativa tanto en servidores como en equipos de uso personal.
3. Barreras estructurales y de ingeniería como utilización de identidades o perfiles de usuario
4. Políticas de control y cumplimiento de las cláusulas establecidas
5. Separación y/o reubicación de actividades y/o recursos de acuerdo a los resultados y estadísticas del cumplimiento de políticas de utilización de red implementadas.
6. A partir de resultados confiables y objetivos impartir sanciones ó remuneraciones según sea el caso y en todos los estamentos que servirán como ejemplo para toda la entidad.

Control de contenidos, fuga de información: En este grupo se encuentran:

- Fallas en los protocolos de conexión

- Fuga de información sensible
- Problemas de Confidencialidad
- Recursos y conocimiento del usuario final
- Responsabilidades corporativas no reconocidas y Multas y pagos judiciales

Se hace evidente por la inclusión de algunos riesgos del grupo anterior, que las actividades allí descritas también son aplicables a esta categoría.

Acciones para disminuir la probabilidad de ocurrencia:

1. Revisión formal de requerimientos, especificaciones, diseño, ingeniería y operaciones
2. Pruebas de laboratorio para la implementación de nuevas tecnologías o equipos de comunicación, disposiciones organizacionales y técnicas de control

Actividades para minimizar las consecuencias:

1. Reducción de exposición a fuentes de riesgos tecnológicos o por causa del recurso humano
2. Planeación de control de fraudes que cubra entes internos y externos a la organización
3. Establecimiento de buenas relaciones publicas, legales y sociales con todos los organismos tanto privados como estatales relacionados con la entidad.
4. Planes de contingencia por sobre costos en el recurso humano y llegado el caso por multas o pagos legales.

Control del ancho de banda: Los riesgos asociados a este grupo son:

- Tasas de Tx descontroladas ó invertidas
- Incremento uso de canales
- Perturbaciones en los patrones normales de uso
- Baja disponibilidad

Actividades enfocadas a disminuir la probabilidad de ocurrencia de un evento riesgoso.

1. Revisión formal de requerimientos, especificaciones, diseño, ingeniería y operaciones
2. Mantenimiento preventivo de la infraestructura de red
3. Políticas de utilización de red
4. Adjudicación por perfil del cargo de equipos y hardware para comunicaciones.
5. Pruebas de laboratorio para la implementación de nuevas tecnologías o equipos de comunicación, disposiciones organizacionales y técnicas de control
6. Pruebas de funcionamiento para casos extremos de tráfico y utilización de los servicios de red

Actividades para restringir las consecuencias

1. Barreras estructurales y de ingeniería para hardware y software como configuración de dispositivos y asignación de perfiles de usuario solo por el administrador de red
2. Separación y/o reubicación de actividades y/o recursos dependiendo de los requerimientos y necesidades de utilización de infraestructura.
3. A partir de resultados confiables y objetivos impartir sanciones ó remuneraciones según sea el caso y en todos los estamentos que servirán como ejemplo para toda la entidad.

Instalación de anti-x: antivirus, antispam, antispyware y demás: finalmente en este grupo se encuentran los siguientes riesgos:

- Troyanos/Keylogger,
- Desinstalación de Antivirus y firewall
- Corrupción o borrado de archivos
- Fallas en los sistemas de seguridad informática
- Falta de autenticidad en los datos compartidos

Actividades encaminadas a disminuir la probabilidad de ocurrencia:

1. Revisión formal de requerimientos, especificaciones, diseño, ingeniería y operaciones
2. Mantenimiento preventivo y pruebas de funcionamiento de los sistemas de seguridad de la información a partir de supuestos ataques informáticos realizados por el grupo de soporte.
3. Pruebas de laboratorio para la evaluación e implementación de nuevas tecnologías tanto hardware como software, disposiciones organizacionales y técnicas de control

Actividades para reducir el impacto ocasionado por las consecuencias

1. Planes de contingencia a nivel de infraestructura de red
2. Planes de recuperación de desastres informáticos como copias periódicas de seguridad de toda la información corporativa tanto en servidores como en equipos de uso personal.
3. Reducción de exposición a fuentes de riesgos tecnológicos o por causa del recurso humano
4. Separación y/o reubicación de actividades y/o recursos para equipos personales, switches, routers y demás elementos de red garantizando la disponibilidad de los recursos y servicios de comunicación.

Transferencia y riesgo residual: Con respecto al tratamiento que implica transferencia del riesgo, específicamente lo que se busca es involucrar otras entidades u organizaciones que compartan parcial o totalmente la responsabilidad de asumir un riesgo; por lo cual se implementan mecanismos como: contratos, pólizas de cumplimiento, acuerdos de seguros, alianzas estratégicas, entre otros. A pesar de la implementación de estas y otras actividades propias de la entidad, es posible que exista un riesgo residual de bajo impacto, sobre éste aspecto es necesario continuar haciendo un seguimiento y control

exhaustivo del riesgo con el fin de garantizar su estado de aceptabilidad.

Una observación a resaltar es que muchas de las actividades mencionadas se aplican para dos o más riesgos, esto no causa ningún tipo de inconvenientes por el contrario puede disminuir los costos que conlleva la implementación de los planes de tratamiento.

- **Planes de tratamiento**: ya se han determinado que acciones y controles se van a seguir para mitigar los riesgos, ahora es necesario documentar como se van a implementar estas soluciones, por medio de la determinación de los siguientes puntos, pero como ya se ha mencionado esta profundización se deja para cada entidad en particular.
    - Identificar responsables
    - Realizar cronogramas
    - Establecer presupuestos
    - Evaluar resultados esperados y medidas de desempeño
    - Realizar procesos de revisión por implementar.
- **Implementación de planes de tratamiento**: Terminado el punto anterior, la alta dirección debe garantizar la buena consecución de este proceso, mediante la implementación de algún seguimiento de gestión en cada área donde sea necesario llevar a cabo un plan de tratamiento.

3.1.6 Paso 6. Monitoreo y revisión

El grupo responsable de la gestión de riesgos ó sus delegados deben estar al tanto de todo el procedimiento, llevando a cabo un acompañamiento, monitoreo, revisión y control de las tareas del sistema de gestión desarrollado para la entidad, con el objeto de garantizar el éxito, la pertinencia y la efectividad del tratamiento.

3.1.7 Paso 7. Comunicación y Consulta

Este paso se desarrolla a lo largo de todo el proceso. Tanto la dirección como el grupo responsable de la gestión de riesgos deben propender por una buena comunicación y difusión de los planes de tratamiento y contingencia. Cabe resaltar que el trabajo de gestión involucra a todos los funcionarios de la entidad, en la medida en que se mejoren las costumbres, las percepciones y la utilización de la red P2P, esto con el fin de garantizar y asegurar el éxito del proceso. Es necesario identificar, documentar y entender estas percepciones y todo el proceso en si desarrollado para futuros planes y análisis de riesgos relacionados.

En el anexo C, se encuentran las fichas de registro correspondientes a la gestión de riesgos implementada.

Los resultados obtenidos de la ejemplificación de la metodología para aplicaciones P2P en un ambiente de investigación, demuestran que éste tipo de aplicaciones a través de conexiones directas puede tener viabilidad siempre y cuando se implementen los debidos sistemas de seguridad de la información y planes de tratamiento que mitiguen los riesgos encontrados y garanticen:

- Confiabilidad
- Integridad
- Disponibilidad

Se resalta una vez más que este análisis de gestión para aplicaciones P2P se realizo en base a una entidad ficticia, con el objetivo de generar pautas estructurales para futuros estudios en organizaciones reales, por ende estos resultados pueden variar dependiendo de la naturaleza de la entidad.

3.2 SOLUCIONES TECNOLÓGICAS PARA MITIGAR LAS AMENAZAS GENERADAS POR EL USO DE APLICACIONES P2P

Esta sección tiene por objeto presentar algunas soluciones tecnológicas que puedan ser implementadas por cualquier tipo de organización, con el fin de mitigar las amenazas e impactos generados por el uso de aplicaciones P2P.

Del análisis previamente realizado y en consecuencia con los riesgos y amenazas encontrados al hacer uso de aplicaciones sobre redes p2p se concluye que el sistema de seguridad, software o *appliance*[1] a implementar debe enfatizar en:

- Control del ancho de banda
- Control en la asignación de usuarios, permisos y contraseñas
- Control de contenidos, fuga de información
- Instalación de anti-x: antivirus, *antispam*, *antispyware* y demás

3.2.1 Control de ancho de banda

Las características del ancho de banda se modifican dando como resultado un *upstream* y *downstream* con demandas similares, normalmente el ancho de banda de subida se caracteriza por tener apariencia de ráfagas, se destacan periodos cortos de tiempo en donde el usuario envía datos.

Con el uso de aplicaciones P2P como: transferencia de voz y video y *File sharing*[2] (requisito para descargar archivos en muchas de las aplicaciones comerciales p2p) las tasas de transferencia se afectan, ya sea porque se invierten o porque se saturan, razón por la cual el ancho de banda total con que dispone una entidad debe ajustarse al envío y recepción de datos en forma constante, se busca entonces con la implementación de controles para ancho de banda la no saturación en ninguno de los dos sentidos y si es el caso restringir grandes demandas tanto para subir como para descargar archivos, en pro de mantener tanto la calidad como la disponibilidad de los recursos y servicios de red.

Así mismo otra de las grandes necesidades para una entidad que haga uso de aplicaciones p2p es el control y restricción personalizada del ancho de banda;

[1] Appliance: Se refiere a un equipo hardware que instala herramientas de seguridad, y posee un sistema operativo especial desarrollado por proveedores de seguridad de la información.

[2] File sharing: Uso compartido de archivos en red

es decir, en ocasiones se hace pertinente implementar además de permisos, restricciones a diferentes usuarios o áreas de trabajo sobre el uso del ancho de banda con el propósito de no permitir el aprovechamiento ó inadecuada utilización del ancho de banda para actividades no laborales. De acuerdo a varias estadísticas encontradas[1] al menos un 80% de los empleados utilizan inadecuadamente los recursos de red y al menos un tercio del tiempo laboral es empleado en otras actividades.

3.2.2 Control en la asignación de usuarios, permisos y contraseñas

Es necesario por parte del administrador de red un estricto control sobre los permisos y la asignación de usuarios así como de contraseñas que realiza, ya sea de tipo personalizado ó por grupos de trabajo.

