Hacia una Taxonomía de Incidentes de Seguridad en Internet

Zulima Ortiz Bayona[1]

Francisco Galindo Pulido[2]

RESUMEN

Este artículo hace un recorrido por la evolución histórica de las taxonomías en la seguridad informática, consideradas estas como elementos fundamentales en el entendimiento y clasificación de la información acerca de ataques e incidentes, cuyo conocimiento permite un adecuado manejo de estos. Se finaliza sugiriendo ajustes a la taxonomía basada en procesos, con orientación a eventos, la cual se considera la aproximación más útil para el estudio de este tema, en especial en Internet.

Palabras clave: incidentes de seguridad, seguridad, taxonomía.

Towards to Security Incidents Taxonomy in Internet

ABSTRACT

This paper does a tracking for historic evolution of security taxonomy, taking this as fundamental elements in understanding and classification of information about security attacks and incidents, which knowledge of them let us get an optimal handle. It finish suggesting changes on taxonomy based in processes, with events orientation, which is consider the most utile approximation in this topic, especially in Internet.

Key words: security, security incidents, taxonomy.

1. INTRODUCCIÓN

Internet, la red de redes, es hogar de muchos. Negocios, música, cine, literatura, han encontrado su espacio en Internet. Pero también han surgido otro tipo de situaciones, amparadas por el anonimato relativo que brinda, como ataques, intrusiones, amenazas, terrorismo, ilegalidad. En este entorno se mueven muchas empresas e industrias que quieren tener su sitio en Internet, estableciendo redes privadas y compartiendo información. Para que esto sea posible, se debe hacer de Internet un lugar mas seguro, con regulaciones, tecnologías y la posibilidad real de defenderse y responder de forma proactiva a las amenazas.

2. DESARROLLO DEL TEMA

En la búsqueda de una forma eficiente de conservar, analizar y representar la información acerca de los incidentes de seguridad en sistemas de información y en particular aquellos ocurridos sobre Internet, se ha optado por diversos tipos de clasificaciones taxonómicas (una clasificación taxonómica permite un mejor entendimiento en un campo de estudio) La taxonomía no es única, es decir dentro de un área determinada no se encuentra un sistema universal de clasificación, por lo que podemos encontrar algunas clasificaciones simples, y otras más elaboradas.

El camino para alcanzar una clasificación apropiada ha empezado por definir en forma precisa el objeto de estudio, esto es, la seguridad informática, tema en el que a lo largo de estos últimos años se han variado las definiciones.

Inicialmente se equiparó seguridad con confidencialidad o secreto, dado que este era un tema militar, relacionado a menudo con espionaje o invasión a la privacidad.

Posteriormente, y debido a las características de compartir recursos y sistemas, cobró importancia la integridad de la información, empezando también la seguridad informática a involucrar no solamente la seguridad de los datos, sino también la seguridad de los recursos («evitar que alguien haga algo que usted no quiere con, sobre o desde sus equipos de cómputo»).

Aparece entonces el concepto de confianza. Un equipo de cómputo es seguro si se puede confiar en que se comporte como se espera. Es así que se confía en el sistema para conservar y proteger los datos. El concepto de confianza, dado que implícitamente tiene involucrado contar con el sistema cuando se requiere, evoluciona hacia la disponibilidad. Se tienen así los tres factores que se han abordado en forma preferente al hablar de seguridad informática: confidencialidad, integridad y disponibilidad.

Pero los eventos que pueden atentar contra estos tres factores son diversos, involucrando desastres naturales, situaciones delincuenciales, accidentes, etc., sobre muchos de los cuales no se

[1] Miembro Grupo de Investigación Arquisoft Rama de Seguridad Informática de la Universidad Distrital Francisco José de Caldas.

[2] Jefe de la Oficina de informática y telecomunicaciones del Instituto Geográfico Agustín Codazzi.

Artículo recibido el 16 de Mayo de 2005, aprobado para publicación el 26 de Mayo de 2006

puede tener mayor control, diferente a la protección y respaldo de los datos. Es por este tipo de situaciones que también se aborda la definición de seguridad informática desde un enfoque procedimental. Se establece la definición de seguridad informática en evitar que un atacante alcance unos objetivos a través de ataques sobre computadores o redes.

Los sistemas informáticos, en general, tienen una función que se establece como normal, es decir, aquella que sus legítimos propietarios o dueños le han asignado. Se tiene un proceso normal que se da en estos sistemas. Seguridad informática, acorde a la definición ya planteada, es garantizar que se tiene un proceso normal en el sistema informático y no aquel que conecta al atacante con sus objetivos. Para entender mejor el tema de la seguridad informática, como en general se hace con cualquier campo de estudio, se opta por realizar clasificaciones o taxonomía que permitan simplificar el análisis.

Dichas clasificaciones o taxonomías, para que realmente aporten en el entendimiento del problema deben cumplir con algunas características definidas como son: Mutuamente excluyente, es decir la clasificación en una categoría excluye a todas las otras. Exhaustiva, tomándolas todas juntas, las categorías incluyen todas las posibilidades, no queda un elemento fuera de la clasificación. No ambigua, clara y precisa para que no sea incierta. Repetible, al realizar nuevamente la clasificación se obtienen los mismos resultados. Aceptada, debe ser lógica e intuitiva, y por último debe se útil contribuye en el entendimiento dentro del campo de estudio [1].

Se han realizado diversos intentos de obtener una clasificación de ataques o incidentes de seguridad, buscando cumplir con la mayor cantidad de las características ya citadas, entre otras tenemos:

Lista de términos. Es una lista simple de términos a los que se les da su correspondiente definición. En estas listas de términos se pueden mencionar como ejemplos la de Cohen [1] y la de Icove [2] que incluye entre sus términos: Negación de servicios, piratería de software, copia no autorizada de datos, degradación de servicios, análisis de tráfico, virus y gusanos, ataques de tiempo, caballos troyanos, bombas lógicas, entre otros.

Lista de categorías. Esta es una segunda aproximación a una taxonomía de ataques, en la cual ya se introduce un elemento de mayor estructura. Se incluye en esta la de Cheswick y Bellovin [3] quienes toman siete categorías para clasificar los ataques: Robo de contraseñas, Ingeniería social, Errores de software y puertas traseras, Fallas de autenticación, Fallas de protocolos, Fugas de información y Negación del servicio.

Categorías de resultados. Esta es otra variación al método de la lista, en donde se agrupan los ataques de acuerdo con los resultados obtenidos. Como ejemplo se puede citar la clasificación proporcionada por Cohen quien habla de corrupción (modificación no autorizada), fuga (cuando la información termina en donde no debiera) y negación (cuando los computadores o redes no están disponibles para su uso por usuarios autorizados). También se puede realizar la definición de la categoría de resultados usando los términos opuestos. Ejemplo de ello es la lista presentada por Russell y Gangemi [4] quienes hablan de 1) secreto y confidencialidad, 2) exactitud, integridad y autenticidad y 3) Disponibilidad.

Listas empíricas. Esta es una variación de la taxonomía de resultados con tres categorías, que se desarrolla usando una lista más larga basada en datos de clasificación empírica. Un ejemplo es la taxonomía de Neumann y Parker [5] con ocho categorías: Robo externo de información, Abuso externo de recursos, Enmascaramiento, Programas plaga, Sobrepasar autenticación o autorización, Abuso de autoridad, Abuso a través de la inacción y Abuso indirecto.

La crítica que se hace a esta clasificación es que resulta más difícil de recordar, menos intuitiva y no hay una estructura que muestre relaciones entre las categorías.

Matrices. Este es un esquema de clasificación, basado en dos dimensiones. Por ejemplo la de Perry y Wallich[6] en donde las dos dimensiones son: vulnerabilidades (destrucción física, destrucción de información, robo de servicios, exploración y robo de información) y atacantes potenciales (Operadores, programadores, encargados de captura de datos, internos, externos, intrusos).