A nivel de Internet y redes P2P se pueden encontrar infinidad de aplicaciones que hacen uso de estas redes; ya se han mencionado las ventajas y amenazas que éste uso conlleva, al igual que la viabilidad de la implementación de dichas aplicaciones siempre y cuando se prevean mecanismos de seguridad que sumado a una correcta administración y gestión de red, mitiguen los riesgos y consecuencias generados.

Existen programas y dispositivos en hardware comerciales ó que pueden ser desarrollados por la misma organización que ejercen control de forma personalizada o por grupos de trabajo, no solo sobre el ancho de banda sino sobre la ejecución de aplicaciones, cómo, cuándo y para qué utilizarlas, descarga ó subida de archivos específicos, bloqueo de archivos que contengan frases o palabras determinadas, bloqueo de puertos, entre otros, de forma que se garantice el uso de aplicaciones P2P sólo en busca del aprovechamiento de las ventajas que en cuando a comunicación posee p2p y que desencadena en beneficios laborales y financieros para la organización.

[1] Fuente de estadísticas: Encuesta anual realizada por el FBI y el Instituto de seguridad de la computación. El documento completo se encuentra en el link http://www.gocsi.com/

3.2.3 Control de contenidos, fuga de información

Otra importante consideración está relacionada con la confidencialidad y la seguridad de los datos que se transmiten o que almacena la organización y siendo este uno de los aspectos más discutidos con el uso de redes P2P, en el sistema de seguridad que se implemente este tema es una prioridad.

Por control de contenidos se hace referencia al control asociado a todos los datos, en la medida que estos puedan ser manipulados, transmitidos, compartidos ó eliminados tanto por usuarios propios de la organización como por terceros de forma accidental o intencionada.

Para toda organización es crucial el control sobre esta información y por ende es necesario implementar los más sofisticados sistemas de seguridad de la información que garanticen su confidencialidad e integridad; debido a esto existen herramientas que tienen como finalidad desarrollar controles basados en la identificación y bloqueo de rangos de IPs que se consideren intrusivos, bloqueo de aplicaciones y *spyware*, bloqueo en el uso compartido y transferencia de determinados tipos de archivos, entre otros.

3.2.4 Instalación de anti-x: antivirus, *antispyware, antimalware* y demás

Finalmente, abordando las amenazas y riesgos tecnológicos que afronta una entidad al incurrir en el uso de aplicaciones P2P, se presenta como solución la instalación de herramientas antivirus, *antispyware, antimalware* y demás que minimizan la probabilidad de infectar equipos y poner en peligro la disponibilidad de los recursos.

El objetivo de un antivirus es detectar y eliminar programas maliciosos o virus informáticos que se ejecutan sin autorización y buscan por lo general: ejecutar recursos, consumir memoria, eliminar información, así como el robo de ésta, realizar suplantaciones con el propósito de identificar patrones de comportamiento, entre otros. Estos son a groso modo los problemas mayormente identificados y asociados al uso de redes P2P. Mediante el

adecuado desarrollo de planes de seguridad como los mencionados anteriormente se disminuye el peligro de infección; sin embargo, es necesario y primordial además la evaluación e implementación de mecanismos de seguridad que se enfoquen en la detección y eliminación de virus, gusanos, troyanos, spyware, etc, ya que no solo el uso de “contrafuegos corporativos” ó *firewall* serían suficientes para controlar éstas vulnerabilidades si se da paso al uso de aplicaciones P2P en ambientes corporativos.

En el medio se encuentran innumerables soluciones comerciales basados en software y hardware (*Appliance*), que pueden implementarse para mitigar dos o más de grupos de riesgos, para abarcar todos las fuentes de riesgo se recomienda la utilización de varias soluciones al tiempo, se destacan algunas a continuación:

- Akonix L7 Enterprise http://www.akonix.com
- Juniper Networks http://www.juniper.net/
- PeerGuardian http://peerguardian.softonic.com/
- Proyecto Blackbeard www.**surfcontrol**.com/
- Websense http://www.websense.com/global/en/
- eSafe 5 http://www.aladdin.es
- McAfee Data Loss Prevention Host http://www.mcafee.com

Se recomienda además tener presente sitios web que se encargan de alertar sobre aplicaciones o utilidades P2P que por su peligrosidad pueden poner en riesgo la integridad de los equipos y por ende de la red, entre éstos se encuentran:

- Comisión de seguridad – Asociación de internautas:
  http://seguridad.internautas.org
- Lista de aplicaciones p2p infectadas, se encuentra en los links:
  - http://www.vsantivirus.com/lista-p2p.htm
  - http://www.kernelnet.com/content/view/176/2/
  - http://www.diginota.com/trucos-y-tutoriales/lista-de-las-aplicaciones-p2p-infectadas.-2.html

4. CONCLUSIONES

La metodología de análisis de riesgos presentada en este documento cumple con los requisitos mínimos establecidos por la norma ISO 27001 para la Gestión de Sistemas de Seguridad de la Información, por lo cual, puede ser empleada por una organización que desee alinearse con este estándar.

Los resultados obtenidos de la ejemplificación de la metodología para aplicaciones P2P demuestran que éste tipo de aplicaciones puede tener viabilidad siempre y cuando se implementen los debidos sistemas de seguridad de la información y planes de tratamiento que mitiguen los riesgos encontrados y garanticen:

- Confiabilidad
- Integridad
- Disponibilidad

En general aunque la prioridad de los riesgos puede variar dependiendo del tipo de organización, el sistema implementado para mitigar las amenazas generadas por el uso de aplicaciones P2P, resume el estudio y se enfoca en:

- Control del ancho de banda
- Control en la asignación de usuarios, permisos y contraseñas
- Control de contenidos, fuga de información
- Instalación de anti-x: antivirus, *antispam*, *antispyware* y demás

El análisis de riesgos para aplicaciones p2p y en general para cualquier SI arroja que el eslabón más débil en los planes de tratamiento para mitigar riesgos es el recurso humano, por lo cual es necesario con el fin de proteger los activos informáticos resaltar en las contrataciones de personal, políticas de utilización de recursos y servicios de red, cláusulas de confidencialidad, así como los componentes de privacidad sobre los bienes de la organización, entre otros.

Existen en el mercado innumerables herramientas software y/o hardware que tienen como finalidad garantizar el buen uso y funcionamiento de la red, la disponibilidad de los recursos, la integridad y confidencialidad de la información así como el control de actividades y registros; no obstante, es responsabilidad del grupo técnico encargado realizar una correcta evaluación de éstas herramientas optando por la mas conveniente de acuerdo a las necesidades y presupuesto de entidad.

El uso de Antivirus/AntiSpyware, aunque soporta el control, bloqueo y detección de virus y/o programas maliciosos no es suficiente para garantizar la integridad de la información almacenada en los equipos cuando se incurre en el uso de utilidades sobre redes p2p.

La gestión de riesgos realizada para el uso de aplicaciones p2p se encuentra directamente relacionada con la misión, visión, objetivos, políticas y estrategias de la organización, se concluye entonces:

- Al implementar los correctos tratamientos para mitigar el riesgo sigue siendo viable la utilización de redes y conexiones P2P en ambientes corporativos, académicos ó estatales, razón por la cual la opción de tratamiento que conduce a evitar el riego no se concibe.
- La evaluación del riesgo será particular para cada entidad, pero no está de más valerse de estudios similares llevados a cabo en otros procesos.
- la metodología de gestión de riesgos permite arrojar resultados diferentes relacionados con la priorización de éstos riesgos dependiendo de las características propias de la entidad

El capitulo 3 condensa las ventajas y desventajas que conlleva el hacer uso de aplicaciones P2P al interior de una organización, independientemente de ésta; razón por la cual es posible adaptar de acuerdo a las necesidades de la entidad el estudio de gestión de riesgos para conexiones P2P, con base en el cuadro resumen de riesgos y ventajas presentado.

Dentro de los planes a seguir para mitigar los riesgos encontrados en un estudio de gestión de riesgos, se considera la relación costo/beneficio sobre los

controles necesarios para poder hacer uso eficiente de los recursos presupuestales, atacando en primera medida, los riesgos de mayor prioridad.

Una de las mejores estrategias para implementar planes de tratamiento que afronten y mitiguen correctamente los riegos encontrados en el proceso de gestión de SI, es la combinación de dos o más actividades como: reducción de consecuencias, reducción de probabilidad de ocurrencia, transferencia del riesgo y/o su retención.

El análisis cuantitativo para este caso no se llevo a cabo debido a la naturaleza de la información estudiada. El análisis cuantitativo aunque en suma exacto, debe realizarse solo con datos precisos, lo cual exige un conocimiento exhaustivo de la entidad.

5. RECOMENDACIONES

Este trabajo describe una metodología para realizar la gestión de riesgos al interior de entidades privadas y estatales que desarrollen cualquier tipo de actividad o servicio; sin embargo, la gestión de riesgos debe contemplarse como un programa de gestión de riesgos que involucre todas las dependencias, de forma que se garantice el éxito del programa.

Llevar fichas de registro como las ilustradas en el anexo B son necesarias si se quiere garantizar el éxito del análisis que termina con la implementación de los planes de tratamiento; sin embargo, las fichas presentadas son solo pautas para condensar información, cada entidad en la medida de sus necesidades debe armar las fichas con la información que el grupo responsable de la gestión considere valiosa y así asegurar el seguimiento del estudio y del tratamiento de los riesgos obtenidos.

Si bien es cierto que del estudio de gestión de riesgos, sea para el caso especifico de este trabajo o en general para cualquier tipo de actividad concluye riesgos que pueden ser aceptados y/o que luego del tratamiento implementado pueden ser retenidos, es necesario realizar constantemente un seguimiento o monitoreo de ellos con el propósito de conservar su aceptabilidad.

Para trabajos posteriores se recomienda estudiar y evaluar diferentes metodologías con el mismo propósito, la gestión de riesgos, pues aunque esta metodología se adapta a cualquier sistema de gestión, conviene contar con opciones arrojadas desde otras perspectivas. Así mismo se recomienda llevar a cabo el análisis de gestión de riesgos para otro tipo de actividades que involucren vulnerabilidad al sistema de seguridad de la información.

Se recomienda finalmente que partiendo de este trabajo, se realicen los correspondientes estudios de gestión de riesgos y en especial el análisis de riesgos en todas aquellas entidades tanto públicas como privadas que pretendan implementar en sus intranets aplicaciones que utilicen redes P2P.