Otra aproximación matricial que se puede mencionar, es la de Landwehr [7] quien utiliza una matriz tridimensional: Génesis (como surge el defecto de seguridad en un programa), tiempo de introducción (en el ciclo de vida del software y el hardware) y ubicación (en software o hardware). Por ejemplo el Génesis se divide en dos categorías amplias: fallos intencionales y fallos inadvertidos.

Taxonomías basadas en procesos. Este tipo de taxonomía provee un marco de trabajo para el análi-

sis de los ataques e incidentes. Se parte de los procesos normales que se tienen en el manejo de la información. Stallings [8] presenta un modelo, enfocado en la información en tránsito, que clasifica las amenazas de seguridad en cuatro categorías

(interrupción intercepción, modificación, fabricación), vistas estas como ataques pasivos o activos. Este es un modelo simplificado que sin embargo, brinda una claridad conceptual, adecuada para el análisis de los ataques.

Taxonomías basadas en procesos – Orientación al acceso. En esta aproximación un ataque se puede ver como un proceso que permite a un atacante alcanzar unos objetivos o motivaciones, es decir, un enlace válido entre un atacante y sus objetivos [9] para lograr esto se requiere un medio, un camino y un fin, que se pueden describir también como una herramienta, un acceso y un resultado, lo cual es más claro en la Figura 1.

Figura 1. Enlace atacante - objetivos

- ***Atacantes***. Rusell [4] presenta dos categorías de atacantes de acuerdo al origen del atacante con respecto a la entidad atacada: internos y externos. En los internos se incluyen empleados, estudiantes, etc., dependiendo del tipo de organización. Los externos incluyen, entre otros, agentes de inteligencia extranjeros, terroristas, criminales, atracadores corporativos y *hackers*.

  Una aproximación alternativa es utilizada por Icove [2] para identificar a los atacantes por su motivación principal, presentando tres categorías: *Hackers*, Criminales y Vándalos.

  Howard, divide a los atacantes en seis categorías: *Hackers*, Espías, Terroristas, Intrusos corporativos, Criminales profesionales y Vándalos.
- ***Herramientas.*** Se establecen las siguientes categorías en cuanto a las herramientas utilizadas para desarrollar el ataque: Comandos de usuario, Script o programas, Agente autónomo, Caja de herramientas (toolkits), Herramientas distribuidas y Tomas de datos (data tap).
- ***Acceso*** Para que el atacante logre alcanzar su objetivo requiere establecer un enlace válido, en donde esta involucrado un acceso no autorizado, o un uso no apropiado, tomando ventaja de una vulnerabilidad de la red o del sistema. Las vulnerabilidades pueden provenir de tres formas: problema de implementación, error del diseño y error de configuración.
- ***Resultados.*** Las categorías de resultados de un ataque se definen así: Corrupción de información, Divulgación de información, Robo de servicios y Negación del servicio.

La taxonomía desarrollada es entonces una representación de la ruta que un atacante debe tomar para alcanzar sus objetivos. Para tener éxito, un atacante debe encontrar uno o más caminos válidos que lo conecten con sus objetivos, tal vez de forma simultánea.

- ***Objetivos***. Se presentan cuatro grupos de objetivos que diferencian los atacantes: cambio, conocimiento y estatus, ganancia financiera, ganancia política y daño.

Taxonomías basadas en procesos – Orientación al evento. Esta clasificación es un refinamiento de la taxonomía orientada al acceso. En este caso, el concepto de evento reemplaza el concepto de acceso que primaba en las taxonomías basadas en procesos anteriores. (ver Howard y Longstaff [10]).

Eventos. Un evento se define como un cambio discreto de estado de un sistema o dispositivo. Este cambio de estado es el resultado de una acción emprendida por un usuario, es decir existen eventos válidos sobre un sistema. Para que dicho cambio sea de interés de la seguridad en redes y computadores, debe ser el resultado de acciones de un atacante contra un blanco en busca de un objetivo determinado.