6. BIBLIOGRAFÍA

[GUALDRON, 2005] Gualdrón Oscar, “Protocolos TCP/IP” Libro para la Especialización en Telecomunicaciones universidad Industrial de Santander, 2005

[TANENBAUM, 2003] Andrew S. TANENBAUM. “Redes de Computadores”, Cuarta Edición. Ed. Prentice Hall, 2003

[INTERNET 2] http://www.fce.unl.edu.ar/ecommerce/diccionario.htm
// Definición de enlaces P2P

[INTERNET 3] http://es.wikipedia.org/wiki/P2P
// Funcionamiento de un enlace P2P

[INTERNET4]www.google.com.co/search?hl=es&lr=&defl=es&q=define:P2P&sa=X&oi=glossary_definition&ct=title
// Generalidades y Tipos de un enlace P2P
[Ref 5] http://es.wikipedia.org/wiki/Historia_de_las_aplicaciones_P2P // Transferencia de archivos

[Ref 6, Artículo] “El 81% de los Responsables de IT reportan incidentes debidos a mensajeria instantanea y greynets” Autor: José Manuel Fernández se encuentra en el URL: http://iso9001-iso27001-gestion.blogspot.com/2006/12/el-81-de-los-responsables-de-it.html

[Ref 7, Artículo] “¿Reemplazará La Mensajería Instantánea Al E-Mail Como Plataforma De Comunicación Y Mensajería?” Sección 4.01 Robbin Good, Edición en español: Miguel Corsi. Se encuentra en la URL: http://www.masternewmedia.org/es/2006/04/28/reemplazara_la_mensajeria_instantanea_al.htm

[Ref 8, PDF] “SIP: El protocolo para los servicios multimedia del futuro” Autor: Miguel Ángel Manso Callejo. Tomado de: http://gauss.topografia.upm.es/~m.manso/docs/resumen-sip.pdf

[Ref 9] http://es.wikipedia.org/wiki/Peer-to-peer#Ventajas_de_las_redes_Peer-to-Peer // Otras aplicaciones P2P

[Ref 10, Presentación PowerPoint] “Gestión e intercambio de contenidos audiovisuales en un entorno P2P basado en JXTA” Autor: Rosa M. Martín. Facultad de Ingeniería de Barcelona – Universidad Politécnica de Cataluña. Se encuentra en el URL: http://www.rediris.es/jt/jt2006/archivo/16Jueves/1600-1830/B/JT006_Jueves_1600_SalaB_P2PJXTA.ppt#45

[MEDINA, 2006] Medina V. Jorge A. “Seguridad en redes de datos” Libro para la Especialización en Telecomunicaciones Universidad Industrial de Santander, Bucaramanga 2006

[Ref 11, PDF] “Aplicaciones distribuidas P2P” autores: Antonio Bonilla Egido y Javier Meler Playan. Facultad de Ingeniería de Barcelona – Universidad Politécnica de Cataluña. Se encuentra en el URL: http://studies.ac.upc.edu/FIB/CASO/seminaris/2q0304/M9.pdf

[Ref 12, Artículo] “El futuro de redes P2P en entornos corporativos” Autor: Jorge Cortell-Albert. Universidad Politécnica de Valencia. Se encuentra en el URL: http://homepage.mac.com/jorgecortell/docs/P2Pcorp.pdf

[Ref 13, Articulo] “Aumentan los ataques de virus informáticos según un primer balance de *Sophos* en 2003” Autor: *Sophos.* Se encuentra en el URL: http://esp.sophos.com/pressoffice/news/articles/2003/07/pr_20030701topten.html

[Ref 14] http://portal.acm.org/citation.cfm?id=997156 http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?arnumber=1181418 //Información referente a DDoS (Ataques Distribuidos de Negación de Servicio)

[Ref 15] “Análisis de los requerimientos tecnológicos para la implementación de servidores web seguros” //Desinstalación de antivirus y firewall URL:

http://www.monografias.com/trabajos12/rete/rete.shtml

[Ayllón & Jiménez, 2004] Nestor Ayllón & Borja Jiménez, “Seguridad en redes, Troyanos” Curso 2003-2004. URL: http://asignaturas.diatel.upm.es/seguridad/trabajos/trabajos/curso%2003%2004/troyanos.pdf

[Hernández, Orlando & Sanchez, 2003] Bello Hernandez, Ramón Orlando y Alfonso Sanchez, “Elementos teórico-prácticos útiles para conocer los virus informáticos”**.** *ACIMED*. sep.-oct. 2003, vol.11, no.5 [citado 30 Enero 2007], p.0-0. URL: http://scieloprueba.sld.cu/scielo.php?script=sci_arttext&pid=S1024-94352003000500004&lng=es&nrm=iso

[Skoudis & Zeltser, 2003] Ed Skoudis, Lenny Zeltser “Malware: Fighting Malicious Code” Publicado 2003 Prentice Hall PTR

[Orallo, Quintana & Ramírez, 2005] JH Orallo, MJR Quintana & CF Ramírez “Introducción a la minería de datos” Publicado 2005 Pearson Prentice Hall

A. ANEXO A. ASPECTOS RELEVANTES DEL ENLACE P2P[1]

A.1 Definición

P2P es un sistema de interconexión que permite que todos los usuarios estén conectados directamente; es decir no existen servidores y clientes fijos, esto debido a que todos los usuarios de la red se comportan simultáneamente como nodos que sirven de servidores y clientes; sin embargo, este modelo de comunicación se rige por una arquitectura monolítica cliente-servidor donde no hay una asignación especifica de tareas, sino una conexión en la que todos los equipos tienen las mismas características y pueden cambiar de posición en cualquier momento, de allí el termino P2P cuya traducción al español sería "par a par", pero que en realidad implica que la comunicación se realiza entre iguales y no exclusivamente entre una pareja de maquinas.

A.2 Funcionamiento

El funcionamiento del enlace P2P difiere cuando se realiza a través de Internet a cuando se realiza en aplicaciones para Intranets. En el primer caso debido a que los equipos por lo general son maquinas domesticas que no tiene una dirección IP fija sino que el proveedor de servicios de Internet (ISP[2]) les asigna una dirección IP diferente cada vez que se conectan a Internet, se realiza la conexión inicial con un servidor o servidores que poseen una dirección IP conocida y quienes se encargan de efectuar la conexión entre los clientes y entre otros servidores mediante la relación de sus direcciones IP; una vez los usuarios obtenga la información del resto de la red, llevan a cabo el intercambio de información entre ellos mismos sin la mediación de los servidores.

La conexión P2P a nivel de Internet se basa en la llamada filosofía P2P que se fundamenta en la idea de que todos los usuarios deben compartir; es decir, que las redes P2P mantiene un sistema meritocrático donde un usuario podrá

[1] Para mayor información sobre los aspectos relevantes de un enlace P2P favor revisar la bibliografía de este documento
[2] Sigla en ingles: Internet Service Provider

descargar más archivos y tener preferencias de velocidad en la medida que comparta más contenido en la red, de esta forma se garantiza la disponibilidad de documentos y por tanto el sostenimiento de la red P2P.

Para el caso 2 la diferencia radica en que los equipos de una red privada por lo general tienen una dirección IP especifica y estática, (las direcciones IP pueden ser dinámicas si la red trabaja con el protocolo DHCP[1]) de esta forma en el momento de realizar la transferencia de archivos, los usuarios conocen previamente la dirección IP necesaria para realizar la descarga o compartir archivos y/o recursos.

Es importante mencionar que este tipo de conexión de nodos se consigue siempre y cuando todos los equipos de la red estén conectados el mayor tiempo posible y por supuesto se encuentren compartiendo sus recursos.

Un ejemplo sencillo es la forma en que se comparten recursos en Windows, donde se pueden crear grupos de equipos que comparten recursos entre ellos mismos. En algunos casos es posible trabajar con contraseñas que agregan seguridad al sistema.

A.2.1 Tipos de redes

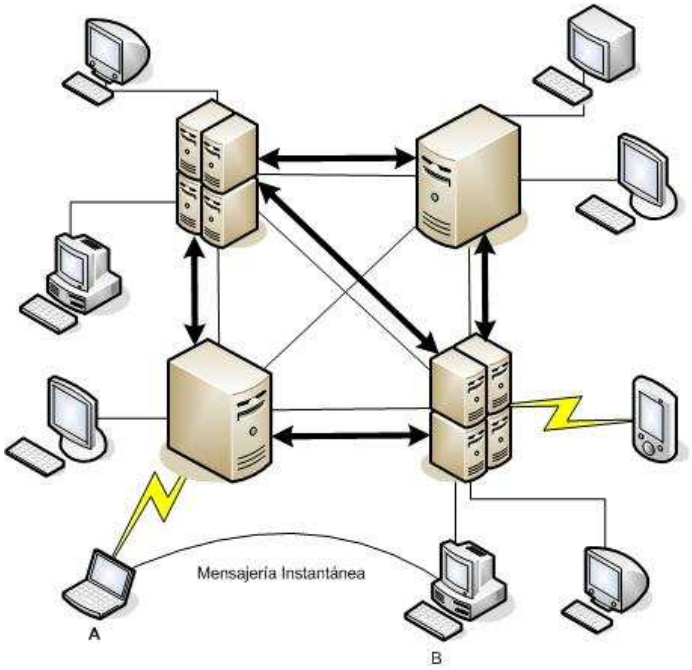
Un enlace P2P presenta tres clasificaciones:

- **Redes P2P centralizadas**
    - Existe un servidor central que almacena información de todos los *hosts*[2] de la red. Además, se encarga de responder a todos los requerimientos de información que son generados por los clientes de la misma.
    - Los servidores centrales no almacenan archivos, sólo poseen información de éstos (nombre, tamaño, tipo de archivo, etc.…) y una lista de los *hosts* que están dispuestos a intercambiar estos archivos.

[1] ***Dynamic Host Configuration Protocol*** : Protocolo de asignación dinámica para la asignación de direcciones IP en una red de datos.
[2] Hosts: se define en español como los equipos o maquinas de la red.

- El servidor central se encarga de enrutar a los clientes, transformando sus credenciales en direcciones IP reales.