La acción se define como un paso tomado por un usuario o un proceso para alcanzar un resultado y el blanco se define como una entidad lógica de cómputo o de red (cuenta, proceso o dato) o una entidad física (componente, computador, red o interred).

El listado de acciones que pueden ser emprendidas son: Prueba, Escaneo, Inundación, Autenticación, Sobrepaso, Inundación, Lectura, Copia, Robo, Modificación y Borrado.

Y los blancos sobre los cuales se da la acción son: Cuenta, Proceso, Datos, Componente, Computador, Red e Interred.

Atacantes: se clasifican de acuerdo con el objetivo que ellos quieren alcanzar (similar a la taxo-

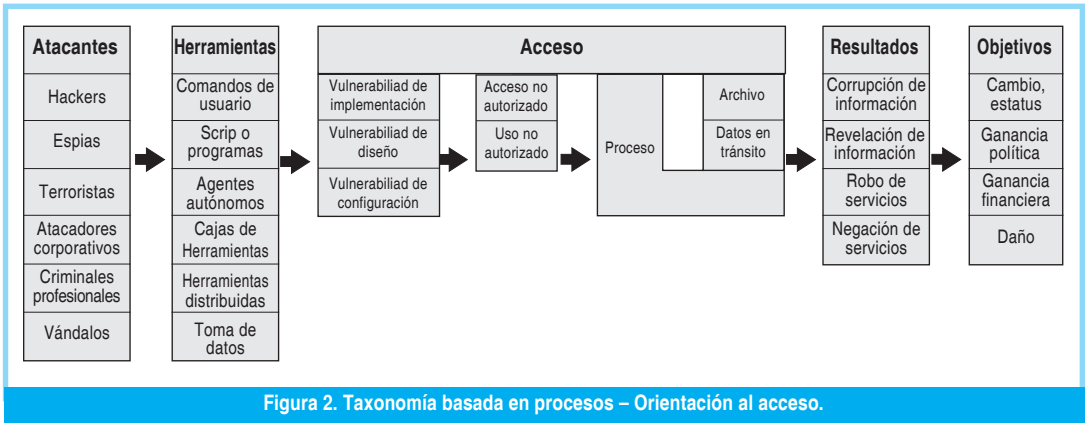

Figura 2. Taxonomía basada en procesos – Orientación al acceso.

nomía orientada al acceso), adicionando una categoría que es la de mirones.

Ataque. Conexión válida que involucra herramientas, vulnerabilidades, eventos y resultados no autorizados. Son los propietarios administradores de los sistemas quienes determinan que es lo que esta autorizado y que no, mediante la definición de políticas de seguridad.

Herramienta: medio que puede ser utilizado para explotar una vulnerabilidad de un computador o de una red. Se completa la lista empleada en la taxonomía orientada al acceso con: Ataque físico e Intercambio de información.

Resultado autorizado es aquel que esta aprobado por los propietarios o administradores y no autorizado es aquel que no es aprobado. Para que tenga éxito, el atacante de- be encontrar caminos que puedan ser conectados (ataques), tal vez en forma simultánea o repetidamente.. En torno al resultado no autorizado, definido como una consecuencia no autorizada de un evento, se adiciona a los contemplados en la taxonomía orientada al acceso la categoría de incremento en el acceso, ampliando la categoría de robo de servicios al robo de recursos.

El éxito del incidente se alcanza por el atacante cuando se cumplen sus objetivos. El éxito de un ataque individual es alcanzado cuando se obtiene un resultado no autorizado.

3. AJUSTES A LA TAXONOMÍA BASADA EN PROCESOS – ORIEN TACIÓN AL EVENTO.

Al definir en forma más acertada el proceso que conecta a un atacante con sus objetivos como «incidente», la taxonomía orientada al evento hace una mejor aproximación, en relación con la definición que realizaba la taxonomía orientada al acceso, que tomaba esta secuencia como un «ataque».

A pesar de que las taxonomías basadas en procesos (orientada a acceso y orientada a evento) describen en una forma clara los incidentes de seguridad, estas clasificaciones adolecen de problemas. Uno de ellos es no ser exhaustivas frente al tema de los atacantes. A pesar de que se trata de cubrir el conjunto de posibles atacantes externos faltan aquellos que completan la secuencia atacante, ataque, objetivos, pero sus objetivos no tienen relación con el sistema afectado, ej. Robo de cable ó negación de servicios en un tercer sistema; la lista también es incompleta, en cuanto a atacantes internos, faltando aquellos que, mediante el uso no autorizado de recursos de cómputo y redes, emprenden una acción en forma accidental que por ser realizada en forma repetitiva pone en riesgo los sistemas (ej Aquellos que descargan programas, música, imágenes, causando degradación o negación de servicios), faltan también aquellos que provocan corrupción de información y pueden ocasionar daños o perdidas financieras para una entidad, sin que puedan ser clasificados como vándalos, ya que su intención no es hacer daño, es decir, lo causan con la actuación descuidada frente a sus labores (operadores incompetentes, administradores descuidados)

Se presenta el problema frente a la relación atacante – motivación, ya que aparentemente el objetivo del atacante en estos tres casos no es provocar la caída o degradación de los servicios, pero este es el resultado alcanzado.

Este tipo de atacante no se ha considerado en las taxonomías presentadas dado que, siendo un atacante interno no utiliza los recursos de interred para acceder a los datos y modificarlos o dañarlos, pero con el auge de los servidores de aplicaciones de Internet se observa que la frontera es cada vez más

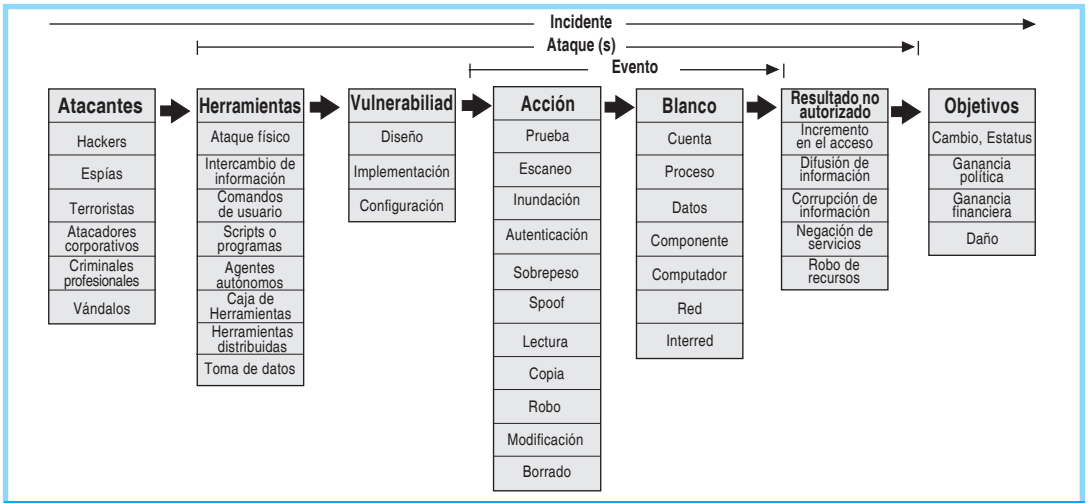

Figura 3. Taxonomía basada en procesos – Orientación al evento

difusa entre las áreas de competencia de seguridad interna y la seguridad de intercedes o Internet.

Haciendo una comparación entre los dos tipos de atacante (internos y externos) tomando como herramientas de análisis su intencionalidad y el tipo de acceso utilizado, se muestra que hay tres tipos de atacantes que pueden ser incluidos en la taxonomía a efectos de hacer exhaustiva la relación de atacantes:

1. Delincuentes: Aquellos que con una motivación de lucro personal, en una forma completamente indirecta provocan negación de servicio por medio de daño físico a redes e infraestructura de soporte.
2. Trabajadores incompetentes: Empleados o agentes internos de una compañía o entidad que debido a la falta de calificación o competencia provocan daño sobre cualquiera de los elementos componentes de un sistema, incluyendo información y pueden llegar a causar negación de servicio.
3. Trabajadores incorrectos: Aquellos que en una forma incidental o intencional provocan daño o afectación en un sistema o cualquiera de sus componentes.