Figura 5. RED P2P CENTRALIZADA



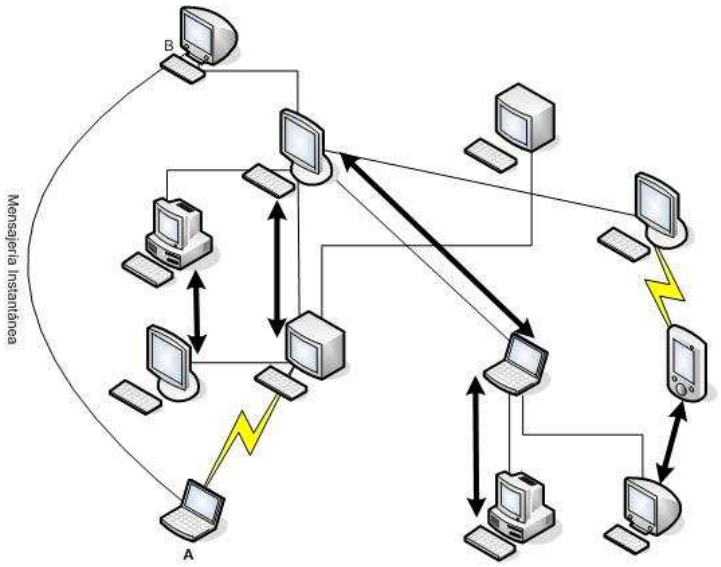
Fuente: Aporte del autor

- **P2P Puros**
  - Los equipos actúan como cliente y servidor.
  - No existe un servidor central que maneje las conexiones de red.
  - No hay un enrutador central que sirva como nodo y administre direcciones.

Algunos ejemplos de una red P2P "pura" son Gnutella, Freenet.[1] (a nivel de Internet) ó una red de datos privada.

[1] Software desarrollado para la transferencia de archivos entre P2P sin la intervención de servidores

Figura 6. RED P2P PURA

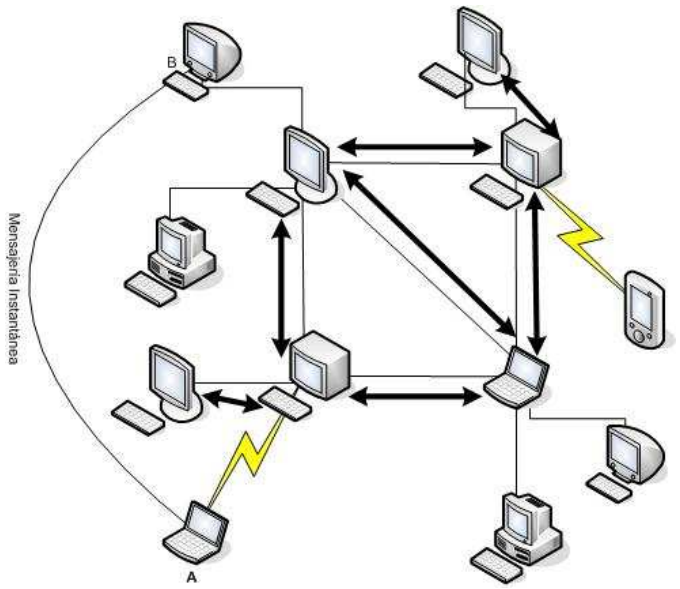


Fuente: Aporte del autor

- **P2P Híbridos**: Poseen características de las redes centralizadas y de las redes puras. En este tipo de red los *hosts* clientes son más robustos; es decir, que poseen mayor capacidad de procesamiento y mayor ancho de banda, actúan como *UltraPeers*; lo que implica que realizan la tarea del servidor central ayudando a las máquinas menos potentes en las tareas de enrutamiento y en la búsqueda de información o fuentes. Características:
    - Tiene un servidor central que guarda información en espera y responde a peticiones para esa información.
    - Los equipos son responsables de guardar la información, que permite al servidor central reconocer los recursos que se desean compartir, y descargar esos recursos compartidos a los equipos que lo solicitan. (El servidor central no almacena este tipo de información)
    - Los terminales de enrutamiento poseen direcciones IP fijas ó que son administradas por un sistema de índices para obtener una dirección absoluta.

Algunos ejemplos de una red P2P hibrida son las aplicaciones para descargar archivos que se encuentran en Internet como Bittorrent e eDonkey2000.

Figura 7. RED P2P HÍBRIDA



Fuente: Aporte del autor

A.2.2 Aplicaciones

Los programas para aplicaciones P2P operan a nivel de la capa de Aplicación y no a nivel de Red, por lo cual se crean relaciones superpuestas a la capa IP, esto es lo que conforma la red para desarrollos P2P. Entre las aplicaciones o usos mas relevantes de la conexión P2P se encuentran:

- **Transferencia de archivos**: Una de las principales aplicaciones que se han desarrollado aprovechando las características especiales que poseen las redes P2P, es la transferencia de archivos. Inicialmente ésta se hacía de forma centralizada, es decir, a través de diferentes servidores que almacenaban la información y las listas de usuarios; sin embargo, este tipo de aplicación fue usada para descargar música de forma gratuita violando derechos de autor y patentes, lo que ocasionó el cierre de muchos de los programas implementados y demandas para los desarrolladores, algunos de los programas mas reconocidos fueron: Napster (Primera aplicación, 1999), Winmx, Audiogalaxy, entre otras; no obstante, el cierre de estos programas dio origen a aplicaciones más desarrolladas que basaban su funcionamiento en redes descentralizadas con lo cual no se tenía un registro de los archivos transferidos. Algunas de estas aplicaciones son: La

red Gnutella, Kazaa, Grokster, Piolet y Bittorent entre otros. Legalmente estas aplicaciones también han sido afectadas.

Cabe mencionar que la transferencia de archivos utilizando redes P2P no ha sido simplemente intercambio ilegal de música, existen aplicaciones encaminadas a brindar soporte, respetando las normas de derechos de autor y patentes como *LionShare* (Instituciones académicas).

- **Mensajería Instantánea**: Otra de las aplicaciones más relevantes es la mensajería instantánea, tanto comercial como privada, esta aplicación permite comunicación inmediata con diferentes usuarios al mismo tiempo, sin la intervención de servidores, ahorrando tiempo y dinero además, algunos de los programas existentes poseen transferencia de archivos y características especiales que los han hecho muy populares entre los usuarios de Internet; no obstante, a nivel corporativo se ha difundido debido a su uso sin costo para ofrecer soporte inmediato a los clientes mejorando así sus servicios; sin embargo, la Mensajería Instantánea (MI) puede resultar un problema para los administradores de red, así como las aplicaciones *greynet*[1] pues en muchos casos estas utilidades se han convertido en la puerta de entrada para malwares.

  Entre las ventajas de esta aplicación se encuentra:
  - Comunicación inmediata
  - Conocimiento de usuarios online/offline.
  - Uso sencillo y directo, no necesita aplicaciones dedicadas.
  - Permite y extiende la comunicación en forma directa y en tiempo real a teléfonos móviles, smartphones y PDA.
  - Menos spam, mayor privacidad (Si se realiza una adecuada configuración de seguridad, es posible reducir en gran medida la cantidad de spam que se recibe normalmente en una comunicación de MI)
  - Aprovecha la comunicación directa P2P: al utilizar redes P2P en vez de una infraestructura de comunicación, permite intercambiar grandes

[1] Greynets: Aplicaciones que permiten el uso de recursos de la red, algunas tienen fines empresariales pero deben contar con las debidas medidas de seguridad de lo contrario son un peligro para la red. EJ: Netmeeting, navegadores, MI, entre otras.

cantidades de datos, sin los requerimientos del recurso que los sistemas existentes demandan.

- Puede integrar fácilmente soporte para RSS[1].

Algunos ejemplos de MI comerciales son: Yahoo Web Messenger, MSN Web Messenger, AIM Express)

- **Transferencia de Voz y Video**: Este tipo de aplicación se ha ido difundiendo de la misma forma que las mismas redes P2P, permite la comunicación visual y auditiva solo con un click, lo cual hace que la comunicación cada día se convierta en un reto para los desarrolladores, pues se busca garantizar privacidad, escalabilidad y seguridad en los datos que se transmiten.

  Las aplicaciones multimedia en general para redes P2P siguen el esquema de funcionamiento descrito a continuación:

  Se inicia el establecimiento de la conexión entre puntos terminales, así como la conexión punto a punto entre los usuarios finales guiados por un protocolo de control de flujo para redes P2P.

  El protocolo SIP[2] y la norma H.323[3] son los protocolos que se encargan del control de la conexión entre terminales. Como medio de transporte se trabaja con el encapsulado definido en las normas H.261[4] ó MPEG[5] *Real Time Protocol* (RTP)[6], para lo cual se utiliza el protocolo IP[7] y se transporta en forma de datagramas. (UDP[8]). Finalmente como mecanismo de señalización de flujo de datos multimedia se utiliza el MGCP/Megaco[9]

[1] RSS: *Really Simple Syndication* Formato que facilita contenidos desde cualquier sitio en la red para su inserción sencilla en una página web.
[2] SIP: Session Initiation Protocol, protocolo genérico para el establecimiento de sesiones multimedia. Se trata de un estándar del IETF y su *RFC* es la 3261.
[3] H.323: Norma de la ITU que se emplea para la señalización de telefonía.
[4] H.261: Norma de la ITU que se emplea para codificación de video
[5] MPEG-4: grupo de estándares de codificación de audio y video.
[6] RTP: Protocolo utilizado para la transmisión de datos en tiempo real, ej: audio y video en una video-conferencia.
[7] IP: Protocolo de Internet para el direccionamiento de paquetes de datos.
[8] UDP: Protocolo de transporte orientado a no conexión.
[9] *MGCP* es utilizado para llevar los datos que viajan de extremo a extremo en las comunicaciones *P2P* al paso por *gateways.* La idea fundamental es la identificación de los puntos terminales de adaptación. Megaco es la evolución de MGCP y la unión de IETF e H.GCP – ITU.

(*Media Gateway Control*) a través de datagramas UDP; a diferencia de H.323 y SIP, MGCP es un protocolo P2P.

Otros servicios de la transferencia de voz y video más complejos son: *Call Hold, Consultation Hold, Unattended Transfer, Call forward Unconditional, Call forward on Busy, Call forward on No Answer, 3-Way Conference, Single line extensión, Find-Me, Incoming Call Screening, Secundary Number – In/Out, Do Not Disturb, Call Waiting*, entre otros.

- **Otras aplicaciones P2P son**:
    - P2P aplicado a dispositivos móviles (se adelantan estudios para determinar protocolos, plataformas y servicios)
    - Computación Distribuida
    - *E-business*: Se busca eficiencia al obtener información de clientes y proveedores.
    - Motores de búsqueda.
    - Bioinformáticos: Utilizan redes P2P para poner en funcionamiento sistemas de software que identifiquen presencia de posibles medicamenteos, como el Centro Computacional para el Descubrimientos de Drogas (*Centre for Computational Drug Discovery* de la Universidad de Oxford en cooperación con la Fundación Nacional para la Investigación del Cancer, *National Foundation for Cancer Research)*. Otro ejemplo de sistemas de administración para biólogos computacionales es el *Chinook* que permite el intercambio de técnicas de análisis a través de más de 25 servicios que tiene para ello.