Con respecto al término *hackers* utilizado por los diferentes autores, no se puede olvidar que no es universalmente aceptado y que se tienen múltiples definiciones del mismo.

En el tema de herramientas empleadas para realizar un ataque, en la taxonomía orientada al acceso se observaba una carencia en el tema del ataque físico que fue subsanada en la taxonomía orientada al evento, dicha falta es notoria cuando se mira la disponibilidad de los servicios como un factor crítico.

Pero al adicionar el ataque físico a la lista de las herramientas empleadas, se encuentra una vulnerabilidad adicional a las de diseño, implementación y configuración, que puede ser mencionada como vulnerabilidad de disposición o ubicación, y que esta relacionada con todas las probabilidades de ataque físico que se tienen en un sistema y sus componentes de soporte (sistemas eléctricos y redes eléctricas reguladas, sistemas de cableado, sistemas de transmisión de información, etc.).

No se puede desconocer que con el auge de los servidores de aplicaciones, servicios brindados en Internet y redes privadas virtuales, una manera muy fácil de causar una negación de servicio es atacar sus sistemas de soporte. Infortunadamente, frente a estos problemas, los encargados de la seguridad computacional e Internet únicamente tienen mecanismos como planes de contingencia con medidas alternativas (accesos vía MODEM, plantas de emergencia, etc.)

Visto el párrafo anterior, se observa también una falta en el listado de acciones directamente relacionada con el ataque físico y que puede ser mencionada como «daño físico», el cual tendrá como consecuencia una negación de servicio, un robo de recursos (componentes de soporte altamente importantes, etc.), con sus correspondientes objetivos, daño, perdida de imagen o perdida financiera para la entidad afectada. De igual manera, los blancos se deben adicionar con los sistemas de soporte, cuya afectación, como se ha analizado, es potencial causa para negación de servicios o pérdida o daño de información. Con las observaciones anteriores, una descripción más completa de la taxonomía de incidentes de seguridad puede presentarse como se muestra en la Figura 4.