A nivel internacional se están generando nuevas plataformas para el uso de redes P2P con un mayor número de servicios agregados y con las características de seguridad y privacidad requeridas, una de ellas es la plataforma JXTA, desarrollada por la facultad de ingenierías de Barcelona,

Universidad Politécnica de Cataluña, acompañada por un grupo de universidades y empresas de Barcelona[1]

A.3 Ventajas, riesgos, amenazas e incidencias legales para redes P2P

Este capítulo es una descripción de las posibles ventajas, riesgos, amenazas y las incidencias legales del uso de las redes P2P a nivel general.

A.3.1 Ventajas del uso de redes P2P

Las ventajas que se describen a continuación suponen el porqué de la popularidad que el uso de redes P2P ha logrado en los últimos años:

- **Conectividad variable y escalabilidad:** A nivel global una red P2P se puede observar como millones de redes virtuales que se agrupan de acuerdo a diferentes intereses, por lo cual esta organización permite que un nodo se conecte o desconecte de forma independiente.

- **No Reestructuración de la red:** Añadir o quitar un nodo a la red, no implica ninguna reestructuración de la misma, esto gracias al tipo de organización que posee, en la cual todos los usuarios son clientes y servidores al tiempo. Esta característica también se ve reflejada en la escalabilidad del sistema.

- **No congestión (Mejor uso del ancho de banda):** Debido a que las conexiones se basan en el esquema punto a punto, los cuellos de botella disminuyen considerablemente en comparación del sistema cliente-servidor, (este sistema realiza la conexión de nodos utilizando conexión por difusión ó acceso compartido, se generan problemas de acceso al medio y por ende cuellos de botella). Es importante mencionar que el mayor tráfico en la red por aplicaciones P2P se genera en el ancho de banda y no en la velocidad

[1] Mayor información revisar el sitio web de la Universidad www.upc.es ó directamente el link al respecto es http://www.rediris.es/jt/jt2006/archivo/16Jueves/1600-1830/B/JT006_Jueves_1600_SalaB_P2PJXTA.ppt#45

de descarga debido a que el upstream[1] modifica su comportamiento de ráfagas y se vuelve constante, comparable con el ancho de banda utilizado para descarga de datos, sucede en líneas ADSL[2] y en general en todo tipo de canales.

- **Descentralización**: La ausencia de un servidor central, donde se almacene toda la información tanto de los usuarios como de los datos a transferir, induce mayor agilidad en el intercambio de archivos, desaparece de esta forma jerarquizaciones que limitan la respuesta y velocidad del sistema, se obtiene con ello una computación cooperativa y social.

- **Distribución y Redundancia de datos:** Todos los archivos que se transmiten se encuentran disponibles para todos lo usuarios al mismo tiempo en diferentes punto de almacenamiento. Con esto se logra mayor velocidad de descarga y disponibilidad de recursos.

- **Balanceo de carga y alta disponibilidad:** La organización de la red que distribuye los datos entre todos los usuarios y descentraliza los recursos, desencadena en una mejor utilización de la red así como una mejor optimización de recursos como procesamiento, almacenamiento, ancho de banda, canales de comunicación, entre otros; por consiguiente el balanceo de carga se hace mas equitativo y la disponibilidad de recursos crece. Ref 11, PDF]

- **Motores de Búsquedas:** La posibilidad de realizar búsquedas por toda la red, de forma asíncrona, en paralelo o distribuida, además de la unión de diferentes herramientas colaborativas que se ejecutan sobre la misma arquitectura, han logrado que el uso de estas redes aumente significativamente. [Ref 12, Artículo]

[1] Upstream: Ancho de banda de subida de datos y su contraparte el Downstream que relaciona el ancho de banda de descarga de datos
[2] ADSL: ***A****symmetric* ***D****igital* ***S****ubscriber* ***L****ine*. (Línea de Abonado Digital Asimétrica)

- **Instalación y facilidad de uso:** Otra de las ventajas que tiene trabajar con las redes P2P es la sencillez y rapidez para instalar y realizar mantenimiento a los programas y aplicaciones que emplean este tipo de redes, por lo cual su uso es inmediato y eficaz.

- **Aplicaciones P2P cada vez más extendidas:** Es claro que el trafico P2P es un buen porcentaje del tráfico total de Internet, de igual forma la eficiencia de las aplicaciones que se han desarrollado para ambientes P2P como transferencia de datos, mensajería instantánea, trabajo colaborativo, entre otros; han demostrado su apreciable despliegue a nivel global. [Ref 10, Presentación PowerPoint]

A.4 Riesgos y amenazas generadas por el uso de redes P2P

A continuación se describen los riesgos y amenazas involucrados al utilizar redes P2P.

A.4.1 Problemas de Confidencialidad

Según la filosofía abierta de las redes P2P, el concepto de confidencialidad se hace relativo. Las redes P2P se basan en la intención de compartir información, por lo tanto, salvaguardar la confidencialidad de la información compartida es prácticamente imposible.
La confidencialidad en las redes P2P se reduce a la correcta elección de la información a compartir, es decir, evitando que la información clasificada no sea compartida intencional o accidentalmente en la red.

A.4.2 Falta de autenticidad en los datos compartidos

La mayoría de los programas P2P poseen algoritmos capaces de garantizar la integridad de los archivos; no obstante, esta “integridad” se limita a garantizarle al usuario que el archivo que descarga a través de la red es idéntico al archivo que los demás usuarios están compartiendo; sin embargo, uno de los mayores inconvenientes que afectan la integridad es la falta de autenticidad de la

información disponible en la red por lo tanto, es posible que el contenido del archivo descargado no sea exactamente lo que aparenta ser. Esta característica permite que los usuarios descarguen aplicaciones maliciosas disfrazadas de programas conocidos e incluso de archivos de música, películas o textos.

A.4.3 Baja disponibilidad

Dada la cantidad de nodos o usuarios en la red, la capacidad de procesamiento y ancho de banda de las redes P2P pueden alcanzar niveles altamente peligrosos. Una red P2P comprometida podría originar fácilmente un ataque de negación de servicios (DoS) contra cualquier equipo o red por la cantidad de conexiones que puede recibir en cualquier momento. De acuerdo a algunas estadísticas[1], en ambientes corporativos alrededor del 80% de los funcionarios hacen uso de aplicaciones como mensajería instantánea y descarga de archivos mediante redes P2P.

A.4.4 Autenticación, usuarios no autorizados

En las redes P2P no existe un esquema de autenticación, por lo tanto cualquier usuario que posea el software P2P podrá conectarse a cualquier otra máquina que se encuentre dentro de la red P2P. Esta falta de autenticación, hace la red muy susceptible a todos los problemas asociados con el ingreso de usuarios no autorizados.

A.4.5 Trazabilidad nula

La arquitectura descentralizada hace que la labor del registro de actividades en los programas P2P sea delimitada, y por lo general, se restringe a mantener un historial de los archivos que se han descargado. Estas limitantes sumadas a que la mayoría de los usuarios de las redes P2P son usuarios comunes de Internet que utilizan direcciones IP dinámicas, hace prácticamente imposible llevar una tarea de seguimiento sobre las actividades realizadas mediante este

[1]Fuente de estadísticas: Encuesta anual realizada por el FBI y el Instituto de seguridad de la computación. El documento completo se encuentra en el link http://www.gocsi.com/

software, dando lugar a escasos registros de aplicación que no permitirían realizar un rastreo detallado, en caso de presentarse un problema.

A.5 incidencias legales ocasionados por aplicaciones P2P

A.5.1 Riesgos Legales: Pagos y Responsabilidad corporativa (Derechos de Autor)

En párrafos anteriores se menciona que la confidencialidad de la información compartida en la red se ve afectada por el proceso de publicación; sin embargo, se dejan a un lado los aspectos legales inherentes a la información como es la protección a los derechos de autor y la propiedad intelectual.

Estos derechos de autor son violados por muchos de los usuarios de las redes P2P, fundamentalmente en la transferencia de archivos. Actualmente, varias cortes a nivel mundial han empezado a aplicar con fuerza las leyes y han sentenciado culpables, bajo el cargo de violación de derechos de autor, tanto a las firmas desarrolladoras (Metro-Goldwyn-Mayer Studios Inc. vs. Grokster & Morpheus)[1] de aplicaciones P2P para el intercambio de archivos como a los usuarios finales (Honk Kong Special Administrative Region Vs. Chan Nai Ming)[2].

La industria del entretenimiento (RIAA[3], SGAE, MPA[4], entre otros) sustenta que iniciará una persecución agresiva a nivel mundial contra los violadores de los derechos de autor (Copyright) debido al uso de las aplicaciones de enlace P2P. Incluso, se ha iniciado la búsqueda de acciones legales en contra de los proveedores de servicios de Internet, como de los usuarios finales de estas aplicaciones; y contra las corporaciones, por no evitar que sus empleados

[1] Supreme Court Of The United States, Metro-Goldwyn-Mayer Studios Inc. Vs. Grokster, Ltd. http://news.bbc.co.uk/1/shared/bsp/hi/pdfs/supreme_court_mgm_grokster_27_06_05.pdf
[2] Hong Kong Special Administrative Region, HKSAR Vs Chan Nai Ming. http://legalref.judiciary.gov.hk/lrs/common/search/search_result_detail_body.jsp?ID=&DIS=46722&QS=%2B&TP=JU
[3] RIAA (Recording Industry Association of America),
[4] MPA (Motion Picture Association)

hagan uso de las mismas, pues de esta forma se está contribuyendo pasivamente a infringir los derechos de autor.

En mayo de 2003, la RIAA, envió notificaciones a más de 300 corporaciones, alegando que sus empleados podían estar usando PC's de uso corporativo para conectarse a Internet por medio de aplicaciones P2P para traficar de forma ilegal material protegido con derechos de autor. Unos meses después, la Corte Federal de US, falló a favor de la RIAA y en contra de Verizon (un proveedor de servicios de Internet para usuarios y corporaciones), obligando a Verizon, a identificar a uno de sus subscriptores que había sido identificado descargando material registrado con derechos de autor, mediante aplicaciones P2P.

Así mismo es importante mencionar algunas acciones que han llevado a cabo empresas desarrolladoras de aplicaciones P2P como la compañía *Metamachine*[1] que en septiembre de 2006 se comprometió en un acuerdo extrajudicial a pagar a la RIAA cerca de U$30 millones para evitar demandas de la industria discográfica.