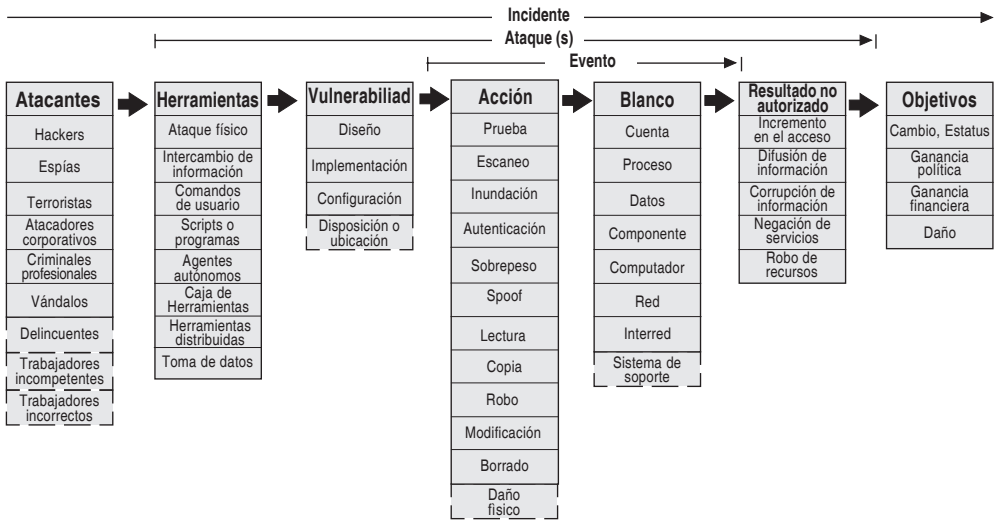

Figura 4. Taxonomía completa de incidentes de seguridad

4. CONCLUSIONES

A pesar de existir diversas aproximaciones a una apropiada clasificación taxonómica de incidentes de seguridad, no se ha llegado a un consenso en cual es la forma más apropiada de mantener y ordenar la información recolectada de este tipo de eventos. Es por ello que se siguen sugiriendo formas para hacerlo. El resumen de las clasificaciones históricas presentado, en general no recoge la idiosincrasia de un país como el nuestro, en donde la seguridad informática no ha cobrado la importancia que tiene y se mira como un tema secundario, al igual que la misma afectación que sufren los sistemas. A pesar de que se sabe de numerosos incidentes, estos no se encuentran adecuadamente documentados, sin tomar en cuenta que ni siquiera existe una entidad que tome como suya la función de coordinar los esfuerzos de manejar incidentes y recopilar información. La clasificación acá presentada sugiere una manera en que una organización o entidad que asuma dicha labor puede acopiar y organizar en forma apropiada todos los datos relevantes de tal forma que se presten para hacer análisis y establecer similitudes que permitan manejar adecuadamente los incidentes de seguridad en informática y en particular en Internet, incluyendo algunos tipos de incidentes particulares nuestros, en donde la afectación surge como una consecuencia no deseada de acciones cuyo propósito específico no es causar daño a nuestros sistemas o datos, sino que surge en forma inintencional, como efecto secundario del descuido, del vandalismo o del intento de causar daño a terceros

5. REFERENCIAS BIBLIOGRÁFICAS

[1] Federick B. Cohen, Protection and Security on the Information Superhighway, John Wiley & Sons, New York, Estados Unidos, 1995.

[2] David Icove, Karl Seger y William VonStorch, Computer Crime: A Crimefighter's Handbook, O'Reilly & Associates, Inc., Estados Unidos, 1995.

[3] William R. Cheswick y Steven M. Bellovin, Firewalls and Internet Security: Repelling the Wily Hacker, Addison-Wesley Publishing Company, Estados Unidos, 1994.

[4] Deborah Russell y G. T. Gangemi, Sr., Computer Security Basics, O'Reilly & Associates, Inc., Sebastopol, Estados Unidos, 1991

[5] Peter Neumann y Donald Parker, «A Summary of Computer Misuse Techniques,» Proceedings of the 12th National Computer Security Conference, 1989.

[6] T. Perry y P. Wallich, «Can Computer Crime Be Stopped?,» IEEE Spectrum, Vol. 21, No. 5.

[7] Carl E. Landwehr, Alan R. Bull, John P. McDermott, y William S. Choi, «A Taxonomy of Computer Security Flaws,» ACM Computing Surveys, Vol. 26, No. 3, Septiembre, 1994, pp. 211-254.

[8] William Stallings, Network and Internetwork Security Principles and Practice, Prentice Hall, Englewood Cliffs, NJ, USA, 1995.

[9] Howard, John D., An Analysis of Security Incidents on the Internet 1989 – 1995, Tesis para optar por el título de Doctor en Filosofía, Carnegie Mellon University, Estados Unidos, 1997

[10] John D. Howard, Thomas A. Longstaff, A Common Language for Computer Security Incidents, Sandia Report, Sandia National Laboratories, Departamento de Energía, Estados Unidos, 1998.

Zulima Ortiz Bayona

Master en Matemáticas, Especialista en Teleinformática Universidad Distrital Coordinadora proyecto curricular de Ingeniería de Sistemas Universidad Distrital Francisco José de Caldas. Profesora Universidad Nacional. zulima@cable.net.co

Francisco Galindo Pulido

Ingeniero de sistemas - Universidad Nacional de Colombia. Master en Teleinformática -Universidad Distrital Francisco José de Caldas. Jefe Oficina Informática y Telecomunicaciones – Instituto Geográfico Agustín Codazzi. fgalindo@igac.gov.co