Además eDonkey 2000 dejó de funcionar, desplegando un aviso que informa sobre lo ilegal que es compartir música y videos que tengan copyright.

Finalmente como una alternativa más para evitar este tipo de violaciones ó para entablar posibles pelitos, se ha implementado el uso de servidores *fake*. Un servidor *fake* se caracteriza por no ser verdaderamente un servidor de la red eDonkey2000 sino que es utilizado para obtener información de los usuarios que se conectan a la red para descargar archivos ó contaminar la red con *elinks* falsos, corruptos, ó simplemente llenos de basura. Un ejemplo de éstos son los servidores Razorback 2.2, 2.3… y 2.6, entre otros.

En Colombia, los derechos de autor están cobijados por dos normativas*:* La Decisión 351 de La Comunidad Andina, sobre Derechos de Autor y Derechos

[1] Metamachine es la propietaria del programa eDonkey, software implementado para descargar archivos a través de redes P2P.

Conexos[1]; la Ley 23 de 1982[2] y Ley 44 de 1993[3] del Congreso de la República de Colombia, sobre Derechos de Autor. Adicionalmente, Colombia ha firmado una serie de convenios internacionales[4] referentes a los Derechos de Autor, la mayoría de ellos, liderados por la OMPI, Organización Mundial de la Propiedad Intelectual.

Al respecto, en el anexo A se mencionan algunos de los artículos que pueden ser usados legalmente para seguir el ejemplo de otros países en la lucha contra la violación de derechos de autor, y que a su vez, podrían ser usados en contra de los usuarios de aplicaciones P2P que realizan intercambio de archivos a través de Internet.

A.6 Riesgos y amenzas Tecnológicas asociadas a la seguridad de la información por el uso de aplicaciones P2P.

A continuación se mencionan en detalle los riesgos tecnológicos asociados a la seguridad de la información que implica realizar el intercambio de archivos a través de redes P2P.

A.6.1 Código Malicioso

Dentro del código malicioso se encuentran los virus, los "*malware"* los errores en el *software* y la fuga de información sensible que a continuación se describe en detalle.

- **Virus:** Hace algunos años, los virus informáticos requerían un medio de transmisión (email, diskette, etc) que los transportara de una máquina a otra y así, poder infectarla. No obstante, a raíz del auge de las aplicaciones

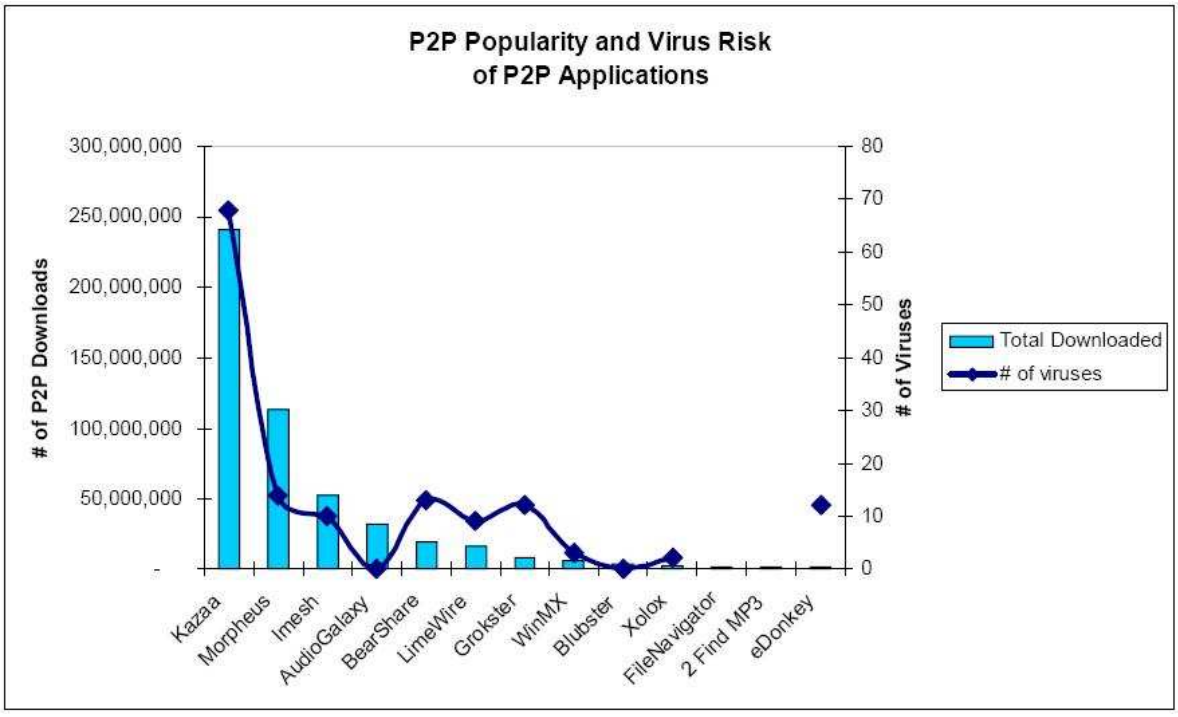
[1] Decisión 351 de La Comunidad Andina, sobre Derechos de Autor y Derechos Conexos. http://www.comunidadandina.org/normativa/dec/D351.htm
[2] Ley 23 de 1982 del Congreso de la República de Colombia, sobre Derechos de Autor. http://www.derautor.gov.co/htm/legal/legislacion/leyes_arch/23.doc
[3] Ley 44 de 1993 del Congreso de la República de Colombia, adiciones y modificaciones a la Ley 23 de 1982. http://www.derautor.gov.co/htm/legal/legislacion/leyes_arch/44.doc
[4] Convenios y Tratados Internacionales firmados por Colombia. http://www.derautor.gov.co/htm/legal/legislacion/convenios.htm

P2P, los virus informáticos han cambiado su táctica. Estos virus actuales sólo necesitan camuflarse en forma de software popular, (películas, música, documentos e incluso imágenes); y esperar hasta que un usuario lo descargue a través de una aplicación de intercambio de archivos.

Según las estadísticas de la firma de Antivirus, *Sophos*, en julio del 2002 existían 10 virus que utilizaban como medio, las aplicaciones P2P. Para julio de 2003, los creadores de virus habían aprendido a explotar las vulnerabilidades de estas grandes comunidades *on-line*[1], logrando incrementar el número de virus a 70. [Ref 13, Artículo]

La figura 5, presenta una gráfica de la relación existente entre la popularidad de las aplicaciones P2P y el número de virus que las afectaban.

Figura 8. APLICACIONES P2P VS RIESGOS DE INFECCIÓN POR VIRUS (2003)



Fuente: Tomado de Internet

[1] On line: indica que la maquina se encuentra conectada a Internet

Una vez descargados los virus, estos ejecutan su carga ocasionando daños y riesgos considerables para una organización. Entre los riesgos más comunes tenemos:

- Ataques Distribuidos de Negación de Servicio (*DDoS, Distributed Denial of Service*[1])**:** El virus contiene código que hace que el PC infectado participe en un ataque DDoS [Ref 14]
- Desactivación de Software Antivirus y *Firewall*: Una de las primeras acciones de estos virus es intentar desactivar las aplicaciones de seguridad, esto con el fin de dejar indefensa la máquina infectada [Ref 15]
- *Troyanos & Keylogger*: Este tipo de virus representa una de las peores amenazas para las corporaciones. Los troyanos generalmente abren un puerto (canal de comunicaciones) en el PC infectado; este canal puede ser usado por un atacante para obtener control total de PC en forma remota. Este tipo de acceso le permitirá al atacante ver, copiar, borrar y modificar la información almacenada en el PC infectado; e incluso, puede permitir al atacante utilizar ese acceso no autorizado para obtener acceso en otras máquinas de la red. [Ayllón & Jiménez, 2004]
- Corrupción o borrado de archivos: Este tipo de virus elimina los archivos de oficina (Documentos de Word, Excel, PowerPoint, etc) y corrompe archivos del sistema operativo y de otras aplicaciones, dejando el PC prácticamente inservible. [Hernández, Orlando & Sanchez, 2003]

- ***Malware (Adware, spyware*)**: 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).

  Según un estudio realizado por la firma Lavasoft, desarrolladora de software *Anti-Spyware*, se encontró que el 98% de las aplicaciones P2P

[1]DDoS: Este ataque busca detener el trabajo de un servidor, es efectivo si se realiza al mismo tiempo desde una gran cantidad de equipos.

contienen algún tipo de *malware*. Estas aplicaciones de tipo *malware* no son necesariamente ilegales, pues el usuario final debe aceptar los términos de la licencia para poder instalar la aplicación P2P. Sin embargo en la mayoría de los casos, después de desinstalado el software P2P, las aplicaciones de tipo *malware* continúan instaladas y ejecutándose en el PC. [Skoudis & Zeltser, 2003]

- **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*[1].

- **Fuga de información sensible:** Dicha amenaza ocurre cuando un dato o software es accedido, leído y posiblemente liberado a un individuo que no tiene autorización para acceder a el. Dadas las características de las redes P2P, cualquier vulnerabilidad o virus podría permitir que un atacante extrajera información clasificada o sensible de la organización.

A.6.2 Riesgos asociados a la Disponibilidad de los Recursos

Para dar una idea de la cantidad de información que se comparte en una red P2P, se presenta el siguiente ejemplo. El 10 de julio del 2003, a las 9:30am, la red P2P Kazaa, tenía 3.5 millones de PC's conectados y compartiendo 738 millones de archivos que juntos sumaban al rededor de 5.7 millones de G*Gigabytes*[2]. Eso quiere decir, que el usuario promedio estaría compartiendo unos 200 archivos o 1.6 *Gbytes* de datos, y qué cualquiera de los otros 3.5 millones de usuarios podrían conectarse a su PC para descargar la información compartida.

[1] CERT: Centro de expertos para la seguridad en Internet, opera en Estados Unidos, Carnegie Mellon University.
[2] Gigabyte es equivalente a 1024x8 bites (Unidad mínima de medida de datos).

Suponiendo que, en promedio, todos los usuarios estuviesen navegando a través de una conexión de banda ancha de 128kbps[1] (lo cual, hoy es altamente probable), esta red habría tenido, ese 10 de julio del 2003, un ancho de banda aproximado de 218.750 E1[2], lo cual sería suficiente para realizar un ataque exitoso de negación de servicio al mejor proveedor de servicios de Internet a nivel mundial.

El uso de aplicaciones P2P dentro de una red corporativa, tiene la capacidad de perturbar el desarrollo de los planes de gestión de ancho de banda de varias formas:

- **Incremento en el uso de los canales de comunicaciones:** Unos pocos usuarios P2P pueden consumir de forma desproporcionada la mayoría o incluso, la totalidad del ancho de banda del canal de telecomunicaciones. Lo cual puede generar lentitud en los demás servicios de la red (email, Web, etc), y en el peor de los casos, puede llegar a dejarlos totalmente fuera de servicio.
- **Perturbaciones en los patrones normales de uso:** Los administradores de las redes de telecomunicaciones por lo general poseen registros detallados del comportamiento de su canal, esto en pro de realizar una buena gestión sobre el ancho de banda, sin embargo, el uso de las aplicaciones P2P altera estos patrones normales de comportamiento, debido a que los usuarios deben mantener las aplicaciones conectadas la mayoría del tiempo (día y noche) para poder finalizar sus descargas.
- **Tasas de transmisión Carga/Descarga (*Upstream/Downstream*) invertidas:** En la mayoría de las redes corporativas, es mayor el tráfico entrante (*Downstream*) que el tráfico saliente (*Upstream*). Sin embargo, con el uso de las aplicaciones P2P el tráfico saliente tiende a aumentar considerablemente, e incluso supera en tráfico entrante. Dado que este tipo de comportamiento no es algo planeado, la inversión de las ratas de transmisión arroja como resultado una congestión general en la red.

[1] Kbps inidica la rata de bites por segundo
[2] E1 equivale a 2048 kbps. La red de la Universidad posee actualmente, sumando los dos proveedores, un ancho de banda en Internet de aproximadamente igual a 10 E1.

A.6.3 Riesgos asociados a factores humanos

- **Recursos y conocimiento del usuario final:** Uno de los principales riesgos de las aplicaciones P2P es el desconocimiento de los usuarios finales, quienes muchas veces se dejan engañar fácilmente por el nombre del archivo que intentan descargar, pues no tienen el conocimiento necesario para identificar el tipo de archivo (video, audio, texto, archivo comprimido, archivo ejecutable, etc.) con la información que tienen a su disposición en la aplicación P2P. Este es el principal motivo por el cual los usuarios terminan descargando y ejecutando aplicaciones maliciosas en sus computadores.

  Adicionalmente, el usuario final promedio, se dedica a descargar videos, películas, música, juegos y programas de uso popular. La mayoría de estos archivos, exceptuando los archivos de audio, son archivos de gran tamaño por lo cual, el consumo de ancho de banda se intensificará, de igual forma, el usuario requerirá aumentar el espacio disponible en su disco duro para poder almacenar todas sus descargas.

A.7 Tablas: resumen ventajas, riesgos y Amenazas.

Tabla 17. Resumen Ventajas

Ventajas	Conectividad Variable y Escalabilidad
	No Reestructuración de la red
	No Congestión (Mejor uso del ancho de banda)
	Descentralización
	Distribución y Redundancia de Datos
	Balanceo de Carga y alta disponibilidad
	Motores de Búsqueda
	Instalación y Facilidad de Uso
	Aplicaciones P2P mas extendidas

Tabla 18. Resumen Riesgos

Riesgos		
Riesgos generados por el uso de redes P2P	Problemas de confidencialidad	
	Falta de autenticidad en los datos compartidos	
	Baja disponibilidad	
	Autenticación, usuarios no autorizados	
	Trazabilidad nula	
Incidencias Legales	Responsabilidades corporativas no reconocidas	
	Violación de derechos de autor y patentes	
	Multas y pagos judiciales	
Riesgos tecnológicos asociados a la seguridad de la información	Código Malicioso	**Virus:** • Ataques DDoS • Desinstalación de Antivirus y Firewall • Troyanos/keylogger • Corrupción o borrado de archivos
		Malware(adware/spyware)
		Errores en el SW
		Fuga de Información sensible
	Riesgos asociados a la disponibilidad de recursos.	Incremento en el uso de canales de comunicación
		Perturbaciones en los patrones normales de uso
		Tasas de Tx superiores al umbral ó invertidas
	Riesgos asociados a factores humanos	Recursos y conocimiento del usuario final

B. ANEXO B INCIDENCIAS LEGALES

B.1 De la Decisión 351 de la Comunidad Andina

Artículo 1. Las disposiciones de la presente Decisión tienen por finalidad reconocer una adecuada y efectiva protección a los autores y demás titulares de derechos, sobre las obras del ingenio, en el campo literario, artístico o científico, cualquiera que sea el género o forma de expresión y sin importar el mérito literario o artístico ni su destino.

Artículo 2. Cada País Miembro concederá a los nacionales de otro país, una protección no menos favorable que la reconocida a sus propios nacionales en materia de Derecho de Autor y Derechos Conexos.

Artículo 4. La protección reconocida por la presente Decisión recae sobre todas las obras literarias, artísticas y científicas que puedan reproducirse o divulgarse por cualquier forma o medio conocido o por conocer, y que incluye, entre otras, las siguientes:

a) Las obras expresadas por escrito, es decir, los libros, folletos y cualquier otro tipo de obra expresada mediante letras, signos o marcas convencionales;

b) Las conferencias, alocuciones, sermones y otras obras de la misma naturaleza;

c) Las composiciones musicales con letra o sin ella;

d) Las obras dramáticas y dramático-musicales;

e) Las obras coreográficas y las pantomimas;

f) Las obras cinematográficas y demás obras audiovisuales expresadas por cualquier procedimiento;

g) Las obras de bellas artes, incluidos los dibujos, pinturas, esculturas, grabados y litografías;

h) Las obras de arquitectura;

i) Las obras fotográficas y las expresadas por procedimiento análogo a la fotografía;

j) Las obras de arte aplicado;

k) Las ilustraciones, mapas, croquis, planos, bosquejos y las obras plásticas relativas a la geografía, la topografía, la arquitectura o las ciencias;

l) Los programas de ordenador;

i.e.) Las antologías o compilaciones de obras diversas y las bases de datos, que por la selección o disposición de las materias constituyan creaciones personales.

B.2 De la Ley 44 de 1993 del Congreso de la República de Colombia

Artículo 51. Incurrirá en prisión de dos (2) a cinco (5) años y multa de cinco (5) a veinte (20) salarios legales mínimos mensuales:

Quien reproduzca fonogramas, videogramas, soporte lógico u obras cinematográficas sin autorización previa y expresa del titular, o transporte, almacene, conserve, distribuya, importe, venda, ofrezca, adquiera para la venta o distribución o suministre a cualquier título dichas reproducciones.

B.3 TITULO III, DELITOS CONTRA LA LIBERTAD INDIVIDUAL Y OTRAS GARANTIAS CAPITULO SEPTIMO, del código penal (Ley 599 de 2000)

B.3.1 De la violación a la intimidad, reserva e interceptación de comunicaciones

Artículo 192. *Violación ilícita de comunicaciones*. El que ilícitamente sustraiga, oculte, extravíe, destruya, intercepte, controle o impida una comunicación privada dirigida a otra persona, o se entere indebidamente de su contenido, incurrirá en prisión de uno (1) a tres (3) años, siempre que la conducta no constituya delito sancionado con pena mayor.

Si el autor de la conducta revela el contenido de la comunicación, o la emplea en provecho propio o ajeno o con perjuicio de otro, la pena será prisión de dos (2) a cuatro (4) años.

Artículo 193. *Ofrecimiento, venta o compra de instrumento apto para interceptar la comunicación privada entre personas*. El que sin permiso de autoridad competente, ofrezca, venda o compre instrumentos aptos para interceptar la comunicación privada entre personas, incurrirá en multa, siempre que la conducta no constituya delito sancionado con pena mayor.

Artículo 194. *Divulgación y empleo de documentos reservados*. El que en provecho propio o ajeno o con perjuicio de otro divulgue o emplee el contenido de un documento que deba permanecer en reserva, incurrirá en multa, siempre que la conducta no constituya delito sancionado con pena mayor.

Artículo 195. *Acceso abusivo a un sistema informático*. El que abusivamente se introduzca en un sistema informático protegido con medida de seguridad o se mantenga contra la voluntad de quien tiene derecho a excluirlo, incurrirá en multa.

Artículo 196. *Violación ilícita de comunicaciones o correspondencia de carácter oficial*. El que ilícitamente sustraiga, oculte, extravíe, destruya, intercepte, controle o impida comunicación o correspondencia de carácter oficial, incurrirá en prisión de tres (3) a seis (6) años.
La pena descrita en el inciso anterior se aumentará hasta en una tercera parte cuando la comunicación o la correspondencia esté destinada o remitida a la Rama Judicial o a los organismos de control o de seguridad del Estado.

B.4 TITULO X, DELITOS CONTRA EL ORDEN ECONOMICO SOCIAL, CAPITULO PRIMERO del código penal (Ley 599 de 2000)

B.4.1 Del acaparamiento, la especulación y otras infracciones

Artículo 306. *Usurpación de marcas y patentes*. El que utilice fraudulentamente nombre comercial, enseña, marca, patente de invención,

modelo de utilidad o diseño industrial protegido legalmente o similarmente confundible con uno protegido legalmente, incurrirá en prisión de dos (2) a cuatro años y multa de veinte (20) a dos mil (2.000) salarios mínimos legales mensuales vigentes.

En la misma pena incurrirá quien financie, suministre, distribuya, ponga en venta, comercialice, transporte o adquiera con fines comerciales o de intermediación, bienes producidos o distribuidos en las circunstancias previstas en el inciso anterior

Artículo 307. *Uso ilegítimo de patentes*. El que fabrique producto sin autorización de quien tiene el derecho protegido legalmente, o use sin la debida autorización medio o proceso patentado, incurrirá en prisión de uno (1) a cuatro (4) años y multa de veinte (20) a mil (1.000) salarios mínimos legales mensuales vigentes.

En la misma pena incurrirá el que introduzca al país o saque de él, exponga, ofrezca en venta, enajene, financie, distribuya, suministre, almacene, transporte o adquiera con fines comerciales o de intermediación producto fabricado con violación de patente.

Artículo 308. *Violación de reserva industrial o comercial*. El que emplee, revele o divulgue descubrimiento, invención científica, proceso o aplicación industrial o comercial, llegados a su conocimiento por razón de su cargo, oficio o profesión y que deban permanecer en reserva, incurrirá en prisión de dos (2) a cinco (5) años y multa de veinte a dos mil (2.000) salarios mínimos legales mensuales vigentes.

En la misma pena incurrirá el que indebidamente conozca, copie u obtenga secreto relacionado con descubrimiento, invención científica, proceso o aplicación industrial o comercial.

La pena será de tres (3) a siete (7) años de prisión y multa de cien (100) a tres mil (3.000) salarios mínimos legales mensuales vigentes, si se obtiene provecho propio o de tercero.

B.5 Modificaciones de los artículos 257, 271, 272 y 306 del código penal.

LEY No. 1032 22 JUN 2006

"POR LA CUAL SE MODIFICAN LOS ARTICULOS 257, 271, 272 Y 306 DEL CÓDIGO PENAL"

El Congreso de Colombia

DECRETA:

Artículo 1. El Artículo 257 del Código Penal quedará así:

ARTICULO 257. De la prestación, acceso o uso ilegales de los servicios de telecomunicaciones. El que, sin la correspondiente autorización de la autoridad competente, preste, acceda o use servicio de telefonía móvil, con ánimo de lucro, mediante copia o reproducción de señales de identificación de equipos terminales de estos servicios, o sus derivaciones, incurrirá en prisión de cuatro (4) a diez (10) años y en multa de quinientos (500) a mil (1.000) salarios mínimos legales mensuales vigentes.

En las mismas penas incurrirá el que, sin la correspondiente autorización, preste, comercialice, acceda o use el servicio de telefonía pública básica local, local extendida, o de larga distancia, con ánimo de lucro.

Iguales penas se impondrán a quien, sin la correspondiente autorización, acceda, preste, comercialice, acceda o use red, o cualquiera de los servicios de telecomunicaciones definidos en las normas vigentes.

Parágrafo 1º. No incurrirán en las conductas tipificadas en el presente artículo quienes en virtud de un contrato con un operador autorizado comercialicen servicios de telecomunicaciones.

Parágrafo 2º. Las conductas señaladas en el presente artículo, serán investigables de oficio.

Artículo 2. El artículo 271 del Código Penal quedará así:

ARTICULO 271. Violación a los derechos patrimoniales de autor y derechos conexos. Incurrirá en prisión de cuatro (4) a ocho (8) años y multa de veintiséis punto sesenta y seis (26.66) a mil (1000) salarios mínimos legales mensuales vigentes quien, salvo las excepciones previstas en la Ley, sin autorización previa y expresa del titular de los derechos correspondientes:

1. Por cualquier medio o procedimiento, reproduzca una obra de carácter literario, científico, artístico o cinematográfico, fonograma, videograma, soporte lógico o programa de ordenador, o, quien transporte, almacene, conserve, distribuya, importe, venda, ofrezca, adquiera para la venta o distribución, o suministre a cualquier título dichas reproducciones.
2. Represente, ejecute o exhiba públicamente obras teatrales, musicales, fonogramas, videogramas, obras cinematográficas, o cualquier otra obra de carácter literario o artístico.
3. Alquile o, de cualquier otro modo, comercialice fonogramas, videogramas, programas de ordenador o soportes lógicos u obras cinematográficas.
4. Fije, reproduzca o comercialice las representaciones públicas de obras teatrales o musicales.
5. Disponga, realice o utilice, por cualquier medio o procedimiento, la comunicación, fijación, ejecución, exhibición, comercialización, difusión o distribución y representación de una obra de las protegidas en este título.
6. Retransmita, fije, reproduzca o, por cualquier medio sonoro o audiovisual, divulgue las emisiones de los organismos de radiodifusión.
7. Recepcione, difunda o distribuya por cualquier medio las emisiones de la televisión por suscripción.

Artículo 3. El artículo 272 del Código Penal quedará así:

ARTICULO 272. Violación a los mecanismos de protección de derecho de autor y derechos conexos, y otras defraudaciones.

Incurrirá en prisión de cuatro (4) a ocho (8) años y multa de veintiséis punto sesenta y seis (26.66) a mil (1000) salarios mínimos legales mensuales vigentes, quien:

1. Supere o eluda las medidas tecnológicas adoptadas para restringir los usos no autorizados.
2. Suprima o altere la información esencial para la gestión electrónica de derechos, o importe, distribuya o comunique ejemplares con la información suprimida o alterada.
3. Fabrique, importe, venda, arriende o de cualquier forma distribuya al público u dispositivo o sistema que permita descifrar una señal de satélite cifrada portadora de programas, sin autorización del distribuidor legítimo de esa señal; o, de cualquier forma, eluda, evada, inutilice o suprima un dispositivo o sistema, que permita a los titulares del derecho controlar la utilización de sus obras o fonogramas, o les posibilite impedir o restringir cualquier uso no autorizado de estos.
4. Presente declaraciones o informaciones destinadas directa o indirectamente al pago, recaudación, liquidación o distribución de derechos económicos de autor o derechos conexos, alterando o

falseando, por cualquier medio o procedimiento, los datos necesarios para estos efectos.

Artículo 4. El artículo 306 del Código Penal quedará así:

ARTICULO 306. Usurpación de derechos de propiedad industrial y derechos de obtentores de variedades vegetales:

El que, fraudulentamente, utilice nombre comercial, enseña, marca, patente de invención, modelo de utilidad, diseño industrial, o usurpe derechos de obtentor de variedad vegetal, protegidos legalmente o similarmente confundibles con uno protegido legalmente, incurrirá en prisión de cuatro (4) a ocho (8) años y multa de veintiséis punto sesenta y seis (26.66) a mil quinientos (1.500) salarios mínimos legales mensuales vigentes.

En las mismas penas incurrirá quien financie, suministre, distribuya, ponga en venta, comercialice, transporte o adquiera con fines comerciales o de intermediación, bienes o materia vegetal, producidos, cultivados o distribuidos en las circunstancias previstas en el inciso anterior.

ARTICULO 5. Derogatoria y Vigencia. La presente ley rige a partir de su promulgación y deroga todas las disposiciones que le sean contrarias.

LA PRESIDENTA DEL H. SENADO DE LA REPUBLICA,

Claudia BLUM DE BARBERI

EL SECRETARIO GENERAL DEL H. SENADO DE LA REPUBLICA,

Emilio Ramón OTERO DAJUD

EL PRESIDENTE DE LA H. CAMARA DE REPRESENTANTES

Julio E. GALLARDO ARCHBOLD

EL SECRETARIO GENERAL DE LA H. CAMARA DE REPRESENTANTES,

Angelino LIZCANO RIVERA

REPUBLICA DE COLOMBIA - GOBIERNO NACIONAL

PUBLIQUESE Y EJECUTESE

Dada en Bogotá, D.C, a los

EL MINISTRO DEL INTERIOR Y DE JUSTICIA,

SABAS PRETELT DE LA VEGA

C. ANEXO C FICHAS DE REGISTRO

C.1 Registro de Riesgo

REGISTRO DE RIESGO

Actividad: Aplicaciones P2P | **Fecha de revisión del riesgo:**

Compilado por: | **Fecha:**

Revisado por: | **Fecha:**

Referencia	Riesgo	Adecuación de controles existent	Clasif. de la probabilidad	Clasif. de la consecuencia	Nivel de riesg	Prioridad
Ap2p1	Recursos y conocimiento del usuario final		Casi cierto	Alto	E (1)	1
Ap2p2	Responsabilidades corporativas no reconocidas		Probable	Medio-Alto	E (0,49)	2
Ap2p3	Multas y pagos judiciales		Probable	Medio-Alto	E (0,49)	3
Ap2p4	Autenticación, usuarios no autorizados		Posible	Alto	E (0,49)	4
Ap2p5	Falta de autenticidad en los datos compartidos	X	Posible	Alto	E (0,49)	5
Ap2p6	Problemas de confidencialidad		Casi cierto	Medio	H (0,4)	6
Ap2p7	Fuga de información sensible	X	Probable	Medio-Alto	H (0,4)	7
Ap2p8	Tasas de Tx descontroladas ó invertidas	X	Posible	Alto	H (0,4)	8
Ap2p9	Fallas en los sistema de seguridad informática	X	Probable	Medio-Alto	H (0,4)	9
Ap2p10	Troyanos/Keylogger	X	Posible	Alto	H (0,4)	10
Ap2p11	Corrupción o borrado de archivos	X	Posible	Alto	H (0,4)	11
Ap2p12	Incremento uso de canales	X	Probable	Medio	M (0,28)	12
Ap2p13	Perturbaciones en los patrones normales de uso		Probable	Medio	M (0,28)	13
Ap2p14	Desintalación de Antivirus y firewall	X	Posible	Medio-Alto	M (0,28)	14
Ap2p15	Baja disponibilidad		Probable	Medio	M (0,28)	15
Ap2p16	Fallas en los protocolos de conexión		Posible	Medio-Alto	M (0,28)	16
Ap2p17	Trazabilidad nula	X	Improbable	Medio	L (0,04)	17
Ap2p18	Ataques DDoS		Posible	Bajo	L (0,04)	18
Ap2p19	Malware	X	Posible	Bajo	L (0,04)	19

C.2 Ficha Ejemplo Cronograma y Plan de Tratamiento

CRONOGRAMA Y PLAN DE TRATAMIENTO DEL RIESGO

Actividad: Aplicaciones P2P — **Fecha de revisión del riesgo:**

Compilado por: — **Fecha:**

Revisado por: — **Fecha:**

Riesgo en orden de prioridad	Opciones preferidas				Clasif. Del riesgo despues del	Resultado del análisis	Responsable de implementar el plan	Cronograma	Acciones monitoreo riesgo y opciones de tratamientos
	1	2	3	4					
Recursos y conocimiento del usuario final		X	X			Aceptar			
Responsabilidades corporativas no reconocidas		X	X	X		Aceptar			
Multas y pagos judiciales		X	X	X		Aceptar			
Autenticación, usuarios no autorizados		X	X	X		Aceptar			
Falta de autenticidad en los datos compartidos		X	X			Aceptar			
Problemas de confidencialidad		X	X			Aceptar			
Fuga de información sensible		X	X			Aceptar			
Tasas de Tx descontroladas ó invertidas		X	X	X		Aceptar			
Fallas en los sistema de seguridad informática		X	X	X		Aceptar			
Troyanos/Keylogger		X	X			Aceptar			
Corrupción o borrado de archivos		X	X			Aceptar			
Incremento uso de canales		X	X			Aceptar			
Perturbaciones en los patrones normales de uso		X	X			Aceptar			
Desintalación de Antivirus y firewall		X	X			Aceptar			
Baja disponibilidad		X	X			Aceptar			
Fallas en los protocolos de conexión			X	X		Aceptar			
Trazabilidad nula						Rechazar			
Ataques DDoS						Rechazar			
Malware						Rechazar			